AutoUni – Schriftenreihe

Christian Jaksch

Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes

Grundrechtsschutz in einem Konzern vor dem Hintergrund neuer Technologien

AutoUni – Schriftenreihe

Band 143

Reihe herausgegeben von/Edited by
Volkswagen Aktiengesellschaft
AutoUni

Die Volkswagen AutoUni bietet Wissenschaftlern und Promovierenden des Volkswagen Konzerns die Möglichkeit, ihre Forschungsergebnisse in Form von Monographien und Dissertationen im Rahmen der „AutoUni Schriftenreihe“ kostenfrei zu veröffentlichen. Die AutoUni ist eine international tätige wissenschaftliche Einrichtung des Konzerns, die durch Forschung und Lehre aktuelles mobilitätsbezogenes Wissen auf Hochschulniveau erzeugt und vermittelt.

Die neun Institute der AutoUni decken das Fachwissen der unterschiedlichen Geschäftsbereiche ab, welches für den Erfolg des Volkswagen Konzerns unabdingbar ist. Im Fokus steht dabei die Schaffung und Verankerung von neuem Wissen und die Förderung des Wissensaustausches. Zusätzlich zu der fachlichen Weiterbildung und Vertiefung von Kompetenzen der Konzernangehörigen fördert und unterstützt die AutoUni als Partner die Doktorandinnen und Doktoranden von Volkswagen auf ihrem Weg zu einer erfolgreichen Promotion durch vielfältige Angebote – die Veröffentlichung der Dissertationen ist eines davon. Über die Veröffentlichung in der AutoUni Schriftenreihe werden die Resultate nicht nur für alle Konzernangehörigen, sondern auch für die Öffentlichkeit zugänglich.

The Volkswagen AutoUni offers scientists and PhD students of the Volkswagen Group the opportunity to publish their scientific results as monographs or doctor’s theses within the “AutoUni Schriftenreihe” free of cost. The AutoUni is an international scientific educational institution of the Volkswagen Group Academy, which produces and disseminates current mobility-related knowledge through its research and tailor-made further education courses. The AutoUni's nine institutes cover the expertise of the different business units, which is indispensable for the success of the Volkswagen Group. The focus lies on the creation, anchorage and transfer of knew knowledge.

In addition to the professional expert training and the development of specialized skills and knowledge of the Volkswagen Group members, the AutoUni supports and accompanies the PhD students on their way to successful graduation through a variety of offerings. The publication of the doctor’s theses is one of such offers. The publication within the AutoUni Schriftenreihe makes the results accessible to all Volkswagen Group members as well as to the public.

Reihe herausgegeben von/Edited by
Volkswagen Aktiengesellschaft
AutoUni
Brieffach 1231
D-38436 Wolfsburg
http://www.autouni.de

Weitere Bände in der Reihe http://www.springer.com/series/15136

Christian Jaksch

Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes

Grundrechtsschutz in einem Konzern vor dem Hintergrund neuer Technologien

Springer

Christian Jaksch
AutoUni
Wolfsburg, Deutschland

Zugl.: Dissertation, Universität Wien, 2018. Das vorliegende Buch ist eine auf Stand Oktober 2019 aktualisierte und modifizierte Fassung der approbierten Dissertation.

Die Ergebnisse, Meinungen und Schlüsse der im Rahmen der AutoUni – Schriftenreihe veröffentlichten Doktorarbeiten sind allein die der Doktorandinnen und Doktoranden.

ISSN 1867-3635 ISSN 2512-1154 (electronic)
AutoUni – Schriftenreihe
ISBN 978-3-658-29449-6 ISBN 978-3-658-29450-2 (eBook)
https://doi.org/10.1007/978-3-658-29450-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar

Springer ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort und Dank

Seit 25. Mai 2018 gilt nun europaweit und unmittelbar anwendbar die Datenschutz-Grundverordung (EU) 2016/679 (DSGVO). Es ist zu prüfen, wie weit dieses Europäische Regelwerk in Zusammenschau mit dem EU-Primärrecht der EU-Grundrechte-Charta (Art 7 und Art 8 EU-GRC) im Grundrechts- und Datenschutz für internationale europäische Konzerne am IT-gestützten Arbeitsplatz eine Vereinheitlichung über die nun europaweit geltenden einheitlichen Grundsätze erreichen kann, oder ob weiter eine völlige Unterschiedlichkeit durch die nationalen Rechtsordnungen bestehen bleibt.

Die Arbeit orientiert sich dabei an den aktuellen Bedrohungszenarien für den IT-gestützten Arbeitsplatz, denen das Datenschutzrecht und die dem Datenschutz zugrundeliegenden Grundrechte mit den dazu korrespondierenden staatlichen Schutzpflichten entgegenwirken wollen.[1] Die Analyse erfolgt rechtsvergleichend zwischen Deutschland und Österreich:

Kapitel 2:

- Grundrechteschutz vor nationalen innerstaatlichen behördlichen Eingriffen;
- direkt aus diesen Grundrechten resultierende staatliche Schutzpflichten, u.a. durch Schaffung von durchsetzbaren Strafbestimmungen (z.B. gegen Cyber-Kriminelle).

Kapitel 3 und **Kapitel 4:**

- Datenschutzrecht und IT-Arbeitsrecht als rechtlicher Rahmen für private Akteure.

Kapitel 5:

- Neue Technologien (z.B. „Digitale Assistenten“) für den IT-gestützten Arbeitsplatz und Technologiekompatibilität der DSGVO.

Kapitel 6:

- Datenschutzrisiken durch ausländische Staaten (z.B. staatliche Auslandsaufklärung).

Aufgrund der Komplexität des europäischen Datenschutzrechts werden in den **Kapitel 3** und **Kapitel 4** die national zusätzlich zur DSGVO weiter bestehenden europarechtlichen Bestimmungen (ePrivacy-RL 2002/58/EG, Citizens‘ Rights Richtlinie 2009/136/EG) und auch die speziellen nationalen gesetzlichen Bestimmungen in Deutschland und Österreich sowie auch das relevante IT-Arbeitsrecht hinsichtlich ihrer weiteren Anwendbarkeit im Zusammenhang mit der DSGVO im Beschäftigtenverhältnis dargestellt und analysiert.

Anschließend erfolgt in **Kapitel 5** die datenschutzrechtliche Prüfung neuer Technologien für den IT-gestützten Arbeitsplatz. Dabei handelt es sich um sogenannte Digitale Assistenten, die sich weitgehend auf folgende datenschutzrelevante Technologien stützen:

- Sprachsteuerung,
- Cloud Computing,

---

1 Definition der Risiken angelehnt an *Friedewald/Quinn/Hansen/Heesen/Hess/Lamla/Matt/Roßnagel/Trepte/Waidner*, White Paper Datenschutz-Folgenabschätzung[3] (2017) 30 f, abrufbar unter: https://www.forum-privatheit.de/wp-content/uploads/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf (zuletzt abgerufen am 20.06.2019).

- Big Data,
- Enterprise Search.

Diese neuen Technolgien für den IT-gestützten Arbeitsplatz schaffen einerseits neue Möglichkeiten effizienter und effektiver zu arbeiten, zugleich werden andererseits die Datenschutzrisiken dramatisch erhöht. Hierzu bedarf es einer Balance um einen rechtssicheren Betrieb sicherstellen zu können.

Aufgrund der Implementierung von Cloud Computing Technologien ist zusätzlich ein besonderes Augenmerk auf die datenschutzrechtlichen Risiken durch Drittstaatszugriffe zu legen. Daher muss es – u.a. bedingt durch das EuGH Urteil v. 06.10.2015, C-362/14 („Schrems") – ein wichtiges Anliegen sein, die konkrete Benennung von Datenschutzrisiken, hervorgerufen durch Drittstaaten, die sich u.a. aus dem gesteigerten Einsatz von Cloud Computing Technologien mit weltweiter Datenverarbeitung ergeben, in einem Exkurs zu untersuchen. Folglich wird den aktuellen Datenschutz- und Vertraulichkeitsrisiken für Beschäftigte (inbs. Führungskräfte und Fachspezialisten) eines internationalen Konzerns insofern **Kapitel 6** gewidmet. Im datenschutzrechtlichen Schriftum wird aktuell von *Drackert* kritisiert, dass *„sich in neuerer Zeit keine systematische Analyse und konzentrierte Zusammenstellung [findet], die sich explizit den Risiken der Verarbeitung personenbezogener Daten widmet."*[2] Weiters wird bemängelt, dass *„in der neueren wie älteren Literatur das Bestehen von Datenschutz-Risiken jedoch vielfach unbestimmt vorausgesetzt oder angedeutet* [*wird*]*, sodass daraus für die Frage, welche Risiken der Datenverarbeitung bestehen, nichts folgt.* (...) *Auch in den hinsichtlich ihres Grundlagenteils ergiebigeren neueren Arbeiten zum Grundrecht auf informationelle Selbstbestimmung werden Risiken eher im Rahmen des jeweiligen Modells vorausgesetzt und wegen der dogmatischen Zielsetzung weniger konkret gefasst und nicht selbst zum Gegenstand der Untersuchung gemacht. Die Unsicherheit, die durch das Fehlen einer Untersuchung zu den Risiken der Verarbeitung personenbezogener Daten entsteht, verdeutlichen die zahlreichen kritischen Stimmen zum Grundrecht auf informationelle Selbstbestimmung, das wegen seiner Unklarheit als Stück »Grundrechtstheologie« oder »Bergpredigt des Datenschutzes« kritisiert wird"*[3]

Eine vergleichbare Kritik gibt es auch durch *Caspar Bowden* (ex-Chief Privacy Adviser von Microsoft) hinsichtlich der behördlichen und betrieblichen Datenschutzpraxis und Kontrolle in Europa. *Bowden* kritisierte in seinem Gutachten für das Europäische Parlament, dass *„eine unrealistische und legalistische Perspektive eine Vernachlässigung des Schutzes der EU-Bürger ermöglicht."*[4]

Kapitel 7 widmet sich der Zusammenfassung der Ergebnisse und einem kurzen Ausblick.

Bedanken möchte ich mich bei *Univ.-Prof. Dr. Nikolaus Forgó* (Universität Wien) für die universitäre Betreuung in Wien und Hannover sowie bei *Prof. Dr. Tina Krügel, LL.M.* (Leibniz Universität Hannover) und *Univ.-Prof. Dr. Wolfgang Brodil* (Universität Wien) für die Gutachtenerstellung.

2 *Drackert,* Die Risiken der Verarbeitung personenbezogener Daten (2014) 9.

3 *Drackert,* Die Risiken der Verarbeitung personenbezogener Daten (2014) 10 f.

4 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 35.

Bei Volkswagen möchte ich mich bedanken bei *Dr. Christoph Alt* und *Gerrit von Daacke* für die Aufnahme im Volkswagen Doktorandenprogramm[5] und ihren sehr wertschätzenden Umgang sowie bei *Sarah Scholle* für ihre starke Kollegialität im August/September 2018.

Danke sagen möchte ich auch meinem *Vater*, meiner Schwester *Elke* und ihrem Lebensgefährten *Emmanuel*, meinen Großeltern *Trude* und *Franz*, meinem Onkel *Dieter* und seiner Frau *Barbara* sowie meiner Nichte *Maya* für ihre moralische Unterstützung.

Vielen Dank an Sie / Euch alle!

Wien/Hannover/Wolfsburg Christian Jaksch

5 Volkswagen Doktorandenprogramm: https://www.volkswagen-karriere.de/de/ihr-einstieg/absolvent/promotion.html

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

Abkürzungsverzeichnis

ABGB	Allgemeines bürgerliches Gesetzbuch
Abs	Absatz
Abschn	Abschnitt
AEUV	Vertrag über die Arbeitsweise der Europäischen Union.
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
AngG	Angestelltengesetz
ArbStättV	Arbeitsstättenverordnung
ArbVG	Arbeitsverfassungsgesetz
Art	Artikel
Aufl.	Auflage
AVRAG	Arbeitsvertragsrechts-Anpassungsgesetz
BDSG	Bundesdatenschutzgesetz
bearb.	bearbeitet
BetrVG	Betriebsverfassungsgesetz
BG	Bundesgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof Deutschland
Blg	Beilage,-n
BlgNR	Beilage(n) zu den stenographischen Protokollen des Nationalrates
BM	Bundesminister/-in, Bundesministerium
BMI	Bundesministerium des Inneren
BT-Drs	Bundestag Drucksache
B-VG	Bundes-Verfassungsgesetz
BVerfG	Bundesverfassungsgericht Deutschland
bzgl	bezüglich
bzw.	beziehungsweise
ca	circa
CALO	Cognitive Assistant that Learns and Organizes
CEO	Chief Executive Officer
CTR	Computing Tabulating Recording Company
d	deutsch (vor einer Abkürzung)
DARPA	Defense Advanced Research Projects Agency
dgl	dergleichen
d.h.	das heißt
d.s.	das sind
DEHOMAG	Deutsche Hollerith Maschinen Maschinen GmbH
DM	Deutsche Mark (Westdeutsche Mark)

DSB	Datenschutzbehörde Österreich
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung (EU) 2016/679
DSK	Datenschutzkomission Österreich
DSRL	EG-Datenschutzrichtlinie 95/46/EG
DSRL-IJ	Datenschutzrichtlinie (EU) 2016/680 für Polizei und Strafjustiz
DV	Datenverarbeitung
ECG	E-Commerce-Gesetz
EDV	Elektronische Datenverarbeitung
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EGMR	Europäische Gerichtshof für Menschenrechte (Europarat)
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten
ePrivacy-RL	Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG
ePrivacy-VO	Verordnung über Privatsphäre und elektronische Kommunikation
Erk	Erkenntnis
ERP	Enterprise-Resource-Planning
etc.	et cetera
EU	Europäische Union
EU-GRC	Europäische Grundrechte Charta
EuGH	Europäischer Gerichtshof (EU)
EUR	Euro
EWR	Europäischer Wirtschaftsraum
f	und der, die folgende
ff	und die folgenden
gem	gemäß
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System
gü.	Gegenüber
GVBl.	Gesetz- und Verordnungsblatt
H.	
I.	Heft
h.A.	herrschende Ansicht
HGB	Handelsgesetzbuch
hL	herrschende Lehre
hM	herrschende Meinung
HP	Hewlett-Packard Company
HR	Human Relation
hrsg.	herausgegeben
Hrsg.	Herausgeber
HTML	Hypertext Markup Language
http	Hypertext Transfer Protocol

IBM	International Business Machines
idF	in der Fassung
idR	in der Regel
idS	in diesem Sinn
ieS	im engeren Sinn
iHv	in Höhe von
inkl	inklusive
insb	insbesondere
iS	im Sinne
iSd	im Sinn des/der
iSv	im Sinn von
IT	Informationstechnik
iVm	in Verbindung mit
iZh.	im Zusammenhang mit
Jud	Judikatur
k.A.	kein Autor
leg cit	legis citatae (der zitierten Vorschrift)
mA.	meiner Ansicht
M.E.	meines Erachtens
m.E.	meines Erachtens
Mio	Million(en)
Mrd	Milliarde(n)
mwN	mit weiteren Nachweisen
Nr.	Nummer
NR	Nationalrat Österreich
ö	österreichisch (vor einer Abkürzung)
OGH	Oberste Gerichtshof Österreich
OLG	Oberlandesgericht
PAL	Personal Assistant that learns
PDF	Portable Document Format
RdW	Recht der Wirtschaft
RL	Richtlinie der EU bzw. EG
RN	Randnummer (-note)
RS	Rechtssätze (iSv OGH Judikatur)
Rsp	Rechtsprechung (iSv Judikatur)
RWZ	Österreichische Zeitschrift für Rechnungswesen
Rz	Randziffer
s	siehe
S.	a) Satz, b) Seite, -n

SRI	Standford Research Institute
str	streitig
tbd	to be determined (noch festzulegen)
TK	Telekommunikation
TKG 2003	Telekommunikationsgesetz Österreich
TKG 2004	Telekommunikationsgesetz Deutschland
TMG	Telemediengesetz Deutschland
tlw.	teilweise
Tz	Textzahl
u.a.	a) und andere b) unter anderem
uÄ	und Ähnliche/-s
udgl	und dergleichen
UGB	Unternehmensgesetzbuch
USD	US-Dollar
usw	und so weiter
u.U.	unter Umständen
v	vom, von
V	Verordnung
va	vor allem
vgl.	vergleiche
VO	EU-Verordnung
vs	versus
VStG	Verwaltungsstrafgesetz 1991
VZG	Volkszählungsgesetz
WWW	World Wide Web
Z	Zahl, Ziffer
z.B.	zum Beispiel

1 Einleitung Datenschutz und Digitalisierung

1.1 Geschichtliche Entwicklung von Datenschutz im Zusammenhang mit technischen Entwicklungen

1.1.1 Staatlicher Datenmissbrauch in den Jahren 1933 – 1945

Der Amerikaner Herman Hollerith – Gründer der *Tabulating Machine Company* (1896) und Begründer des gesamten Industriezweigs der Datenverarbeitung – hatte Ende des 19. Jahrhunderts mit der Lochkartenmaschine eine Technik entwickelt, welche die staatliche und wirtschaftliche Datenverarbeitung revolutionieren sollte und bis zum Aufkommen der ersten Computer das Kernstück der staatlichen und industriellen Datenverarbeitung bis weit in das 20. Jahrhundert bildete. Gestützt auf diese Technologie eröffnete im Jahr 1910 der Industrielle Willy Heidinger – mit den gesamten Produktions- und Vertriebsrechten von Hollerith-Maschinen für Deutschland und Südosteuropa in seinen Händen – in Berlin die Deutsche Hollerith Maschinen GmbH (DEHOMAG). Sogleich erhielt das Unternehmen staatliche Aufträge für Volkszählungen in Württemberg, Elsaß-Lothringen, Baden und Preußen, die erfolgreich abgeschlossen werden konnten. Im Jahr 1911 verkaufte Herman Hollerith in den USA sein Unternehmen, welches sich anschließend zur *Computing Tabulating Recording Company* (CTR) umbenannte.

Thomas J. Watson war vom Verkäufer von Klavieren und Nähmaschinen zum Ende des 19. Jhdt durch harte Arbeit schließlich im Jahr 1922 zum Vorstandsvorsitzenden bei der CTR aufgestiegen, die 2 Jahre später durch ihn selbst zur *International Business Machines Corporation* (IBM) umbenannt wurde. Die 1910 von Willy Heidinger in Berlin gegründete DEHOMAG war seither Lizenznehmerin von CTR (ab 1924 IBM) und konnte aufgrund der Geldentwertung im Deutschen Reich in den 1920er Jahren keine Lizenzgebühren für Hollerith Maschinen in die USA auszahlen. Der Vorstandsvorsitzende Watson fuhr 1922 persönlich von New York nach Deutschland und stellte den Eigentümer der DEHOMAG, Willy Heidinger, vor die Wahl: Entweder Konkurs oder Übertragung von substanziellen Anteile iHv. 90% an Watsons amerikanische IBM, womit die DEHOMAG schließlich eine unmittelbare Tochtergesellschaft von IBM wurde und direkt von New York aus geleitet wurde.[6]

Durch die Machtübernahme der Nationalsozialisten 1933 erreichte die Bedeutung von Datenverarbeitung im Deutschen Reich eine neue Dimension. Ziel des NS-Regimes war es mit Hilfe immer neuer Datenverarbeitungstechniken die soziale und demografische Zusammensetzung der deutschen Bevölkerung zu erfassen und nach den ideologischen Erkenntnissen der NS Erb- und Rassenhygiene umzugestalten und „Volksfeinde“ aufzuspüren. Bereits schon am 12. April 1933 wurde per Reichsgesetz eine Volkszählung angeordnet, welche dann mit Unterstützung der deutschen IBM Tochter DEHOMAG durchgeführt wurde. Im

6 *Sander/Spengler,* Die Entwicklung der Datenverarbeitung von Hollerith Lochkartenmaschinen zu IBM Enterprise-Servern (2011) Kapitel E.1. 7 ff, abrufbar unter: https://www.informatik.uni-leipzig.de/cs/Literature/History/SandnerSpengler.pdf (zuletzt abgerufen am 20.06.2019); *Black*, IBM und der Holocaust (2001) 55.

C. Jaksch, *Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes*,
AutoUni – Schriftenreihe 143, https://doi.org/10.1007/978-3-658-29450-2_1

Juli 1934 wurde das *„Gesetz über die Vereinheitlichung des Gesundheitswesens"* erlassen, welches Ärzte und sonstiges medizinisches Personal verpflichtete, detaillierte Erfassungsbögen über den Gesundheitszustand ihrer Patienten auszufüllen. Die Formulare wurden an die Gesundheitsämter weitergeleitet und im Statistischen Reichsamt in Berlin und den statistischen Landesämtern verarbeitet. Zusammen mit umfangreichen Erfassungsbögen aus dem Versicherungsbereich ergab dies ein detailliertes Gesundheitsprofil der deutschen Gesellschaft. Die Daten wurden über DEHOMAG Maschinen verarbeitet, die von der Hand auszufüllenden Meldebögen waren vorab von DEHOMAG-Ingenieuren und NS-Experten so entworfen worden, dass alle erhobenen Daten auf Hollerith-Lochkarten übertragen werden konnten. Ende 1934 lieferten neben medizinischen Einrichtungen und Versicherungen auch Pflege- und Erholungsheime und sonstige Beschäftige aus dem Gesundheitswesen Daten für die Verarbeitung mittels Hollerith-Lochkarten. Auf Basis dieser Daten konnte schließlich ein Register aller *„gemeinschaftsunfähigen Personen*" erstellt werden. Zudem konnte im Jahr 1934 der Statistiker Karl Keller die politische Wunschvorstellung des NS-Regimes bestätigen, dass es durch die detaillierte Auswertung der Stammbücher gelingen würde, alle Juden (inkl. Nichtgläubiger bzw. zum Christentum konvertierten) in Deutschland zu identifizieren. Um dies zu erreichen bräuchten nur die Übertritte der letzten 130 Jahre aus Kirchenbücher und Standesamtsregister festgestellt werden, weil vor der Judenemanzipation die Zugehörigkeit zur jüdischen Konfession und zum jüdischem Volkstum sich im Wesentlichen deckten. Mit Hilfe der Hollerith-Maschinen wurden daraufhin Taufbücher, Geburts- und Sterberegister sowie Kirchenbücher im gesamten Deutschen Reich durchkämt um Juden herauszufiltern. Schließlich konnte als Ergebnis eine *„Fremdstämmigen-Taufkartei"* erstellt werden, welche tausende Namen von Juden und Angehöriger sonstiger Religionen umfasste, die im letzten Jahrhundert in Deutschland zum Christentum konvertiert waren. Es lagen dem NS-Regime ab Ende der 1930er Jahre somit äußerst sensible Dateien und Register über die deutsche Bevölkerung vor, wie allein die zwei Beispiele zeigen:

- „Register aller gemeinschaftsunfähigen Personen" und
- „Fremdstämmigen-Taufkartei",

mit letztlich tödlichen Folgen für die dort aufgelisteten Betroffenen.[7]

Am 28. Juni 1937 kam es in Berlin zu einem persönlichen Treffen zwischen IBM Vorstandsvorsitzenden Thomas J. Watson und Reichskanzler Adolf Hitler. Watson wurde von Hitler direkt in der Reichskanzlei in Berlin empfangen, anschließend ging es in die Berliner Krolloper, wo Watson von Hitler mit dem "Verdienstkreuz vom Deutschen Adler" (spätere

7 *Black*, IBM und der Holocaust (2001) 50 ff; 69; 119; 121; 133 f; 216 ff; *Snowden*, Permanent Record[2] (2019), 235 ff; *von Lewinski*, Geschichte des Datenschutzrechts von 1600 bis 1977 in Arndt/Betz (Hrsg), Freiheit – Sicherheit – Öffentlichkeit: 28. Assistententagung Öffentliches Recht, Heidelberg 2008 (2009) 196 ff (203).

Rückgabe durch Watson im Jahr 1940) ausgezeichnet wurde[8] (für Verdienste um die Datenverarbeitung mit Hollerith-Maschinen[9]). In einem persönlichen Brief vom 5. Juli 1937 bedankte sich Thomas J. Watson persönlich bei Adolf Hitler: *„Vor meiner Abreise möchte ich Ihnen meinen Stolz und meine tiefe Dankbarkeit für die große Ehre aussprechen, die ich durch die Ordensauszeichnung durch Sie erfahren habe. Ich schätze den Geist der Freundschaft sehr, der dieser Ehre zugrunde liegt und versichere Ihnen, dass ich wie bisher auch in Zukunft mein Bestes geben werde, um noch engere Bande zwischen unseren beiden großartigen Nationen zu schaffen. Meine Frau und meine Familie schließen sich den Grüßen an.“*[10] Im Januar 1938 wurde vom NS-Regime eine neue Reichsmeldeordnung erlassen, welche für das Deutsche Reich eine erste reichseinheitliche Meldegesetzgebung darstellte. Ursprünglich diente das Melderecht als reines Landesrecht der deutschen Staaten bis Ende 1937 den Sicherheitsbehörden als ein Hilfsmittel, den möglichst lückenlosen Nachweis des jederzeitigen Aufenthalts eines Bürgers zu liefern. Durch das NS-Regime erhielt das deutsche Meldewesen gemäß der Reichsmeldeordnung 1938 und darauf erlassenen Runderlässen eine andere Funktion, nämlich Informationen über die Einwohner auch anderen Behörden zur Verfügung zu stellen. Den Meldebehörden wurde eine Reihe von Mitteilungspflichten gegenüber anderen Behörden übertragen und es enthielt auch Regelungen über die Zusammenarbeit von Behörden und über die Erteilung von Auskünften aus dem Melderegister. Aus einem ursprünglich nur sicherheitspolizeilichem Instrument bildete sich der Kern eines Informationssystems für kommunale und staatliche Dienststellen und Behörden über verwaltungsrelevante Daten der Einwohner.[11] Es wurde minutiös geregelt, wem alles die Angaben aus dem Melderegister zu übermitteln waren (z.B. Dienststellen NSDAP, Geheime Staatspolizei – Gestapo, etc.). Diese Daten sollten durch Mitteilungen von Behörden über Vorstrafen, Fahndungsmaßnahmen, Kirchenaustritte, Waffenscheine, Berufsverbote und Inhaftierungen, etc. ergänzt werden. Als nächsten Schritt wurde eine sogenannte „Volkskartei“ geplant – am 18. November 1938 sprach Hermann Göring: *„Durch die Gründung einer Volkskartei soll eine restlose Übersicht über alle Deutschen gewonnen werden.“*[12] Die „Volkskartei“ sollte die Melderegister der Gemeinden ergänzen, denn man wollte Angaben über die Ausbildung und die persönlichen Fähigkeiten und Fertigkeiten registrieren und damit ganze Gruppen und Jahrgänge von Deutschen für staatliche Dienste vorbereiten. Es waren erste Schritte um ein Instrument zur umfassenden Überwachung der deutschen Bevölkerung zu schaffen.[13] Der politische Hintergrund der „Volkskartei“ wurde am 15. Februar 1939 wie folgt beschrieben: „*Von besonderer Wichtigkeit*

8 *Black*, IBM und der Holocaust (2001) 172 ff; DER SPIEGEL 07/2001, 36 ff, Der programmierte Massenmord, abrufbar unter: http://magazin.spiegel.de/EpubDelivery/spiegel/pdf/18479605 (zuletzt abgerufen am 20.06.2019).

9 Vgl. die Liste der Ordensträger: *Wikipedia*, Verdienstorden vom Deutschen Adler, abrufbar unter: https://de.wikipedia.org/wiki/Verdienstorden_vom_Deutschen_Adler (zuletzt abgerufen am 20.06.2019).

10 *Black*, IBM und der Holocaust (2001) 176.

11 BT-Drs. VI/2654, 7; BT-Drs. 7/1059, 9.

12 *Aly/Roth*, Die restlose Erfassung – Volkszählen, Identifizieren, Aussondern im Nationalsozialismus[2] (2005) 54.

13 *Aly/Roth*, Die restlose Erfassung – Volkszählen, Identifizieren, Aussondern im Nationalsozialismus[2] (2005) 26 ff; 49 ff; *Bull*, Datenschutz oder Die Angst vor dem Computer (1984) 192 f; *von Lewinski*, Geschichte des Datenschutzrechts von 1600 bis 1977 in Arndt/Betz (Hrsg), Freiheit –

wird die Kartei für die Reichsverteidigung sein, da sie nicht nur Wehrpflichtige, sondern die gesamte Bevölkerung erfaßt. Es wird im Kriegsfall der Einsatz der Gesamtbevölkerung nur möglich sein und gemäß den Fähigkeiten der einzelnen Personen durchgeführt werden können, wenn in der Volkskartei ein einwandfreier Nachweis der verwendbaren Jahrgänge zur Verfügung steht. Der eigentliche Zweck der Kartei ist ihre Verwendung als Erfassungsmittel. Dieser Zweck ist sofort erfüllt, wenn die Kartei aufgestellt ist und die Wohnungs- und Personenstandsveränderungen laufend eingetragen werden."[14] Während das NS-Regime „Volksfeinden" das Recht auf Leben absprach, sollten die deutschen und österreichischen Bürger und Bürgerinnen im Rahmen der vom NS-Regime ausgerufenen Volksgemeinschaft primär zum reinen Leistungsobjekt für die jeweiligen aktuellen macht- und geopolitischen Bedürfnisses und Ziele des Deutschen Reiches unter nationalsozialistischer Führung degradiert werden und jederzeit ohne bzw. geringe eigene Selbstbestimmung zur unmittelbaren Verwendung dem Reich zur Verfügung stehen. Zur weiteren Effizienzsteigerung gab es Überlegungen zur Einrichtung eines „Deutschen Turms" für die sogenannte „deutsche Kartei". Es handelt sich dabei um Planungen zur Schaffung eines handbetriebenen Großspeichers als nationale Datenbank über jeden deutschen Bürger. Die Überlegung war es in Berlin oder einer anderen zentrale gelegenen deutschen Stadt einen Turm mit 25. Geschoßen zu errichten. Jedes der 25 Geschoße sollte über zwölf kreisförmig angeordnete Räume – für jeden Monat einen – verfügen, in welchem dann wieder jeweils 30 bzw. 31 Schränke für den Tag des Monats eingerichtet werden sollten, die die eigentliche Registratur bzw. Kartei dann enthalten hätten. Das Suchverfahren sollte wie folgt funktionieren: Jeder Deutsche und jede Deutsche sollte eine Nummer als festen Index erhalten (eine Art *Personenkennzeichen*), welche ihm/ihr und seine Daten einen lebenslangen festen Platz im Datenspeicher zuweist. Je nachdem welche Angaben zu einer Person dem Deutschen Reich bekannt gewesen wären, hätten im „Deutschen Turm" verschiedene Verzeichnisse abgesucht werden können, welche alle so strukturiert gewesen wären, dass sie nicht verändert werden hätten müssen.[15]

Am 17. Mai 1939 wurden 750.000 Volkszähler für die Volkszählung 1939 im – bis dahin um das Saarland, um Österreich und die damals (bis Sommer 1945) mehrheitlich deutschsprachigen Grenzregionen der Tschechischen Republik (Sudetenland, Österreichisch-Schlesien, Deutschsüdmähren) vergrößerte – Deutsche Reich eingesetzt. Rund 80 Millionen Bürger mussten im Rahmen einer weiteren Volkszählung detaillierte Informationen über Abstammung, religiöses Bekenntnis und materiellem Besitz angeben. In einem speziellen Formular war zusätzlich anzugeben, ob man von „reinem arischen Blut" wäre. Der Status jedes Großelternteils musste angegeben werden und im Fall von Nachforschungen mit Beweisen belegt werden können. Es wurde das erste Mal auch abgefragt, ob ein Teil der Großeltern „Volljude" wäre. Die Ergänzungskarte für die Abstammung hatte den Zweck die in Planung befindliche Zentralkartei für das zukünftige „Großdeutsche Reich" zu ermöglichen. Jede Karte enthielt eine für die Abstammung codierte Spalte. Insgesamt

---

Sicherheit – Öffentlichkeit: 28. Assistententagung Öffentliches Recht, Heidelberg 2008 (2009) 196 ff (203).

14 *Aly/Roth*, Die restlose Erfassung – Volkszählen, Identifizieren, Aussondern im Nationalsozialismus[2] (2005) 56.

15 *Aly/Roth*, Die restlose Erfassung – Volkszählen, Identifizieren, Aussondern im Nationalsozialismus[2] (2005) 44.

wurde 25 Millionen Ergänzungskarten ausgegeben, für jeden Haushalt. Die Zähler unterlagen dabei dem gesetzlich vom NS-Regime streng verankerten Volkszählungsgeheimnis[16], wodurch jedes Eindringen in die Vermögens- und Einkommensverhältnisse von Seiten der Finanzbehörden ausgeschlossen war. Die Volkszähler waren per Gesetz zur absoluten Verschwiegenheit verpflichtet und sie wurden auch sensibilisiert, dass sie jedes Misstrauen bekämpfen sollten, indem sie den einzelnen Familien eindringlich versicherten, dass die Informationen aus der Volkszählung nicht an die Finanzbehörden weitergegeben werden. Allerdings war das gesetzlich verankerte Volkszählungsgeheimnis für die Volkszählung 1939 im Vergleich zum Volkszählungsgeheimnis für die Volkszählung 1933 in einem entscheidenden Punkt durchbrochen; nämlich in der Form, dass der Passus, der besagte, dass die erhobenen Daten aus der Volkszählung nur zu statistischen Arbeiten verwendet werden dürften und nicht zu andern Zwecken benutzt werden dürften, gestrichen worden war.[17] Die Ergebnisse der Volkszählung waren präzise: Bspw. in Wien wurden 91.480 „Volljuden" und 22.344 „Teiljuden" neu identifiziert. Die Berechnungen der DEHOMAG ergaben im Ergebnis, dass durch die Angliederung des Saarlandes, Österreichs und des Sudentenlandes zwar viele Juden im Vergleich zur Volkszählung 1933 hinzugekommen waren, aber dass gleichzeitig das bisherige Deutsche Reich bereits über 50% seiner ursprünglich jüdischen Bevölkerung (durch Verfolgung, Emigration und Mord) in diesen ersten sechs Jahren NS-Herrschaft verloren hatte.[18]

Das Beispiel der besetzten Länder Frankreich und Niederlande zeigt ebenso tragisch die tödliche Effektivität von Datenerfassung und -verarbeitung: In Frankreich wurde in der Verwaltung bis in die 1940er Jahren keine Hollerith-Technik eingesetzt, das heißt die Katalogisierung und das Aufspüren der zu ermordenden und auszurottenden Menschen musste über Hinweise aus der Bevölkerung und andere polizeilichen Maßnahmen erfolgen. In Frankreich wurden bis zum Ende des II. Weltkrieges 24 % der dort lebenden Juden von den Nationalsozialisten ermordet. In den Niederlanden gab es eine funktionierende Hollerith-Infrastruktur in der Verwaltung und auch die niederländische Bürokratie arbeitete sehr bereitwillig mit Adolf Eichmann zusammen: Bis zum Ende des II. Weltkrieges wurden dort 73 % der niederländischen Juden ermordet.[19] Wie *Aly/Roth* analysieren, war der Rückfall in die Barbarei mit den Methoden einer modernen Bürokratie vorbereitet worden.[20] *Christl* spricht vom mörderischen Missbrauch bürokratischer Datenmacht im Nationalsozialismus.[21]

16 G. v. 12.4.1933 (RGBl. I. S. 199), G. v. 4.10.1937 (RGBl. I. S. 1053).

17 *Supik*, Statistik und Rassismus: Das Dilemma der Erfassung von Ethnizität (2014) 66 f.

18 *Black*, IBM und der Holocaust (2001) 216 ff; *Aly/Roth*, Die restlose Erfassung – Volkszählen, Identifizieren, Aussondern im Nationalsozialismus[2] (2005) 30; *von Lewinski*, Geschichte des Datenschutzrechts von 1600 bis 1977 in Arndt/Betz (Hrsg), Freiheit – Sicherheit – Öffentlichkeit: 28. Assistententagung Öffentliches Recht, Heidelberg 2008 (2009) 196 ff (210).

19 *Meyer* in computerwoche.de (10.04.2001), IBM und der Holocaust: War Watson einer der größten Verbrecher? abrufbar unter: https://www.computerwoche.de/a/ibm-und-der-holocaust-war-watson-einer-der-groessten-verbrecher,559460 (zuletzt abgerufen am 20.06.2019).

20 *Aly/Roth*, Die restlose Erfassung – Volkszählen, Identifizieren, Aussondern im Nationalsozialismus[2] (2005) Klappentext.

21 *Christl*, Kommerzielle Digitale Überwachung im Alltag. Studie im Auftrag der Bundesarbeitskammer (2014) 7, abrufbar unter: https://www.arbeiterkammer.at/infopool/wien/Digitale_Ueberwachung_im_Alltag.pdf (zuletzt abgerufen am 20.06.2019).

Während des Krieges verfügten auch die NS-Konzentrationslager über eigene Hollerith-Abteilungen, denn auch die SS war Kunde bei DEHOMAG und ließ die SS-Rasseerfassung sowie die Datenverarbeitung zu KZ-Häftlingen über Hollerith-Maschinen laufen. Spätestens ab Sommer 1943 wurde jedem nichtdeutschen Häftling die ihm zugewiesene fünfstellige Hollerith-Lochkartennummer zur unmittelbaren Identifizierung auf den Arm tätowiert.[22]

1.1.2 Entwicklung des Datenschutzrechts in Deutschland

Die Erfahrungen der Datenmissbräuche u.a. des NS Regimes führten dazu, dass sich Ende der 1960er Jahre vor dem Hintergrund der informationstechnischen Entwicklungen Persönlichkeiten im universitären Hochschulbereich wie *Wilhelm Steinmüller* und *Adalbert Podlech* intensiv Gedanken machten, wie man diese aufkommenden neuen Technologien als neuen Realitätsbereich sinnvoll normieren könnte.[23] Im Jahr 1970 wurde aufgrund dieser wissenschaftlichen Vorarbeiten das westdeutsche Bundesministeriums des Innern (BMI) in Bonn auf Wilhelm Steinmüller (seit 1966 Professor für Kirchenrecht an der Universität Regensburg) aufmerksam und beauftragte ihn im Dezember 1970 im Rahmen einer „Arbeitsgemeinschaft Datenschutz" ein Gutachten für 40.000 (West-)Deutsche Mark (DM) über Grundfragen des Datenschutzes zu erstellen. Der den Gutachtensauftrag vergebende BMI Referent Auernhammer habe nach *Steinmüller* später kundgetan, dass es sich hier um ein „Himmelfahrtsgutachten" handeln würde.[24] Das Steinmüller-Gutachten (BT-Drs. VI/3826) wurde im Sommer 1971 abgegeben und im September 1972 dem Deutschen Bundestag präsentiert.[25]

Das westdeutsche Bundesland Hessen hatte relativ zeitgleich das landespolitische Ziel vor Augen, informationstechnologischer Vorreiter in der staatlichen Datenverarbeitung für

---

22 *Schönberger*, Big Data – Die Revolution, die unser Leben verändern wird (2014) 191; *Aly/Roth*, Die restlose Erfassung – Volkszählen, Identifizieren, Aussondern im Nationalsozialismus[2] (2005) 26; *Black*, IBM und der Holocaust (2001) 470 ff.

23 *Steinmüller*, Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann, RDV 2007/4, 158 ff; *Steinmüller/Podlech*, Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann, FIfF-Kommunikation 03/2007, 15 ff, abrufbar unter: https://www.fiff.de/publikationen/fiff-kommunikation/fk-2007/fk-3-2007/03_2007_steinmueller.pdf (zuletzt abgerufen am 20.06.2019); *Rost*, Interview mit Prof. Dr. Steinmüller vom März 2009, abrufbar unter: https://www.maroki.de/pub/video/steinmueller/start_video_steinmueller.html (zuletzt abgerufen am 20.06.2019); *Rost*, Interview mit Prof. DDr. Podlech vom November 2008, abrufbar unter: https://www.maroki.de/pub/video/podlech/start_video_podlech.html (zuletzt abgerufen am 20.06.2019); *Rost*, Interview mit Prof. Dr. Lutterbeck vom März 2009, abrufbar unter: https://www.maroki.de/pub/video/lutterbeck/start_video_lutterbeck.html (zuletzt abgerufen am 20.06.2019).

24 *Steinmüller/Podlech*, FIfF-Kommunikation 03/2007, 15 ff; *Steinmüller*, RDV 2007/4, 158 ff; *Rost*, Interview mit Prof. Dr. Steinmüller vom März 2009, ab 8:35min, abrufbar unter: https://www.maroki.de/pub/video/steinmueller/start_video_steinmueller.html (zuletzt abgerufen am 20.06.2019); *Schultze-Melling*, Datenschutz jenseits und diesseits des Atlantiks – Ein Nachruf zum Tod von Alan F. Westin und Wilhelm Steinmüller, ZD 2013, 145; *Lutterbeck,* 20 Jahre Dauerkonflikt: Die Novellierung des Bundesdatenschutzgesetzes*,* in Sokol (Hrsg), 20 Jahre Datenschutz – Individualismus oder Gemeinschaftssinn? (1998) 7 ff (10).

25 BT-Drs. VI/3826, 1.

ganz Westdeutschland zu werden und wurde legistisch in Form eines neuen und weltweit ersten Landesdatenschutzgesetzes aktiv.[26] Der Aufbau und die Konzeption dieses Hessischen Datenschutzgesetzes (GVBl. 1970 I. 625.) unterschied sich jedoch stark vom Konzept des phasenorientierten Datenschutzes aus dem Steinmüller-Gutachten von 1971 (BT-Drs. VI/3826). Das Hessische Datenschutzgesetz fokussierte sich primär auf den Schutz der Datenverarbeitung vor unbefugten Eingriffen (Datensicherheit) und etablierte die Institution des Datenschutzbeauftragten als Kontrollorgan für diese Datensicherheit.[27]

Für Westdeutschland trat am 01. Januar 1978 das Bundesdatenschutzgesetz (BDSG 77) in Kraft. Dieses Gesetz folgte klar dem Konzept des „phasenorientierten Datenschutzes" aus dem Steinmüller-Gutachten von 1971 („erheben", „verarbeiten" und „nutzen"). Nicht umgesetzt wurde die Empfehlung *Steinmüllers* einer verfassungsrechtlichen Absicherung des Datenschutzes im Grundgesetz (GG): *„Ein Datenschutzgesetz ohne verfassungsrechtliches Fundament wäre ein dogmatisch zweifelhafter Ausweg* (…)*"*[28]. Die verfassungsrechtliche Klärung erfolgte im Dezember 1983 durch das BVerfG:[29]

In Westdeutschland war im Jahr 1983 das Volkszählungsgesetz 1983 (VZG 1983)[30] erlassen worden, welches datenschutzrechtliche bzw. verfassungsrechtliche Fragen aufwarf. Problem war dabei nicht allein die Volkszählung selbst (Kritik: umfangreiche Fragebögen), sondern primär ein zugleich geplanter Abgleich der Volkszählungsdaten mit den Melderegistern.[31] *Steinmüller* führte im Jahr 1983 im *Spiegel* dazu aus: *„Das ist für mich das Hauptproblem* [Anm. Auswertung der Daten durch die Meldebehörden]. *Deutschland hat ja im Gegensatz zu praktisch allen anderen zivilisierten Ländern der Welt eine Einwohnererfassung, die allerdings ursprünglich, bis 1935, nur Zuzug, Wegzug und Aufenthalt betraf; für Zwecke der Wehrerfassung und der Judenvernichtung hat man dann immer mehr Daten für immer mehr Behörden gesammelt, etwa für das Reichssicherheitshauptamt, und seinerzeit auch eine Volkskartei geplant, aber die damalige Hollerith-Technik war dafür nicht geeignet. Das konnten erst die Computer ab 1965. Nach 1945 wurde zunächst das Melderecht auf den Stand von 1935 zurückgeschraubt* (...). *Das Melderechtsrahmengesetz von 1980 sieht die Erfassung von etwa 45 Einwohnerdaten mit Zusatzdaten vor, die die zugrundeliegenden Akten bei den verschiedenen Behörden erschließen. Die durch Bundesrecht vorgesehenen wenigen Daten reichen bereits aus, um alle anderen personenbezogenen Dateien des öffentlichen Bereichs zu erschließen.* (...) *Das Ziel ist* (...) *getrennt liegende Daten über Personen zusammenführen zu können. Allerdings gibt es auf dem Weg zum Personenkennzeichen vorerst noch ein Hindernis. Die Melderegister sind teilweise in desolatem Zustand,*

26 Hessischer Landtag 6. Wahlperiode Drucksache Nr. 3065, 7; Hessischer Landtag 7. Wahlperiode Drucksache Nr. 1495, 10 f; *von Lewinski*, Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive, in Schmidt/Weichert (Hrsg), Datenschutz – Grundlagen, Entwicklungen und Kontroversen (2012) 23 ff (28).

27 *von Lewinski* in Schmidt/Weichert (Hrsg), Datenschutz – Grundlagen, Entwicklungen und Kontroversen (2012) 29.

28 BT-Drs. VI/3826, 85.

29 BVerfG Urteil v. 15.12.1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil).

30 BGBl. 1982 I. 369.

31 *Bundestag.de*, Beschluss des Volkszählungsgesetzes 1983, abrufbar: https://www.bundestag.de/dokumente/textarchiv/2012/38024038_kw10_kalender_volkszaehlung/207898 (zuletzt abgerufen am 20.06.2019).

weil viele Leute sich nicht rechtzeitig oder gar nicht ummelden oder nicht abmelden und so weiter. Das macht sie für Computerzwecke weithin unbrauchbar. Da ist die Volksbefragung die einzige Chance für die Verwaltung, die Melderegister up to date zu bringen. Und nur dann, wenn sie auf diesem Stand sind, ist es möglich, die Meldedaten als Personenkennzeichen-Ersatz zu verwenden (Anm. – die Einführung eines offiziellen bundeseinheitlichen Personenkennzeichens[32] für jeden Bürger in Westdeutschland war in den Jahren 1971[33] und 1973[34] an verfassungsrechtlichen Bedenken des Rechtsausschusses des Deutschen Bundestages gescheitert[35]; spätestens seit Oktober 2008 existiert in Deutschland mit der sogenannten Steueridentifikationsnummer „Steuer-ID" in eingeschränkter Form nun doch ein solches Personenkennzeichen[36]). *Man stelle sich nur vor, daß in diesem demokratischen Staat einmal nachdemokratische Strukturen entstehen. Es ist unverantwortlich, einen so großen Datenbestand für nicht sauber definierte Zwecke vorrätig zu halten – ohne zureichende juristische, technische und politische Sicherung."*[37]

Im Volkszählungsurteil 1983 des BVerfG erfolgte die verfassungsrechtliche Absicherung des Datenschutzrechts durch die Entwicklung des Rechts auf informationelle Selbstbestimmung unmittelbar aus Art 2 Abs 1 GG (freie Entfaltung der Persönlichkeit) iVm. Art 1 Abs 1 GG (Menschenwürde). Die vorgesehenen Übermittlungsregelungen und insbesondere der Melderegisterabgleich der Daten – nach Ansicht *Steinmüllers* zur Verwendung der „*Meldedaten als Personenkennzeichen-Ersatz"*[38] – und die damit verbundene Verknüpfung statistischer mit administrativen Zwecke im Rahmen der Volkszählung 1983 wurden vom BVerfG als verfassungswidrig erklärt. Als vom allgemeinen Persönlichkeitsrecht gemäß

32 **Personenkennzeichen:** Für die Speicherung und Verarbeitung großer Bestände personenbezogener Daten ist eine Kurzadressierung jedes Datensatzes in Form eines eindeutig identifizierbaren Personenkennzeichens eine technische Lösungsmöglichkeit mit der Vielzahl an Namensübereinstimmungen in großen Melderegistern eine Identifizierung der im Einzelfall richtigen Person eindeutig zu erreichen. Die besondere Bedeutung eines Personenkennzeichens für die Datenverarbeitung liegt jedoch in seiner Funktion als Verknüpfungszeichen zum Zweck der Zusammenführung verschiedener Dateiinhalte und Verwaltungsvorgängen. Sind die Grund- und Folgedaten jeweils unter dem gleichen unveränderlichem und unverwechselbarem Personenkennzeichen zugeordnet, lassen sie sich leicht zusammenführen und gleichzeitig verarbeiten bzw. übermitteln. Voraussetzung für ein solches Informationssystem ist ein nach einheitlicher Systematik aufgebautes unveränderliches und unverwechselbares Personenkennzeichen für jeden einzelnen Bürger, vgl. BT-Drs. VI/2654, 8 f; BT-Drs. 7/1059, 10 f.

33 BT-Drs. VI/2654.

34 BT-Drs. 7/1059.

35 BT-Drs. 8/3825, 11.

36 *Schaar*, „Steuer-ID darf kein allgemeines Personenkennzeichen werden!", ZD 2011, 49; *Martini/Wagner/Wenzel*, „Rechtliche Zulässigkeit einer Personenkennziffer", ZD-Aktuell 2017, 04272; *Öchsner* in sueddeutsche.de (08.07.2010), Steuer-Identifikationsnummer – Elf Ziffern, die Angst machen, abrufbar unter: http://www.sueddeutsche.de/geld/steuer-identifikations nummer-elf-ziffern-die-angst-machen-1.971540 (zuletzt abgerufen am 20.06.2019); *Krempl* in heise.de (03.08.2011), Datenschützer bemängelt schleichende Ausweitung der Steuer-ID, abrufbar unter: https://heise.de/-1317621 (zuletzt abgerufen am 20.06.2019).

37 DER SPIEGEL 12/1983, 106 ff, Interview mit Wilhelm Steinmüller, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/14021551 (zuletzt abgerufen am 20.06.2019).

38 DER SPIEGEL 12/1983, 106 ff, Interview mit Wilhelm Steinmüller, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/14021551 (zuletzt abgerufen am 20.06.2019).

Art 2 Abs 1 iVm. Art 1 Abs 1 GG erfasst, wurde vom BVerfG auch die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten angesehen. Jeder Einzelne hat grundsätzlich die Befugnis, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkung sind nur im überwiegenden Allgemeininteresse zulässig, welche einer verfassungsgemäßen gesetzlichen Grundlage bedürfen, die dem rechtsstaatlichem Gebot der Normenklarheit, dem Grundsatz der Verhältnismäßigkeit entsprechen muss sowie organisatorische und verfahrensrechtliche Vorkehrungen treffen muss, um einer Verletzung des Persönlichkeitsrechts entgegen zu wirken.[39]

Aufgrund der umfangreichen wissenschaftlichen Vorarbeiten insbesondere von *Steinmüller*[40], *Podlech*[41] und *Mallmann*[42] lesen sich weite Teile der Urteilsbegründung des Volkszählungsurteils 1983 wie Auszüge aus *Steinmüllers* Gutachten aus 1971 (BT-Drs. VI/3826) bzw. *Podlechs* Kommentierung des Art 2 Abs 1 GG im Alternativkommentar zum GG (AK-GG, 1 Auflage 1984).[43] Gemäß den Erinnerungen von *Steinmüller*, *Podlech* und *Lutterbeck* geschah nämlich Folgendes[44]: Verfassungsrichter Hermann Heußner (langjähriger Vorsitzender der Vereinigung für Rechtsinformatik) hatte als Berichterstatter das Volkszählungsurteil beim BVerfG vorzubereiten und kontaktierte im Rahmen des Verfahrens ab einem gewissen Zeitpunkt Adalbert Podlech (Universitätsprofessor an der TU Darmstadt) telefonisch. Podlech war zu diesem Zeitpunkt nicht am Verfahren beteiligt. BVerfG-Berichterstatter Heußner erklärte nun Podlech, dass es im für die Volkszählungsbeschwerden zuständigen Ersten Senat[45] darauf ankomme, dass das Senatsmitglied Bundesverfassungsrichter Konrad Hesse überzeugt werden müsse, weshalb die Beschwerdeführer – wenn sie erfolgreich sein wollten – dem Verfassungsrichter Konrad Hesse unbedingt eine Konstruktion von Art 2 Abs 1 GG vorlegen müssten, die diesen dann letzt-

39 BVerfG, Urteil v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83; *Podlech* in Bäumlin/Azzola (Hrsg), AK-GG (1984) Art. 2 Abs. 1 Rn 44 ff; Art. 1 Abs. 1 Rn 39 f; *Borchers* in heise.de (15.12.2008), Vor 25 Jahren: Informationelle Selbstbestimmung wird Grundrecht, abrufbar unter: https://www.heise.de/newsticker/meldung/Vor-25-Jahren-Informationelle-Selbstbestimmung-wird-Grundrecht-189834.html (zuletzt abgerufen am 20.06.2019).

40 BT-Drs. VI/3826, 85 ff.

41 *Podlech* in Bäumlin/Azzola (Hrsg), AK-GG (1984) Art. 1 Abs. 1 Rn 39 f; *Podlech* in Bäumlin/Azzola (Hrsg), AK-GG (1984) Art. 2 Abs. 1 Rn 44 ff.

42 *Mallmann*, Datenschutz in Verwaltungs-Informationssystemen: Zur Verhältnismäßigkeit des Austausches von Individualinformationen in der normvollziehenden Verwaltung (1976) 47 ff.

43 *Steinmüller*, RDV 2007/4, 158 ff (160); *Steinmüller/Podlech*, FIfF-Kommunikation 03/2007, 15 ff; BT-Drs. VI/3826, 85 ff; *Podlech* in Bäumlin/Azzola (Hrsg), AK-GG (1984) Art. 1 Abs. 1 Rn 39 f; *Podlech* in Bäumlin/Azzola (Hrsg), AK-GG (1984) Art. 2 Abs. 1 Rn 44 ff.

44 *Steinmüller/Podlech*, FIfF-Kommunikation 03/2007, 15 ff (17 ff); *Steinmüller*, RDV 2007/4, 158 ff (160); *Rost*, Interview mit Prof. Dr. Steinmüller vom März 2009, ab 18:22min bzw. ab 33:30min, abrufbar unter: https://www.maroki.de/pub/video/steinmueller/start_video_steinmueller.html (zuletzt abgerufen am 20.06.2019); *Rost*, Interview mit Prof. DDr. Podlech vom November 2008, ab 21:30min, abrufbar unter: https://www.maroki.de/pub/video/podlech/start_video_podlech.html (zuletzt abgerufen am 20.06.2019); *Rost*, Interview mit Prof. Dr. Lutterbeck vom März 2009, ab 23:00min, abrufbar unter: https://www.maroki.de/pub/video/lutterbeck/start_video_lutterbeck.html (zuletzt abgerufen am 20.06.2019).

45 Ernst Benda, Helmut Simon, Konrad Hesse, Dietrich Katzenstein, Gisela Niemeyer, Hermann Heußner, Johann Friedrich Henschel.

lich überzeugen würde. Er – Podlech – müsse dazu vor Gericht auftreten, um diese Auslegung vorzutragen. Nach diesem Anruf direkt vom BVerfG aus Karlsruhe ließ sich Podlech für das Volkszählungsverfahren von einem der zahlreichen Beschwerdeführer dann schnell beauftragen, stieg in das Verfahren ein und schickte dem BVerfG seine in Druckfahnen vorliegende finale Entwurfsfassung der Kommentierungen zu Art 2 Abs 1 GG für den geplanten „Alternativkommentar zum Grundgesetz“[46] im Schriftsatz mit. Das Problem war jetzt, dass die einzigen beiden vorzeigbaren Argumentationen, die das datenschutzrechtliche Problem der Volkszählung 1983 mit Art 2 Abs 1 GG beschreiben konnten, einerseits das *Steinmüller* Gutachten aus 1971 (BT-Drs. VI/3826), andererseits die in finalen Druckfahnen vorliegende Kommentierung *Podlechs* zu Art 2 Abs 1 GG (kurze Zeit später publiziert im AK-GG, 1 Auflage 1984) waren. Die Mehrzahl der Verfassungsrichter im zuständigen Ersten Senat stimmte inhaltlich der Auslegung iSv. *Steinmüller* und *Podlech* jeweils zu und wollte diese Argumentation in das Urteil übernehmen, sah aber ein Problem in der Zitierung der Quellen. Also wurde Podlech vor der entscheidenden Sitzung des Ersten Senats des BVerfG nochmals direkt aus Karlsruhe angerufen, dass eine Zitierung seiner Arbeiten nicht möglich wäre, ob er damit einverstanden wäre? Podlech stimmte zu. Anschließend folgte in Karlsruhe ein interner Beschluss der Verfassungsrichter, im Urteil keine Quellen zu zitieren, weil alle verwendeten Zitate von Seiten der Beschwerdeführer, also insbesondere von *Steinmüller* oder *Podlech* stammen würden, die darüber hinaus als allgemein „linksverdächtig“ galten. Die Kommentierung von *Podlech* wurde letztlich teilweise sogar wörtlich übernommen, ohne dies als Zitate im Urteil auszuweisen, was aufgrund der Veröffentlichung des AK-GG (1. Auflage 1984) ganz kurz nach der Verkündung des Volkszählungsurteils auch manchen Beobachtern auffiel.[47]

Das Volkszählungsurteil 1983 machte im BDSG 77 Veränderungen erforderlich, welche im BDSG 90 (BGBl. 1990 I. 2954.) mit 01.06.1991 umgesetzt wurden. Die EG-Datenschutzrichtlinie 95/46/EG wurde zum 23.05.2001 im BDSG 2001 (BGBl. 2001 I. 904.) umgesetzt. Im Jahr 2009 erfolgten umfassende Veränderungen (drei Novellen) im BDSG.[48] Im Frühjahr 2017 wurde das BDSG zur Anpassung an die Datenschutz-Grundverordnung (EU) 2016/679 und der Datenschutzrichtlinie (EU) 2016/680 für Polizei und Strafjustiz (DSAnpUG-EU BGBl. 2017 I. 2097) neu gefasst, im Sommer 2019 folgte noch eine Novelle durch das 2. DSAnpUG-EU (BGBl. 2019 I. 1626). Das BDSG regelt gemeinsam mit der DSGVO den Datenschutz für private Stellen und öffentliche Stellen bzw. Behörden der zivilen Politikbereiche (vgl. §§ 1 – 44 BDSG idF. 2. DSAnpUG-EU). Gleichzeitig enthält das BDSG

46 Bäumlin/Azzola (Hrsg), AK-GG (1984).

47 *Steinmüller*, RDV 2007/4, 158 ff (160); *Steinmüller/Podlech*, FIfF-Kommunikation 03/2007, 15 ff (17 ff); *Rost*, Interview mit Prof. Dr. Steinmüller vom März 2009, ab 18:22min bzw. ab 33:30min, abrufbar unter: https://www.maroki.de/pub/video/steinmueller/start_video_steinmueller.html (zuletzt abgerufen am 20.06.2019); *Rost*, Interview mit Prof. DDr. Podlech vom November 2008, ab 21:30min, abrufbar unter: https://www.maroki.de/pub/video/podlech/start_video_podlech.html (zuletzt abgerufen am 20.06.2019); *Rost*, Interview mit Prof. Dr. Lutterbeck vom März 2009, ab 23:00min, abrufbar unter: https://www.maroki.de/pub/video/lutterbeck/start_video_lutterbeck.html (zuletzt abgerufen am 20.06.2019); BVerfG, Urteil v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83; *Podlech* in Bäumlin/Azzola (Hrsg), AK-GG (1984) Art. 2 Abs. 1 Rn 44 ff.

48 BDSG-Novelle I (BGBl. 2009 I. 2254.); BDSG-Novelle II (BGBl. 2009 I. 2814.); BDSG-Novelle III (BGBl. 2009 I. 2384.).

Regelungen für den Datenschutz bei Polizei und Strafverfolgungsbehörden (vgl. §§ 1 – 21, §§ 45 – 84 BDSG).[49] Der militärische Bereich der „nationalen Sicherheit" ist – wie bisher – nicht vom Unionsrecht erfasst (Art 4 Abs 2 Satz 3 EUV iVm. Art 51 EU-GRC; Art 2 Abs 2 lit a DSGVO; Art 2 Abs 3 lit a DSRL-JI) und verbleibt in den nationalen Materiengesetzen (BVerfSchG, BND-G, MAD-G, etc.).

1.1.3 Entwicklung des Datenschutzrechts in Österreich

In Österreich entwickelte sich zeitgleich zu Deutschland eine Diskussion zum Thema Datenschutz, die sehr heftig ausfiel, sodass nach Analyse von *Stadler* das spätere DSG 1978 eines der wenigen Gesetze der Zweiten Republik wäre, das dann fast zur Gänze vom Parlament erarbeitet wurde.[50] In der Regierungsvorlage aus 1975 (72 BlgNR 14. GP) wird unter Bezugnahme auf *Steinmüller* und *Podlech* die Problemstellung im Zusammenhang mit dem Datenschutz erläutert.[51] Die Regierungsvorlage 1975 (72 BlgNR 14. GP) verzichtete jedoch noch auf eine Verfassungsbestimmung zum Schutz der in Datenbanken gespeicherten Daten, mit der Begründung, dass der Schutz des Privatlebens ein ganz allgemeines Problem wäre, welches nicht isoliert hinsichtlich der Datenverarbeitung behandelt werden könnte. Es wurde aber an gleicher Stelle angeregt in das Staatsgrundgesetz 1867 (StGG 1867) einen Artikel 10b einzufügen, welcher den seit 1964 in Verfassungsrang stehenden Art 8 Europäische Menschenrechtskonvention (EMRK) insofern ergänzen sollte.[52]

Die ÖVP (Abgeordnete Dr. Ermacora, Dr. Hauser u.a.) brachte am 31. März 1976 im Nationalrat einen Initiativantrag 21/A für ein Bundesverfassungsgesetz ein, womit allgemeine (verfassungsgesetzliche) Regelungen auf dem Gebiet des Datenschutzes und der Datensicherungen getroffen werden sollten, mit folgender Begründung ein: *„Verschiedene Staaten haben einen Datenschutz ausgearbeitet oder arbeiten an einem solchen* (...) *Und Österreich? Von der Öffentlichkeit nicht registriert wurde, dass jeder Sozialversicherte eine Kennziffer erhalten hat, die elektronisch genützt wird. Einem darauf aufbauenden Vorgang wurde kaum Beachtung geschenkt: Am 28. Mai 1973 berichtete Innenminister Rösch, daß man an der Einführung eines Personenkennzeichens arbeite* (...) *Es soll ein staatliches Personenkennzeichen eingeführt werden, es soll 11-stellig sein, die Sozialversicherungsnummer, unter der 5 Millionen Staatsbürger registriert sind, soll die Basis für die Personenkennziffer sein;* (...). *Aber ein Datenschutz ist noch nicht sichergestellt."*[53] Im Verfassungsausschuss des Parlaments wurde sowohl die Regierungsvorlage von 1975[54] als auch der Initiativantrag 21/A der ÖVP Abgeordneten Dr. Ermacora und Dr. Hauser u.a. aus dem Jahr 1976[55] behandelt. Im Bericht des Verfassungsausschusses von 1978 heißt es

---

49 Vgl. Art 16 AEUV iVm. Art 7 u. 8 EU-GRC iVm Art 2 Abs 1 DSGVO iVm. Art 2 Abs 1 DSRL 2016/680 für Polizei und Strafjustiz iVm. BDSG idF. DSAnpUG-EU.

50 *Stadler*, Das österreichische Datenschutzgesetz als Markstein der Verfassungspolitik und des Informationsrechts, JBl 1979, 358.

51 ErläutRV 72 BlgNR 14. GP 22.

52 ErläutRV 72 BlgNR 14. GP 17 ff.

53 *Dohr/Pollirer/Weiß*, DSG – Datenschutzgesetz (1988) Anh I/3 (Initivativantrag 21/A vom 31. März 1976, 442 BlgNR 14. GP).

54 72 BlgNR 14. GP.

55 *Dohr/Pollirer/Weiß*, DSG – Datenschutzgesetz (1988) Anh I/3 (Initivativantrag 21/A vom 31. März 1976, 442 BlgNR 14. GP).

schließlich: *„Als Ergebnis der Unterausschussberatungen wurde dem Verfassungsausschuss am 5. Oktober 1978 der gegenständliche Gesetzesentwurf vorgelegt, in dem die Bestimmungen über den Datenschutz gegenüber der Regierungsvorlage 72 der Beilagen zur Gänze neu gefasst sind. Insbesondere enthält der Entwurf nunmehr im Sinne des Initiativantrages 21/A verfassungsgesetzliche Bestimmungen über ein Grundrecht auf Datenschutz. Ferner wurde über einem Abschnitt über den Datenschutz im öffentlichen Bereich ein weiterer gleichartig gegliederter Abschnitt über den Datenschutz im privaten Bereich aufgenommen."*[56]

Das österreichische Datenschutzgesetz (DSG 1978) trat am 1. Januar 1980 in Kraft und enthielt in § 1 DSG 1978 ein Grundrecht auf Datenschutz, welches gemäß § 1 Abs 6 DSG 1978 mit unmittelbarer Drittwirkung ausgestattet wurde. Das Grundrecht auf Datenschutz kommt seither in Österreich auch unmittelbar zwischen Privaten zur Anwendung.[57] Im Rahmen der Umsetzung der EG-Datenschutzrichtlinie 95/46/EG wurde das DSG 1978 mit BGBl. I Nr. 165/1999 zum 1. Januar 2000 durch das DSG 2000 ersetzt, welches bis 24. Mai 2018 galt. Die Anpassung an die Datenschutz-Grundverordnung (EU) 2016/679 erfolgte durch BGBl. I Nr. 120/2017 (Datenschutz-Anpassungsgesetz 2018), durch BGBl. I Nr. 24/2018 (Datenschutz-Deregulierungsgesetz 2018) und durch BGBl. I Nr. 14/2019 in Form einer Neufassung der §§ 4 ff DSG. Der Datenschutz für die Polizei und Strafjustiz in Umsetzung der Datenschutzrichtlinie (EU) 2016/680 findet sich in den neugefassten §§ 36 – 61 DSG. Das in § 1 DSG formulierte Grundrecht auf Datenschutz bleibt unverändert in Kraft (vgl. BGBl. I Nr. 120/2017, BGBl. I Nr. 23/2018, BGBl. I Nr. 24/2018, BGBl. I Nr. 14/2019). Der Politikbereich „nationale Sicherheit" ist vom österreichischen DSG erfasst (vgl. §§ 1, 4 Abs 1 iVm. § 36 Abs 1 DSG). Der Verfassungsausschusses des Nationalrates stelllt klar: *„Vom Anwendungsbereich des 3. Hauptstücks sollen etwa auch die nachrichtendienstliche Aufklärung und die Luftraumüberwachung sowie andere Tätigkeiten der Landesverteidigung* (…) *erfasst sein."*[58]

1.1.4 EMRK und Konvention Nr. 108

Auf der Ebene des Europarats sind die beiden wichtigsten verbindlichen und von allen 47 Mitgliedstaaten ratifizierten Dokumente für den Datenschutz Art 8 der Europäischen Menschenrechtskonvention vom 04. November 1950[59] und das Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Konvention Nr. 108).[60] Ein wesentlicher Unterschied zwischen Art 8 EMRK im Vergleich zum primärrechtlichen Datenschutzrecht der Europäischen Union (Art 7, Art 8 EU-GRC) ist, dass Einschränkungen des sachlichen Anwendungsbereichs der EMRK nicht zulässig sind, denn die Vertragsparteien hatten zum Zeitpunkt der Unterzeichnung und Ratifikation die Gelegenheit entsprechende Vorbehalte anzumelden. Art 8 EMRK gelangt somit – mangels solcher Vorbehalte – in allen politischen Sachbereichen (inklusive der nationalen Sicherheit) vollständig zur Anwendung. Die EMRK als Grundrechtekatalog gilt

56 AB 1024 BlgNR 14. GP 1 (Bericht des Verfassungsausschusses).
57 *Dohr/Pollirer/Weiß*, DSG – Datenschutzgesetz (1988) § 1 Anm. 22.
58 AB 1761 BlgNr 25. GP 18 (Bericht des Verfassungsausschusses).
59 Deutschland: BGBl. 1952 II. 685 (Neubek.: BGBl. 2002 II. 1054, 1055); Österreich: BGBl. Nr. 210/1958.
60 Deutschland: BGBl. 1985 II. 539; Österreich: BGBl. Nr. 317/1988.

dabei grundsätzlich nur im Verhältnis zwischen dem Bürger und den Vertragsstaaten, wobei die Grundrechte der EMRK nicht nur als reine Abwehrrechte der Bürger gedeutet werden, sondern die Vertragsstaaten auch positiv zu deren Schutz verpflichtet sind. Im Rahmen der Annahme solcher Schutzpflichten besteht auch eine Pflicht der Gerichte, zivilrechtliche Generalklauseln EMRK-grundrechtskonform zu interpretieren.[61]

Art 8 EMRK schützt u.a. die Privatsphäre und die Vertraulichkeit der Kommunikation und erlaubt (staatliche) Eingriffe in allen Politikbereichen nur, wenn sie gesetzlich vorgesehen sind, in einer demokratischen Gesellschaft notwendig sind und zu den in Art 8 Abs 2 EMRK abschließend genannten Zwecken tatsächlich erforderlich sind (siehe **Kapitel 2.3.3**).[62]

Die Konvention Nr. 108 des Europarats[63] ist die erste internationale Datenschutzregelung mit völkerrechtlichem Charakter. Aus ihr ergeben sich weitgehende Auswirkungen für die Vertragsstaaten in diesem Bereich.[64] Die aktuelle Novelle der Konvention 108 vom Frühjahr 2018 durch das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 223[65]) wurde am 18. Mai 2018 nach sieben Jahren intensiver Verhandlungen vom Ministerkomitee des Europarats angenommen[66] (Stand Juli 2019: 30 Staaten unterzeichnet; 0 Staaten ratifiziert).[67] Die Modernisierung der Konvention Nr. 108 durch das Protokoll Nr. 223 (SEV Nr. 223) zielte u.a. darauf ab, sowohl eine Anpassung an die gesellschaftlichen und technischen Veränderungen sicherzustellen als auch eine Angleichung an die DSGVO (EU) 2016/679 und die DSRL (EU) 2016/680 zu ermöglichen.[68] Die Konvention Nr. 108 entfaltet keine unmittelbare Wirkung für die Bürger der Vertragsstaaten in denen sie ratifiziert wurde. Die Konvention 108 (idF. 1981) hat aber trotzdem eine große Bedeutung, da sie einen – über

61 *Mayer/Kucsko-Stadlmayer/Stöger,* Bundesverfassungsrecht[11] (2015) Rz 1336; *Siemen*, Datenschutz als Europäisches Grundrecht (2006) 201 ff.

62 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2016).

63 Deutschland: BGBl. 1985 II. 539; Österreich: BGBl. Nr. 317/1988.

64 *Burkert,* Die Konvention des Europarates zum Datenschutz, CR 9/1988, 751; *Henke*, Die Datenschutzkonvention des Europarates (1986) 48 ff.

65 *Council of Europe*, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), abrufbar unter: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e (zuletzt abgerufen am 02.07.2019).

66 *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, abrufbar unter: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (zuletzt abgerufen am 20.06.2019).

67 *Council of Europe*, Chart of signatures and ratifications of Treaty, abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (zuletzt abgerufen am 02.07.2019).

68 *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, abrufbar unter: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (zuletzt abgerufen am 20.06.2019).

die 28 EU-Mitliedstaaten hinausgehenden – europäischen "Datenschutzkonsens" der 47 europäischen Mitgliedstaaten des Europarats darstellt.[69] Die Vertragsstaaten sind zu Umsetzungsmaßnahmen verpflichtet.[70] Die Konvention Nr. 108 (idF. 1981) wird vom EGMR im Rahmen der Urteilsfindung mittlerweile als maßgeblicher gemeinsamer europäischer Standard herangezogen.[71] Differenzierter ist die Lage hinsichtlich des Datenschutzübereinkommen-Zusatzprotokolls vom November 2001 (SEV Nr. 181), welches Bestimmungen zu unabhängigen Kontrollstellen und Regelungen zu Datentransfers enthält.[72] Bisher wurde dieses von 36 der 47 Mitgliedstaaten ratifiziert, was allerdings mehr als die Hälfte der Mitgliedstaaten des Europarats darstellt. Der EGMR könnte insofern auch beim Zusatzprotokoll zur Konvention Nr. 108 begründet von einem gemeinsamen europäischen Standard ausgehen.[73]

1.1.5 EG-Datenschutzrichtlinie – Datenschutz-Grundverordnung

Die EG-Datenschutzrichtlinie 95/46/EG hat ihre Grundlage im *Vorschlag der Kommission für eine allgemeine Europäische Datenschutzrichtlinie* aus dem Jahr 1990.[74] Durch eine allgemeine Richtlinie sollte in allen EG-Mitgliedsstaaten für den Bereich des Binnenmarktes (insb. Wirtschaft und Zivilverwaltung) ein gleichwertiges hohes Schutzniveau etabliert werden, mit dem Ziel bestehende Hemmnisse für den Austausch von Daten abzubauen, was für ein Funktionieren des mit 1. Januar 1993 errichteten vollendeten Europäischen Binnenmarktes unerlässlich war. Die Freizügigkeit personenbezogener Daten in der Europäischen Gemeinschaft im wirtschaftlichen Bereich sollte durch die Mitgliedstaaten nicht mehr mit der Begründung auf Datenschutz eingeschränkt werden dürfen.[75] Der Vorschlag für eine allgemeine Datenschutzrichtlinie aus dem Jahr 1990 KOM(90) 314 endg. wurde von der Europäische Kommission in den Dokumenten KOM(92) 422 endg. vom 12. Oktober 1992[76] bzw. KOM(95) 375 endg. vom 18. Juli 1995 mehrfach adaptiert.[77] Erst am 24. Oktober 1995 wurde die EG-Datenschutzrichtlinie 95/46/EG (DSRL) nach fünfjähriger Verhandlungsdauer und letzlich zwei Jahre nach Etablierung des Europäischen Binnenmarktes (1. Januar 1993) vom Europäischen Parlament und vom Rat, gestützt auf die Binnenmarktkompetenz Art 100a EGV[78] (Maastricht) / Art. 95 EGV[79] (Amsterdam) / heute Art 114 AEUV[80] (Lissabon), erlassen. Die DSRL nennt in einem Atemzug den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten mit dem Ziel der Sicherstellung

69 *Burkert,* Die Konvention des Europarates zum Datenschutz, CR 9/1988, 751 (753); *Henke*, Die Datenschutzkonvention des Europarates (1986) 60 f.
70 *Gridl*, Datenschutz in globalen Telekommunikationsystemen (1999) 193.
71 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2016) 174 f.
72 Deutschland BGBl. 2002 II. 1882, 1887, 2004 II. 1093, 1416; Österreich BGBl. III Nr. 91/2008
73 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2016) 175.
74 KOM(90) 314 endg. 10 ff.
75 KOM(90) 314 endg. 6.
76 BT-Drs. 12/8329, 4. (abgedruckt KOM(92) 422 endg.).
77 KOM(95) 375 endg. 2.
78 Vertrag zur Gründung der Europäischen Gemeinschaft.
79 Vertrag von Amsterdam.
80 Vertrag über die Arbeitsweise der Europäischen Union.

eines freien Datenverkehrs in der EU. Folgt man dem Wortlaut des Art 1 Abs 2 DSRL ganz genau, ist nach Ansicht des Europäischen Gesetzgebers der Datenschutz nur solange tolerabel, wie er den freien Datenverkehr nicht gefährdet. Der freie Datenverkehr für den EU-Binnenmarkt wurde konzeptionell jedoch nicht auf Kosten des Datenschutzes, sondern mit seiner Hilfe durch Harmonisierung realisiert.[81] Durch die DSRL sollte das Spannungsverhältnis zwischen einem funktionsfähigem Binnenmarkt und der gleichzeitigen Wahrung des Grundrechteschutzes iZh. mit personenbezogenen Daten sinnvoll aufgelöst werden.[82]

Gleich zu Beginn des europäischen Datenschutzes im Jahr 1990 versuchte die EU-Kommission auch energisch in Politikbereichen eine Harmonisierung des Datenschutzes zu erreichen, wo eigentlich keine Gesetzgebungskompetenz der Europäischen Gemeinschaft (Europäischen Union) damals bestand und bis heute nicht besteht. Dies sollte durch einen „*Entwurf einer Entschließung der im Rat vereinigten Vertreter der Regierungen der EG-Mitgliedstaaten über die Anwendung der Grundsätze der EG-Datenschutzrichtlinie auf den öffentlichen Bereich, der nicht in den Anwendungsbereich des Gemeinschaftsrechts fällt.*“[83] erreicht werden. Die Europäische Kommission führte als Begründung für ihren Entschließungsentwurf aus dem Jahr 1990 an den Rat aus: *„Im Sinne stärkerer Kohärenz wäre es wünschenswert, daß für alle Dateien von Verwaltungen, auch wenn sie nicht unter die allgemeine Richtlinie* [EG-Datenschutzrichtlinie] *fallen, dieselben Schutzprinzipien gelten. Dazu müssten sich die Mitgliedstaaten verpflichten, die erforderlichen Gesetzgebungsverfahren auf einzelstaatlicher Ebene einzuleiten.“*[84] Eine solche Entschließung des Rats – wie von der Kommission bereits 1990 vorgeschlagen und erhofft – existiert bis heute [Oktober 2019], also 29 Jahre später, nicht.[85] Zur eindeutigen Nichtanwendbarkeit des europäischen Datenschutzrechts in den Politikbereichen außerhalb des Unionsrechts erläuterte ErwGr 13 EG-Datenschutzrichtlinie 95/46/EG im Jahr 1995 klarstellend: „*Die* (…) *Tätigkeiten, die die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates oder die Tätigkeiten des Staates im Bereich des Strafrechts betreffen, fallen* (…) *nicht in den Anwendungsbereich des Gemeinschaftsrechts. Die Verarbeitung personenbezogener Daten, die zum Schutz des wirtschaftlichen Wohls des Staates erforderlich ist, fällt nicht unter diese Richtlinie, wenn sie mit Fragen der Sicherheit des Staates zusammenhängt.*“[86]

Durch den Vertrag von Lissabon wurde im Jahr 2009 insofern eine Kompetenzausweitung zugunsten des Europäischen Datenschutzes erreicht, dass zumindest der Datenschutz auch im Bereich der Strafverfolgung und der öffentlichen Sicherheit eine Kompetenz der EU ist. *Vivian Reading* leitete im November 2010 als Vizepräsidentin der EU-Kommission und EU-Kommissarin für das Ressort Justiz, Grundrechte und Bürgerschaft in der Kommission Barroso II (2009–2014)[87], gestützt auf diese erweiterte Kompetenz in Art 16 AEUV, sogleich eine Reform des Datenschutzes ein, welche am 25. Januar 2012 der Öffentlichkeit

81 *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997) C. Einleitung Rn 4; Rn 8.
82 *Ehmann/Helfrich,* EG Datenschutzrichtlinie Kurzkommentar (1999) Einleitung Rn 4.
83 KOM(90) 314 endg. 78.
84 KOM(90) 314 endg. 7.
85 Abfrage Eurlex.eu (01.10.2019).
86 ErwGr 13 EG-Datenschutzrichtlinie 95/46/EG.
87 Homepage Europäische Kommission, Vivian Reading, abrufbar unter: http://ec.europa.eu/archives/commission_2010-2014/reding/ (zuletzt abgerufen am 20.07.2019); Dokumentarfilm unter der Regie von *David Bernet*, „Democracy, im Rausch der Daten“ (2015).

präsentiert wurde.[88] Im Ergebnis gibt es nun die unmittelbar anwendbare Datenschutz-Grundverordnung (EU) 2016/679 für den EU-Binnenmarkt und die Datenschutzrichtlinie (EU) 2016/680 für Polizei und Strafverfolgungsbehörden.[89]

Für den Bereich der „nationalen Sicherheit" (Geheimdienste, Militärs, etc.) besteht im Datenschutz auch nach Inkraftretens der DSGVO weiterhin die ausschließliche und alleinige Kompetenz und Zuständigkeit auf nationaler Ebene bei den EU-Mitgliedstaaten (vgl. Art 4 Abs 2 Satz 3 EUV iVm. Art 51 EU-GRC; ErwGr 16 iVm. Art 2 Abs 2 lit a DSGVO; Art 2 Abs 3 lit a DSRL-JI, Art 1 Abs 3 ePrivacy-RL bzw. Art 2 Abs 2 lit a ePrivacy-VO-E). Einziger existierender gemeinsamer „Europäischer Standard" für Datenverarbeitungen im Bereich der „nationalen Sicherheit" (z.B. strategische TK-Überwachungen durch Geheimdienste von EU-Mitgliedsstaaten) sind die völkerrechtlichen Verträge EMRK und die Datenschutzkonvention (Konvention Nr 108[90]) des Europarats von 1981 inklusive der dazu erlassenen Judikatur des EGMR in Straßburg.[91] Das *Europäische Parlament* führte im Jahr 2001 zur Nichtanwendbarkeit des EU-Datenschutzrechts auf Datenverarbeitungen zu Zwecken der „nationalen Sicherheit" aus: „*Tätigkeiten und Maßnahmen im Dienste der Staatssicherheit* (…) *fallen grundsätzlich nicht in den Regelungsbereich des EG-Vertrages.* (…) *Die Beteiligung eines Mitgliedstaates an einem Abhörsystem im Dienste der Staatssicherheit kann somit nicht im Widerspruch zu Datenschutzrichtlinien der EG stehen.*"[92] Allerdings bezweifelte das *Europäische Parlament* an gleicher Stelle, ob z.B. „Wirtschaftsspionage" durch Nachrichtendienste von EU-Mitgliedstaaten von dieser ausdrücklichen primärrechtlichen Herausnahme des Politikbereichs der „nationalen Sicherheit" vom Unionsrecht (Art 4 Abs 2 Satz 3 EUV iVm. Art 51 EU-GRC) tatsächlich miterfasst sei und stellte dazu fest: „*Würde ein Mitgliedstaat einem Abhörsystem, das u.a. auch Konkurrenzspionage betreibt, Vorschub leisten, indem er die eigenen Nachrichtendienste dafür instrumentalisieren lässt bzw. fremden Nachrichtendiensten eigenes Territorium für diesen Zweck zur Verfügung stellt, läge sehr wohl ein Verstoß gegen* [EU-Recht[93]] *vor. Die Mitgliedstaaten sind nämlich nach* [Art 4 Abs 3 EUV[94]] *zur umfassenden Loyalität verpflichtet, insbesondere zur Unterlassung aller Maßnahmen, die die Verwirklichung der Ziele des Vertrages gefährden würden. Selbst wenn das Abfangen von Telekommunikation nicht zugunsten der heimischen Wirtschaft erfolgt (was übrigens in der Wirkung einer Staatsbeihilfe gleichkäme, und damit gegen* [Art 107 AEUV[95]] *verstieße), sondern zugunsten von*

88 KOM(2010) 609 endg. 2 ff; KOM(2012) 9 endg. 2 ff; KOM(2012) 10 endg. 2 ff.

89 Art 2 Datenschutz-Grundverordnung (EU) 2016/679 (Art 3 EG-Datenschutzrichtlinie 95/46/EG); Art 2 Datenschutzrichtlinie (EU) 2016/680 JI.

90 Deutschland: BGBl. 1985 II. 539; Österreich: BGBl. Nr. 317/1988.

91 *Europäisches Parlament* v 11. Juli 2001, Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 84 ff; *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 174 f.

92 *Europäisches Parlament* v 11. Juli 2001, Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 84 f.

93 Original: EG-Recht.

94 Original: Art 10 EGV.

95 Original: Art. 87 EGV.

Drittstaaten, würde eines solche Tätigkeit in fundamentalem Widerspruch zu dem EG Vertrag zugrunde liegenden Konzept eines Gemeinsamen Marktes stehen, da sie eine Verzerrung des Wettbewerbs bedeuten würde. Ein solches Verhalten würde nach Ansicht der Berichterstatters überdies eine Verletzung der Datenschutzrichtlinie für den Bereich der Telekommunikation[96] *bedeuten, da die Frage der Anwendbarkeit der Richtlinien nach funktionellen Gesichtspunkten und nicht nach organisatorischen gelöst werden muss. Dies ergibt sich nicht nur aus dem Wortlaut der Regelung des Anwendungsbereichs, sondern auch aus dem Sinn des Gesetzes. Benützen Nachrichtendienste ihre Kapazitäten zur Konkurrenzspionage, so erfolgt ihre Tätigkeit nicht im Dienste der Sicherheit oder Strafverfolgung, sondern ist zweckentfremdet und fällt folglich voll in den Anwendungsbereich der Richtlinie. Diese verpflichtet aber die Mitgliedstaaten in ihrem Artikel 5, die Vertraulichkeit der Kommunikation zu sichern, insbesondere das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikation durch andere Personen als die Benutzer zu untersagen. Ausnahmen dürfen nach* [Art 15 ePrivacy-RL 2002/58/EG[97]] *nur dort gemacht werden, wo sie zur Staatssicherheit, Landesverteidigung und Strafverfolgung notwendig sind. Da Wirtschaftsspionage nicht zu Ausnahmen legitimiert, würde in diesem Fall eine Verletzung von Gemeinschaftsrecht vorliegen*."[98]

Die *Art 29 Datenschutzgruppe* bestätigte im Jahr 2014 diese Ansicht des Europäischen Parlaments aus dem Jahr 2001: *„Wie oben erörtert ist der Bereich der nationalen Sicherheit vom Geltungsbereich des Unionsrechts – einschließlich der Charta – ausgenommen. Dagegen sind die Vertragsstaaten der EMRK durch den Wortlaut der Konvention verpflichtet, allen ihrer Hoheitsgewalt unterstehenden Personen bestimmte Rechte und Freiheiten zuzusichern, darunter das Recht auf Achtung des Privatlebens, und die EMRK enthält keine allgemeine Ausnahme für den Bereich der nationalen Sicherheit."*[99]

Art 8 EMRK ist – anders als das EU-Datenschutzrecht und die Art 7 und Art 8 EU-GRC – bei staatlichen Eingriffen in allen Politikbereichen zu beachten (vgl. **Kapitel 2.3.3**).[100]

96 Original: ISDN-Richtlinie 97/66/EG; heute ePrivacy-Richtlinie 2002/58/EG.
97 Original: Artikel 14 ISDN-RL 97/66/EG.
98 *Europäisches Parlament* v 11. Juli 2001, Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 84 f.
99 *Art 29 Datenschutzgruppe* WP 228 (2014) 42.
100 *Art 29 Datenschutzgruppe* WP 228 (2014) 42 f.

2 Verfassungs- und europarechtliche Einordnung

2.1 Datenschutz als Abwehrrecht und gleichzeitig Schutzpflicht des Staates

Nach heutigem Verständnis dienen Grundrechte nicht mehr nur als reine Abwehrrechte gegenüber dem Staat, sondern sie verpflichten den Staat auch zum Schutz des Bürgers durch konkrete staatliche Maßnahmen gegen Eingriffe Dritter (sog. Schutzpflichten des Staates).[101] Adressat der nach hM aus den Grundrechten abgeleiteten Schutzpflichten ist der Staat. Das heißt Grundrechte im heutigen Verständnis sind sowohl Abwehrrechte gegen den Staat als auch konkret adressierte Pflichten an den Staat, seine Bürger zu schützen.[102] Die heutigen Gefahrenquellen im Zusammenhang mit dem Grundrecht auf Datenschutz bzw. dem deutschen Recht auf informationelle Selbstbestimmung sind insbesondere:

- innerstaatliche Behörden;
- (Cyber-)Kriminelle;
- neue Technologien;
- private Dritte (z.B. Arbeitgeber) bzw. globale Konzerne;
- ausländische Staaten (z.B. Auslandsaufklärung).[103]

Der Gesetzgeber hat durch den Erlass von Gesetzen seinen aus den Grundrechten abgeleiteten Schutzpflichten gegenüber den Bürgern nachzukommen. *Di Fabio* sieht in der grundsätzlichen Annahme bzw. Forderung an grundrechtlichen staatlichen Schutzpflichten aber häufig einen gleichzeitigen Eingriff in Rechte Dritter zu Gunsten eines anderen Grundrechtsträgers und fordert insofern eine starke Zurückhaltung bei der Annahme von solchen staatlichen Schutzpflichten unmittelbar aus Grundrechten.[104]

2.2 Bundesrepublik Deutschland

Das Recht auf informationelle Selbstbestimmung (Datenschutzrecht) ist in Deutschland als eine Ausprägung des Allgemeinen Persönlichkeitsrechts seit 1983 vom BVerfG verfassungsrechtlich anerkannt. Das deutsche Allgemeine Persönlichkeitsrecht ist entwicklungsoffen und so konnten Rechtsprechung und Literatur in wechselseitiger Ergänzung in den letzten Jahrzehnten Fallgruppen des Allgemeinen Persönlichkeitsrechts herausbilden.[105]

---

101 *Klein*, Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633.

102 *Di Fabio* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 2 Rn 135-136; *Wiederin* in Merten/Papier/Kucsko-Stadlmayer (Hrsg), Handbuch der Grundrechte Band VII/1 Grundrechte in Österreich[2] (2014) § 10 Rn 127; *Schmitz* in Spindler/Schmitz (Hrsg), TMG[2] (2018) § 11 Rn 20.

103 Definition der Risiken angelehnt an *Friedewald/Quinn/Hansen/Heesen/Hess/Lamla/Matt/Roßnagel/Trepte/Waidner*, White Paper Datenschutz-Folgenabschätzung[3] (2017) 30 f.

104 *Di Fabio* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 2 Rn 61.

105 *Schmidt,* Datenschutz für „Beschäftigte“ (2016) 55.

C. Jaksch, *Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes*,
AutoUni – Schriftenreihe 143, https://doi.org/10.1007/978-3-658-29450-2_2

Das Recht auf informationelle Selbstbestimmung ordnet sich im Verhältnis zu den Grundrechten des GG mit ähnlichen Schutzzielen im verfassungsrechtlichen Kontext[106] wie folgt ein:

2.2.1 Fernmeldegeheimnis (Art 10 Abs 1 GG)

Art 10 Abs 1 GG (Post- und Fernmeldegeheimnis) schützt die unkörperliche Übermittlung von Informationen (Kommunikationsinhalte und Begleitumstände wie Verbindungsdaten[107]) an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs. Das aus Art 2 Abs 1 in Verbindung mit Art 1 Abs 1 GG folgende Recht auf informationelle Selbstbestimmung (Datenschutz) tritt nach Rechtsprechung des BVerfG hinter diese speziellere Gewährleistung des Fernmeldegeheimnisses aus Art 10 GG zurück, soweit die Schutzbereiche beider Grundrechte sich überschneiden.[108] Der Schutzbereich des Art 10 Abs 1 GG (einfachgesetzlich § 88 TKG 2004) erstreckt sich auf den Bereich der Übermittlung; nicht mehr erfasst sind daher die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers unmittelbar gespeicherten Inhalte und Umstände der Telekommunikation, denn es bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Fernmeldegeheimnis abgewehrt werden sollen, insofern nicht mehr fort.[109] Damit endet der Schutz des Fernmeldegeheimnisses in dem Moment, in dem die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang beendet ist, denn ab diesem Zeitpunkt unterscheiden sich die gespeicherten Inhalte und Verbindungsdaten in ihrer Schutzwürdigkeit nicht mehr von Daten, die der Nutzer selbst auf seinem Endgerät bereits gespeichert hat und, die sich damit voll in seinem Herrschaftsbereich befinden. Hier gilt dann das Recht auf informationelle Selbstbestimmung. Etwas anderes gilt für Nachrichten und Daten, die z.B. auf einer Voicebox oder einer Mailbox des Providers zwischengespeichert werden; sie unterfallen noch dem Schutz des Art. 10 Abs 1 GG (§ 88 TKG 2004).[110] Insofern sind bereits gelesene und weiter auf dem Mailserver des Providers gespeicherte eMails noch von Art 10 Abs 1 GG erfasst. Begründet wird dies damit, dass zwar die Nutzer jederzeit ihre eMails löschen oder auf ihren privaten Rechner speichern können und damit die eMails durchaus in ihrem Herrschaftsbereich bereits liegen würden, aber wenn sich die Nutzer für eine weitere Speicherung beim Provider entscheiden, würden sie sich weiterhin in die spezifische Gefährdungslage begeben, die unter dem Schutz des Art 10 Abs 1 GG steht.[111] Hingegen wird eine Nachricht auf dem Anrufbeantworter zu Hause aus den oben genannten Erwägungen nicht mehr von Art 10 Abs 1 GG geschützt.[112]

---

106 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 181 ff.

107 *Ogorek* in Epping/Hillgruber (Hrsg), BeckOK Grundgesetz[41. Edition] (Stand: 15.11.2018) Art 10 Rn 39 f.

108 BVerfG Beschluss v.14.07.1999, Az. 1 BvR 2226/94 Rn 158; BVerfG, Urteil v. 27.07.2005, Az. 1 BvR 668/04 Rn 79.

109 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 182 ff.

110 *Durner* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 10 Rn 82.

111 BVerfG Beschluss v. 16.06.2009, Az. 2 BvR 902/06 Rn 42-54.

112 *Durner* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 10 Rn 82.

Hinsichtlich Cloud Computing gelte es nach *Ogorek* folgendes zu differenzieren:

- Greifen staatliche Stellen auf in einer reinen Online-Speicher-Cloud abgelegte Daten zu (ausschließliche externe Datenspeicherung), liege kein Eingriff in Art 10 GG vor, weil darin kein Eingriff in einen laufenden Kommunikationsvorgang zu erblicken sei.
- Werde die Cloud (auch) zu Kommunikationszwecken eingesetzt inklusive, dass ein Nutzungsberechtigter ein in der Cloud hinterlegtes Dokument einer anderen Person in der Cloud zugänglich macht, handle es sich um einen nach geschützten Kommunikationsvorgang, die Daten der Cloud unterliegen somit Art 10 GG.[113]

Art 10 GG kennt keinen verpflichtenden Richtervorbehalt direkt aus dem GG.[114] Vom deutschen Gesetzgeber kann der – durch Art. 10 GG nicht von vornherein zwingend gebotene – Richtervorbehalt als verfahrensrechtliche Schutzvorkehrung berücksichtigt werden.[115] Im Jahr 2008 adressierte das BVerfG an den Deutschen Bundestag und den Landesgesetzgeber die konkrete verfassungsrechtliche Anforderung: „*Bei einem Grundrechtseingriff von besonders hohem Gewicht* (…) *reduziert sich der Spielraum dahingehend, dass die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen ist. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren* (…).“[116] Art 19 Abs 1 Satz 2 GG normiert ein ausdrückliches Zitiergebot des konkret einzuschränkenden Grundrechts im konkreten Eingriffsgesetz. Das einfachgesetzliche Fernmeldegeheimnis verlangt (§ 88 Abs 3 Satz 3 TKG 2004) zusätzlich, dass ein solches Gesetz sich ausdrücklich auf Telekommunikationsvorgänge beziehen muss.

Der räumliche und sachliche Anwendungsbereich des Art 10 Abs 1 GG wird zusammengefasst nach *Karl/Soiné* aktuell wie folgt praktiziert (vgl. § 6 Abs 1 BND-G[117]):

- „Deutsche natürliche Personen unterfallen stets dem (personalen und sachlichen) Schutzbereich des Fernmeldegeheimnisses. Auf ihren Aufenthaltsort während der Kommunikation (In- oder Ausland) kommt es nicht an.“[118]
- „Ausländische natürliche Personen genießen im Geltungsbereich des Grundgesetzes ebenfalls den Schutz des Art. 10 I GG. (…) Ausländische natürliche Personen mit Aufenthalt im Ausland werden durch Art. 10 I GG grundsätzlich nicht geschützt.“ [119]
- „Juristische Personen des Privatrechts mit Sitz in Deutschland fallen in den Schutzbereich des Art. 10 I GG (…) Bei juristischen Personen, die sich nur durch natürliche Personen mitteilen können, muss deren funktionsbezogene Kommunikation unmittelbar den juristischen Personen zugerechnet werden (sog. Funktionsträgertheorie). Geschützt sind demnach zum Beispiel Telefonate ausländischer Mitarbeiter in ausländischen Niederlassungen inländischer juristischer Unternehmen im Rahmen ihrer Funktion.“[120]

---

113 *Ogorek* in Epping/Hillgruber (Hrsg), BeckOK Grundgesetz[41. Edition] (Stand: 15.11.2018) Art 10 Rn 42 f.
114 *Durner* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 10 Rn 152.
115 *Durner* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 10 Rn 148.
116 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 259.
117 BT-Drs. 18/9041, 22; BT-Drs. 18/9142, 3 Fn. 4.
118 *Karl/Soiné*, Neue Rechtsgrundlagen für die Ausland-Ausland-Fernmeldeaufklärung, NJW 2017, 919 (920).
119 *Karl/Soiné*, NJW 2017, 919 (920).
120 *Karl/Soiné*, NJW 2017, 919 (920).

- „Ob ausländische juristische Personen im Ausland oder ausländische juristische Personen mit Vertretung im Inland dem Schutzbereich des Art. 10 I GG unterfallen, hängt von deren Sitz ab. Nach Auffassung des BVerfG sind juristische Personen mit Sitz in einem EU-Mitgliedstaat ebenso zu behandeln wie inländische juristische Personen. Damit unterliegt der funktionsbezogene Fernmeldeverkehr (Telefonate, E-Mails usw.) natürlicher ausländischer Personen im Inland, die nicht Bürger eines europäischen Staates sein müssen, soweit er unmittelbar ausländischen juristischen Personen der EU zuzurechnen ist, dem Schutzbereich des Art. 10 I GG. Ausländische juristische Personen außerhalb der EU können nicht den Schutz des deutschen Fernmeldegeheimnisses beanspruchen.“[121]

Nach *Papier*, *Durner* und *Ogorek* gehe der Schutzbereich des Art 10 Abs 1 GG jedoch viel weiter als diese oben zitierte und aktuell praktizierte Aufassung (vgl. § 6 Abs 1 BND-G) zu Art 10 Abs 1 GG.[122]

Bestimmungen zur Telekommunikationsüberwachung finden sich u.a. in den § 100a StPO, in § 23a Zollfahndungsdienstgesetz, im Artikel 10-Gesetz, in § 6 BND-G („Auslandsaufklärung im Inland“)[123] und in den jeweiligen Polizeigesetzen der Länder.

Der deutsche Gesetzgeber ist der staatlichen Schutzpflicht durch die Schaffung äußerst strenger strafrechtlicher Bestimmungen zum Schutz des Fernmeldegeheimnisses (§ 206 StGB), des gesprochenen Wortes gegen Abhören und Aufzeichnen (§ 201 StGB) und dem Schutz von nicht-öffentlichen Datenübertragung (§ 202b StGB) nachgekommen. Art 10 Abs 1 GG begründet nach hA neben dem Abwehrrecht zugleich einen Auftrag an den deutschen Staat, Schutz auch insoweit vorzusehen, als private Dritte sich rechtswidrig Zugriff auf die Kommunikation verschaffen.[124]

2.2.2 Unverletzlichkeit der Wohnung (Art 13 Abs 1 GG)

Art 13 Abs 1 GG gewährleistet die Garantie der Unverletzlichkeit der Wohnung inklusive Betriebs- und Geschäftsräume (klarer Richtervorbehalt für Eingriffe). Der Grundrechtsschutz erschöpft sich dabei nicht nur in der Abwehr eines körperlichen Eindringens in die Wohnung, sondern auch Maßnahmen, die es ermöglichen, Einblick in Vorgänge innerhalb der Wohnung bzw. des Betriebs- und Geschäftsraumes zu verschaffen, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind (z.B. Messung elektromagnetischer Abstrahlungen zur Überwachung eines – z.B. „offline“ arbeitenden – informationstechnischen Systems in einer Wohnung bzw. Betriebs- und Geschäftsraums; oder das Eindringen in eine Wohnung um ein dort befindliches informationstechnisches System physisch zu manipulieren, womit bestimmte Vorgänge innerhalb der Wohnung überwacht werden können).[125]

---

121 *Karl/Soiné*, NJW 2017, 919 (920); ähnlich: BT-Drs. 18/9041, 22; BT-Drs. 18/9142, 3 Fn. 4.

122 *Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, 1 ff; *Durner* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 10 Rn 64 f; *Ogorek* in Epping/Hillgruber (Hrsg), BeckOK Grundgesetz[41. Edition] (Stand: 15.11.2018) Art 10 Rn 47 f.

123 BT-Drs. 18/9041, 22 f. (Erläuterung zu § 6 BND-G).

124 *Durner* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 10 Rn 112.

125 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 192 ff.

Bestimmungen zur Hausdurchsuchung finden sich in den §§ 102 ff StPO bzw. für die Online-Durchsuchung in § 100b StPO und für die akkustische Wohnraumüberwachung in § 100c StPO und unterliegen dem Richtervorbehalt (§§ 100e, 105 StPO).

Der Gesetzgeber ist der staatlichen Schutzpflicht durch die Schaffung strafrechtlicher Bestimmungen nachgekommen[126]: § 123 StGB (Hausfriedensbruch), § 303 StGB (Sachbeschädigung), § 201 StGB (Verletzung der Vertraulichkeit des Wortes), § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen), § 202a StGB (Ausspähen von Daten), § 202b (Abfangen von Daten aus einer elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage), § 23 GeschGehG (Geschäfts- und Betriebsgeheimnisse) sowie § 42 BDSG (Strafbestimmung bei Datenschutzverletzungen).

2.2.3 Allgemeines Persönlichkeitsrecht (Art 2 Abs 1 iVm. Art 1 Abs 1 GG)

Art 2 Abs 1 iVm. Art 1 Abs 1 GG gewährleisten den Schutz des Allgemeinen Persönlichkeitsrechts in jeweils unterschiedlicher entwickelter Ausprägung. Dies umfasst:

Recht auf Gewährleistung des Schutzes der Privatsphäre

Der Schutz der Privatsphäre gewährleistet jedem Einzelnen einen räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll. Ob aber ein Bereich bzw. eine Information überhaupt der Privatsphäre zugeordnet werden kann, hängt vom jeweiligen Kontext ab, der im Einzelfall schwer zu bestimmen ist.[127]

Diese Thematik der Relativität der Privatsphäre wurde bereits von *Steinmüller*[128] im Gutachten für das BMI aus dem Jahr 1971, sowie auch von *Podlech*[129] und *Mallmann*[130] umfangreich diskutiert, weshalb man bei der Entwicklung des Rechts auf informationelle Selbstbestimmung von Anbeginn vom Schutz der Privatsphäre Abstand nahm, sondern einem rein formellen Ansatz – nämlich auf Informationen abzustellen – folgte, was letztlich zur Entwicklung des Rechts auf informationelle Selbstbestimmung in seiner heutigen Form und dem reinen Abstellen auf personenbezogene Daten führte.[131]

Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung als Ausprägung des Schutzes des allgemeinen Persönlichkeitsrechts geht über die Gewährleistung des Schutzes der Privatsphäre weit hinaus. Beim Recht auf informationelle Selbstbestimmung wird hinsichtlich seiner Anwendbarkeit ausschließlich auf das Vorliegen von personenbezogenen Daten (persönlichen

126 *Papier* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 13 Rn 8.
127 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 197.
128 BT-Drs. VI/3826, 48 ff.
129 *Podlech* in Bäumlin/Azzola (Hrsg), AK-GG (1984) Art. 1 Abs. 1 Rn 39 f; *Podlech* in Bäumlin/Azzola (Hrsg), AK-GG (1984) Art. 2 Abs. 1 Rn 44 ff.
130 *Mallmann*, Datenschutz in Verwaltungs-Informationssystemen: Zur Verhältnismässigkeit des Austausches von Individualinformationen in der normvollziehenden Verwaltung (1976), 47 ff.
131 So führt *Steinmüller* im Jahr 1971 aus: *„Der Begriff der Privatheit ist für das [Datenschutzrecht] ungeeignet. Vielmehr ist an den Begriff der Information anzuknüpfen: Gegenstand des [Datenschutzes] sind nur Individualinformationen (einschl. der gruppenbezogenen Informationen). Sie sind in der Realität jeweils eindeutig bestimmbar.“*, BT-Drs. VI/3826, 57.

Daten) abgestellt. Jeder Einzelne hat direkt aus Art 2 Abs 1 iVm. Art 1 Abs 1 GG die grundsätzliche Befugnis, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Eine Einwilligung iSv. Selbstbestimmung der betroffenen Person ist nur dann nicht erforderlich, wenn eine verfassungsgemäße gesetzlichen Grundlage existiert (datenschutzrechtliche Erlaubnisnorm), die dem rechtsstaatlichen Gebot der Normenklarheit entspricht und zudem vom deutschen Gesetzgeber beim Erlass der Norm der Grundsatz der Verhältnismäßigkeit beachtet wurde, inklusive organisatorischer und verfahrensrechtlicher Vorkehrungen zum Schutz vor Verletzungen des Persönlichkeitsrechts von Betroffenen.[132] Nach *v. Lewinski* kommen daher nur Gesetze im formellen Sinn als Erlaubnistatbestände für eine Datenverarbeitung in Betracht.[133] Nach *Gersdorf* kann auch untergesetzliches Recht (z.B. Rechtsverordnungen) eine Datenverarbeitung legitimieren (materielles Gesetz), vorausgesetzt es werden dort nur Verfahrensmodalitäten oder technische Regelungen von untergeordneter Bedeutung geregelt, die das formelle Gesetz näher ausführen.[134]

Das Recht auf informationelle Selbstbestimmung schützt auch juristische Personen im Rahmen ihrer wirtschaftlichen Tätigkeit.[135]

Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht")

Das „IT-Grundrecht" als aktuellste Ausprägung des Schutzes des allgemeinen Persönlichkeitsrechts greift ein, wenn andere Grundrechte keinen hinreichenden Schutz mehr gewähren können („lückenfüllende Funktion"). Es zielt auf heimliche Online Durchsuchung mittels Schadsoftware „Bundestrojaner" ab, denn eine Online Durchsuchung mittels Schadsoftware geht nach BVerfG weit über die bisherigen Risiken der klassischen „Telekommunikationsüberwachung" hinaus (es ermöglicht das Ausspähen von sämtlichen Daten am Endgerät, also auch solche, die keinen Bezug zur telekommunikativen Nutzung aufweisen wie bspw. das Verhalten bei der Bedienung des IT-Systems, Abrufhäufigkeit von Inhalten, Inhalte von am Endgerät abgelegter Daten, die nie versendet werden sollten, oder bspw. bei Infiltration eines Smart Homes, wird es möglich das gesamte Verhalten in der eigenen Wohnung sichtbar zu machen). Art 10 Abs 1 GG (Fernmeldegeheimnis) bietet hier keinen Schutz, weil es sich um keine „Daten am Übertragungsweg" handelt. Art 13 Abs 1 GG (Unverletzlichkeit der Wohnung) kann ebenso keinen effektiven Schutz gewähren, da der Eingriff auf das IT-System unabhängig vom Standort erfolgen kann, vielfach teilweise auch nicht bekannt ist, wo das IT-System sich konkret befindet, womit ein raumbezogener Schutz insofern nicht greift. Das Grundrecht auf informationelle Selbstbestimmung (klare verhältnismäßige gesetzliche Erlaubnisnorm) bietet in einem solchen Fall ebenso keinen ausreichenden Schutz. Denn ein allein auf eine Erlaubnisbestimmung gestützter heimlicher

132 BVerfG Urteil v. 15.12.1983, Az. 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83; BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 198 f.

133 *v. Lewinski* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer BDSG [aF][4] (2014) Einleitung Rn 53.

134 *Gersdorf* in Gersdorf/Paal (Hrsg), BeckOK Informations- und Medienrecht[24.Edition] (Stand: 01.05.2019) Art 2 GG Rn. 71.

135 zuletzt: BVerfG Beschluss v. 27.06.2018, Az. 2 BvR 1405/17 Rn. 61.

Zugriff auf das IT-System (z.B. Bundestrojaner[136]) ermöglicht es einen umfassenden Einblick in wesentliche Teile der Lebensgestaltung eines Betroffenen zu gewinnen und damit ein aussagekräftiges Bild der Persönlichkeit zu erhalten (Online-Durchsuchung von Personal Computer, Laptops oder Smartphones).[137] Es müssen nach einer heimlichen Online-Durchsuchung eines IT-Systems eines Betroffenen aufgrund der Ergiebigkeit der abgegriffenen Informationen in der Regel keine weiteren Daten mehr über einen Betroffenen erhoben werden. Als Beispiel für eine Abgrenzung zwischen dem Grundrecht auf informationelle Selbstbestimmung und dem IT-Grundrecht führt das BVerfG den Datenzugriff auf eine klassische nicht-vernetzte elektronische Steuerungsanlage der Haustechnik an, wo nur Daten mit punktuellem Bezug auf einen bestimmten Lebensbereich eines Betroffenen enthalten sind, also der *Recht auf informationelle Selbstbestimmung* (klare verhältnismäßige gesetzliche Erlaubnisnorm) hinsichtlich der gesamten Datenermittlung über den Betroffenen insofern ausreichend Schutz bietet. Beim heimlichen Online-Zugriff auf ein vernetztes IT-System ist dies nicht mehr der Fall, weil über den heimlichen Online-Zugriff zugleich alle Daten über eine Person ausgespäht werden können.[138] Folglich stellte das BVerfG heimliche Eingriffe dieser Art wie Online-Durchsuchungen via staatlicher Schadsoftware „Bundestrojaner" unter einem verpflichtenden Richtervorbehalt.[139]

Bestimmungen zum staatlichen Einsatz der Schadsoftware „Bundestrojaner" mit Richervorbehalt finden sich u.a. in §§ 100a und 100b StPO, § 49 BKAG, Art 45 Bay PAG, § 31c POG RP, etc.[140] Eine eigene Rechtsgrundlage für Online-Durchsuchungen durch den Bundesverfassungsschutz ist in Vorbereitung.[141] Die deutsche Auslandsaufklärung stützt Online Durchsuchungen und Quellen-TKÜs nach Angaben der *Deutschen Bundesregierung* direkt auf § 1 Abs 2 BND-G ohne Richtervorbehalt (Stand: März 2018).[142]

Der deutsche Gesetzgeber ist nach *Di Fabio* der staatlichen Schutzpflicht zum Schutz des Allgemeinen Persönlichkeitsrechts aus Art 2 Abs 1 iVm. Art 1 Abs 1 GG in seiner unterschiedlichen Ausprägung insbesondere durch die Schaffung strafrechtlicher und zivilrechtlicher Bestimmungen nachgekommen.[143] Schutz besteht durch die strafrechtlichen § 42 BDSG (Strafbestimmung bei Datenschutzverletzungen), § 202a StGB (Ausspähen von Daten), § 303a StGB (Datenveränderung), § 303b StGB (Computersabotage), § 201 StGB (Verletzung der Vertraulichkeit des Wortes) und § 23 GeschGehG (Geschäftsgeheimnisse) sowie Ordnungswidrigkeitsrecht (Art 83 DSGVO, § 43 BDSG) und zivilrechtlichen Schadenersatz (Art 82 DSGVO iVm. § 44 BDSG; § 823 Abs 1 BGB).

---

136 *Grunert* in faz.net (22.06.2017), Bundestrojaner: Durch die Hintertür zur Online-Überwachung; abrufbar unter: https://www.faz.net/aktuell/politik/online-durchsuchung-quellen-tkue-bundestrojaner-wird-gesetz-15071053.html (zuletzt abgerufen am 20.06.2019).

137 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 201 ff.

138 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 185 ff; Rn 201 ff.

139 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 192 ff.

140 *Soiné*, Die strafprozessuale Online-Durchsuchung, NStZ 2018, 497.

141 *dpa* in heise.de (15.03.2019), Bundesverfassungsschutz soll Befugnis für Online-Durchsuchungen erhalten, abrufbar unter: https://www.heise.de/newsticker/meldung/Bundesverfassungsschutz-soll-Befugnis-fuer-Online-Durchsuchungen-erhalten-4336985.html (zuletzt abgerufen am 20.06.2019).

142 BT-Drs. 19/1434, 15 (Antwort auf Frage 45).

143 *Di Fabio* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 2 Rn 61; Rn 135 f.

2.2.4 Verhältnis GG mit Art 7 und Art 8 EU-GRC und Art 8 EMRK

Zu beachten ist, dass im Anwendungsbereich des EU-Rechts (EU-Vertrag, AEUV, EU-GRC) die aus dem GG im oben beschriebenen Zusammenhang gewährleisteten Grundrechte (Art. 10 Abs 1, Art 13 Abs 1 und Art 2 Abs 1 iVm. Art 1 Abs 1 GG) und deren Auslegung durch den BVerfG durch die Grundrechte der Charta der Grundrechte der Europäischen Union (EU-GRC), insbesondere Art 7 EU-GRC (Achtung Privat- und Familienlebens, Kommunikation) und Art 8 EU-GRC (Schutz personenbezogener Daten) ergänzt bzw. insofern verdrängt[144] werden (**Details zu Art 7 – Art 8 EU-GRC siehe Kapitel 2.3.3** und **Kapitel 2.3.4**). Aus Datenschutzperspektive wird dies folgendes in Zukunft für die Rechtsanwendung in Deutschland bedeuten:

- für die (zivile) öffentliche Verwaltung, welche umfassend den Art 7 und Art 8 EU-GRC sowie der DSGVO (EU) 2016/679 unterliegt, ergänzen bzw. verdrängen[145] die europäischen Grundrechte gemäß EU-GRC sowie sekundärrechtlich die DSGVO (EU) 2016/679 mit Anwendungsvorrang das deutsche GG und die Judikatur des BVerfG.
- für staatliche Behörden, welche zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, tätig sind und personenbezogene Daten verarbeiten (z.B. Polizei, StA), gilt ebenso vorrangig Art 7 und Art 8 EU-GRC. Das deutsche GG und die Judikatur des BVerfG werden durch die EuGH Rechtsprechung insofern ergänzt bzw. verdrängt.[146]
- für Militärs und Nachrichtendienste sind weiterhin nur die durch das GG gewährleisteten Grundrechte und ihre Auslegung durch das BVerfG allein maßgeblich. Gemäß Art 4 Abs 2 Satz 3 EU-Vertrag iVm. Art 51 EU-GRC erfolgt im Bereich der „nationalen Sicherheit" keine Anwendung des Unionsrechts, es gilt ausschließlich deutsches Recht.

Das BVerfG verlangt für Eingriffe in das Recht auf informationelle Selbstbestimmung grundsätzlich ein Gesetz im formellen Sinn[147], nach *Gersdorf* können jedoch auch untergesetzliche Rechtssätze (Rechtsverordnung, etc.) in Betracht kommen, soweit sie – ein formelles Gesetz konkretisierend – nur Verfahrensmodalitäten oder technische Regelungen von untergeordneter Bedeutung regeln.[148] Der EuGH lässt für „gesetzliche" Eingriffe in das Privatleben und den Datenschutz (Art 7 und Art 8 EU-GRC) auch ein Gesetz im materiellen Sinn zu (z.B. Durchführungsverordnungen der EU Kommission ohne Beteiligung des EU-Parlaments).[149] Insofern scheint es aktuell so, dass das deutsche Recht auf informationelle Selbstbestimmung (Art 2 Abs 1 iVm. Art 1 Abs 1 GG) strengere Garantien vorsieht als die unionsrechtlichen Grundrechte Art 7 und Art 8 EU-GRC.

---

144 EuGH Rs. 6/64, Slg. 1964, S. 1251, 1269 – Costa/ENEL.
145 EuGH Rs. 6/64, Slg. 1964, S. 1251, 1269 – Costa/ENEL.
146 EuGH Rs. 6/64, Slg. 1964, S. 1251, 1269 – Costa/ENEL.
147 BVerfG Urteil v. 15.12.1983, Az. 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83; *v. Lewinski* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer BDSG [aF][4] (2014) Einleitung Rn 53.
148 *Gersdorf* in Gersdorf/Paal (Hrsg), BeckOK Informations- und Medienrecht[24.Edition] (Stand: 01.05.2019) Art 2 Rn. 71.
149 EuGH Urteil v. 09. 11. 2010, C-92/09, C-93/09 („Schecke") Rn 56 ff; *Jarass* in Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016) Art 52 Rn. 23 ff.

In allen Politikbereichen ist in Deutschland zusätzlich die Europäische Menschenrechtskonvention EMRK als völkerrechtlicher Vertrag zu beachten. Sie steht in Deutschland (nur) im Rang eines einfachen Gesetzes (BGBl. 2002 II. 1054.). Die EMRK ist im Vergleich mit bundesgesetzlichen gleichartigen Regelungen dem „lex posterior"-Grundsatz unterworfen und müsste daher in speziellen Fällen hinter neueren gesetzlichen Regelungen zurücktreten. Das BVerfG verlangt aber, dass andere gesetzliche Bestimmungen entsprechend EMRK konform auszulegen seien, denn der EMRK komme im deutschen Recht zwar kein verfassungsrechtlicher, aber dennoch ein gewisser übergesetzlicher Rang zu. Insofern geht das BVerfG von einer weitgehenden, aber nicht absoluten Bindung deutscher Gerichte an die Entscheidungen des EGMR aus. Deutsche Gerichte sind verpflichtet sich mit der einschlägigen EGMR-Judikatur zu beschäftigen und sie trifft eine besondere Begründungslast, wenn sie von der Judikatur des EGMR abweichen wollen.[150]

Da insbesondere Art 7 iVm. Art 52 Abs 3 EU-GRC weitgehend Art 8 EMRK entspricht, der EuGH die EMRK aber nur als reine Rechtserkenntnisquelle und nicht als Rechtsquelle betrachtet, sind nach *Kingreen* Rechtsprechungsdivergenzen zwischen EuGH und EGMR denkbar, *„aber nicht sonderlich wahrscheinlich"*[151]. Über Individualbeschwerden aus den jeweiligen EMRK-Mitgliedstaaten (zugleich EU-Mitgliedsstaaten) – gestützt auf eine europarechtskonforme Anwendung des nationalen Rechts – erfolgt letztlich die dbzgl. finale Überprüfung des Unionsrechts anhand von Art 8 EMRK durch den EGMR in Straßburg.[152] Eine Einheitlichkeit der EuGH und EGMR Rechtsprechung wäre folglich sinnvoll.

2.3 Österreich

Das aktuell in Österreich in Kraft stehende Grundrechtesystem beruht auf einem Konglomerat von verfassungsrechtlich gewährleisteten Rechten aus verschiedenen Epochen (19. Jhdt, 20. Jhdt und 21. Jhdt). Im hier relevanten Fokus stehen das Staatsgrundgesetz v. 21.12.1867 über die allgemeinen Rechte der Staatsbürger für die im Reichsrate vertretenen Königreiche und Länder (StGG 1867, RGBl. 1867/142 idF. BGBl. 1988/684.), das Gesetz v. 27.10.1862 zum Schutze des Hausrechts (HausrechtsG 1862, RGBl. 1862/88 idF. BGBl. 1974/422.), die seit dem Jahr 1964 gemäß Art 2 Z 7 Bundesverfassungsgesetz BGBl. 59/1964 als österreichischer Grundrechtekatalog im Verfassungsrang stehende Europäische Menschenrechtskonvention (EMRK, BGBl. 1958/210.) und die seit dem Jahr 2009 als EU-Primärrecht unmittelbar geltende Europäische Grundrechte Charta (EU-GRC) als zentraler Grundrechtekatalog der EU, deren Rechte ebenso bereits vom VfGH als auch in Österreich

150 *Eschelbach* in Widmaier/Müller/Schlothauer (Hrsg), Münchner Anwaltshandbuch Strafverteidigung[2] (2014) § 31 Beschwerde zum EGMR Rn 1 ff.

151 *Kingreen* in Calliess/Ruffert (Hrsg), EUV/AEUV[5] (2016) Art 6 EU-Vertrag Rn 23.

152 *Kingreen* in Calliess/Ruffert (Hrsg), EUV/AEUV[5] (2016) Art 6 EU-Vertrag Rn 23; *Kingreen* in Calliess/Ruffert (Hrsg), EUV/AEUV[5] (2016) Art 52 EU-GRCharta Rn 33; *Jarass* in Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016) Art 7 Rn 6; Rn 1 f; *Chadoian*, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung (2015) 80 f; *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1347.

„verfassungsgesetzlich gewährleistete Rechte“ mit entsprechender selbstständiger Justiziabilität anerkannt wurden.[153] Die höchstgerichtliche Rechtsprechung zum Grundrechteschutz stellt sich in Österreich insofern als ein kompliziertes Gefüge verschiedener Grundrechte und ein Ineinandergreifen von Entscheidungen von fünf Höchstgerichten (EGMR, EuGH, VfGH, VwGH und OGH) dar.[154] In Österreich sind die Grundrechte primär als Abwehrrechte ausgestaltet, aus der im Verfassungsrang stehenden EMRK – und nach *Wiederin* auch aus dem StGG 1867 – ergeben sich aber zugleich staatlichen Schutzpflichten.[155]

Das Grundrecht auf Datenschutz (§ 1 DSG [2000]; Art 8 EU-GRC) ordnet sich auf verfassungsrechtlicher und europarechtlicher Ebene im Verhältnis zu anderer Grundrechten mit ähnlicher Schutzausrichtung demgemäß wie folgt ein:

2.3.1 Fernmeldegeheimnis (Art 10a StGG 1867), Recht auf Achtung der Korrespondenz (Art 8 EMRK); Recht auf Achtung der Kommunikation (Art 7 EU-GRC)

Das Fernmeldegeheimnis wird in Österreich durch zwei verfassungsrechtlich gewährleistete Grundrechte, nämlich Art 10a StGG 1867 (Fernmeldegeheimnis) und Art 8 Abs 1 EMRK (Recht auf Achtung der Korrespondenz), sowie dem primärrechtlichem Art 7 EU-GRC (Recht auf Achtung der Kommunikation) umfassend garantiert. Art 10a StGG 1867 und Art 8 Abs 1 EMRK bzw. Art 7 EU-GRC haben jedoch jeweils einen unterschiedlichen Anwendungsbereich und stellen unterschiedliche verfassungsrechtliche Anforderungen an den Gesetzgeber und die Vollziehung.

Gemäß Art 10a StGG 1867 darf ein Eingriff in das Fernmeldegeheimnis nur aufgrund eines formellen Gesetzes und eines darauf ergangenen richterlichen Befehls erfolgen (Richtervorbehalt).[156] Telekommunikation wird als technischer Vorgang des Aussendens, Übermittelns, Empfangens von Nachrichten jeder Art in der Form von Zeichen, Sprache, Bildern, Töne mittels dazu dienender technischer Einrichtungen verstanden.[157] Mit den Erkenntnissen des VfGH in den Jahren 2012[158] und 2017[159] sowie der Entscheidung des VwGH im Jahr 2013[160] wurde der Schutzbereich des österreichischen Fernmeldegeheimnisses (Art 10a StGG 1867) umfassend präzisiert. Seit dem Jahr 2012 (bestätigt 2017) sind vom

153 VfGH 14.03.2012, U 466/11 = VfSlg 19.632/2012; *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1317; Rn 1347.

154 *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1347.

155 *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017) Art 1 Rn 8; Art 8 Rn 2; *Mayer/Kucsko-Stadlmayer/Stöger,* Bundesverfassungsrecht[11] (2015) Rn 1333; *Wiederin* in Merten/Papier/Kucsko-Stadlmayer (Hrsg), Handbuch der Grundrechte in Deutschland und Europa, Band VII/1 Grundrechte in Österreich[2] (2014) § 10 Rn 127; *Siemen*, Datenschutz als Europäisches Grundrecht (2006) 177 f; *Di Fabio* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 2 Rn 61; Rn 135 f.

156 Vgl. Art 10a StGG 1867 iVm. §§ 135 Abs 3 iVm. § 137 Abs 1 Satz 2 StPO.

157 *Fabrizy*, StGB[13] (2018) § 119 Rn 2.

158 VfGH 29.06.2012, B 1031/11 = VfSlg. 19.657.

159 VfGH 29.11.2017, G 223/2016.

160 VwGH 24.04.2013, 2011/17/0293 = VwSlg 18612 A/2013.

Schutzbereich des Art 10a StGG 1867 und damit vom verfassungsrechtlich vorgeschriebenen Richtervorbehalt bei Eingriffen in das Fernmeldegeheimnis nur noch Inhaltsdaten erfasst, also die konkreten Inhalte übertragener Nachrichten (§ 92 Abs 1 Z 5 TKG 2003). Vom einfachgesetzlichem Kommunikationsgeheimnis in § 93 Abs 1 TKG 2003 sind sowohl Inhalts- als auch Verkehrsdaten erfasst. Unter dem Inhalt von Nachrichten ist die „Übermittlung von Gedankeninhalten“[161] zu verstehen. Bei Verkehrsdaten im Sinne des § 92 Abs 1 Z 4 TKG 2003 handelt es sich – anders als bei Inhaltsdaten – nur um die äußeren Verbindungsdaten, welche zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs entstehen und verarbeitet werden. Solche äußeren Verbindungsdaten (Verkehrsdaten) sind seit dem Jahr 2012 nicht (mehr[162]) vom Schutz des Grundrechts Art 10a StGG 1867 erfasst, sondern nur noch einfachgesetzlich durch § 93 Abs 1 TKG 2003 geschützt.[163] Ganz anders der deutsche Art 10 GG, der sowohl Inhalts- als auch Verkehrsdaten von seinem grundrechtlichen Schutzbereich erfasst[164], dafür aber nicht wörtlich den strengen Richtervorbehalt für jeden einzelnen Eingriff in das deutsche Fernmeldegeheimnis gemäß Art 10 GG kennt[165] wie das dbzgl. österreichische Pendant Art 10a StGG 1867. In Deutschland verlangt das BVerfG seit 2008 einen Richtervorbehalt bei *„einem Grundrechtseingriff von besonders hohem Gewicht“*.[166]

Hinsichtlich der der Frage, ob nach Abschluss des Übertragungsvorgangs weiter beim Provider gespeicherte „Inhaltsdaten“ iSd. der VfGH und VwGH Judikatur[167] (z.B. eMail-Postfach beim Provider mit dort weiter gespeicherten aber bereits „empfangenen“ und „gelesenen“ eMails des Nutzers) doch noch dem Schutz des Fernmeldegeheimnisses nach Art 10a StGG 1867 unterliegen sollten und damit ein solcher Zugriff auch auf bereits übertragene und empfangene Nachrichten weiter dem Richtervorbehalt unterliegen sollte, verlangt *Chadoian* eine entsprechende Anwendung des österreichischen Art 10a Abs 1 StGG 1867 wie in Deutschland Art 10 Abs 1 GG gemäß BVerfG Judikatur.[168] Als Begründung führt *Chadoian* an, dass der Zweck der österreichischen Grundrechtsbestimmung Art 10a StGG 1867

161 *Fabrizy*, StGB[13] (2018) § 119 Rn 3.

162 zuvor sehr wohl: vgl. VwGH 27.05.2009, 2007/05/0280; OGH 17.06.1998, 13 Os 68/98; OGH 01.10.2002, 11 Os 64/02; OGH 13.04.2011, 15 Os 172/10y = EvBl 2011/62 S 419 – EvBl 2011,419 = jusIT 2011/44 S 93 (Karel) – jusIT 2011,93 (Karel) = MR 2011,153 (Hasberger) = Jus-Extra OGH-St 4538 = Jus-Extra OGH-St 4552 = Jus-Extra OGH-St 4553 = RdW 2011/316 S 317 (Info aktuell) – RdW 2011,317 (Info aktuell) = Rn 2011/23 S 252 – Rn 2011,252 = JBl 2011,726 (Reindl-Krauskopf) = Rn 2011,223 EÜ190 – Rn 2011 EÜ190 – ÖBB-Online-Tickets – Stammdatenauskunft.

163 VfGH 29.06.2012, B 1031/11 = VfSlg. 19.657; VfGH 29.11.2017, G 223/2016; VwGH 24.04.2013, 2011/17/0293 = VwSlg 18612 A/2013.

164 BVerfG Beschluss v. 25.03.1992, Az. 1 BvR 1430/88 Rn 47; BVerfG Urteil v. 27.07.2005, Az. 1 BvR 668/04 Rn 81; *Sievers*, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes (2002), 133; *Ogorek* in Epping/Hillgruber (Hrsg), BeckOK Grundgesetz[41. Edition] (Stand: 15.11.2018) Art 10 Rn 39 ff.

165 *Durner* in Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019) Art 10 Rn 148; Rn 152.

166 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 259; vgl. § 100a iVm. § 100e Abs 1 Satz 1 dStPO idF. BGBl. 2017 I. 3202.

167 VfGH 29.06.2012, B 1031/11 = VfSlg. 19.657; VfGH 29.11.2017, G 223/2016; VwGH 24.04.2013, 2011/17/0293 = VwSlg 18612 A/2013.

168 BVerfG Beschluss v. 16.06.2009, Az. 2 BvR 902/06 Rn 42 ff.

genau jenem Zweck des deutschen Art 10 Abs 1 GG entspräche und die beim Provider gespeicherten Inhaltsdaten[169] weiter insofern außerhalb des Einflussbereiches (Herrschaftsbereiches) des Nutzers liegen würden, womit die spezifische Gefährdungslage, die das klassische Fernmeldegeheimnis vor Augen hat, in einer solchen Konstellation fortgesetzt bestehe.[170]

Art 8 Abs 1 EMRK („Recht auf Achtung der Korrespondenz") steht als Grundrecht gleichzeitig in Verfassungsrang und schützt sowohl Inhalts- (§ 92 Abs 1 Z 5 TKG 2003) als auch Verkehrsdaten (§ 92 Abs 1 Z 4 TKG 2003). Art 8 EMRK verlangt – anders als Art 10a StGG 1867 – nicht in jedem Fall eines Eingriffs in die „Korrespondenz" einen Richtervorbehalt. Ein Richtervorbehalt ist nur insoweit ein verfassungsrechtliches Erfordernis nach Art 8 EMRK, als ohne den Richtervorbehalt das konkrete Eingriffsmittel nicht als in einer demokratischen Gesellschaft für notwendig eingestuft werden könnte, demgemäß ist ein solcher Richtervorbehalt nach EMRK immer nur in gravierenden Eingriffsfällen erforderlich.[171] Nach Rechtsprechung des EGMR fallen unter „Korrespondenz" iSd. Art 8 Abs 1 EMRK bspw. „Telefongespräche", „E-Mails", „SMS" und „Internet".[172] Dieser Schutz der Kommunikation durch Art 8 Abs 1 EMRK ergibt sich nach EGMR Rechtsprechung nicht nur über das „Recht auf Achtung der Korrespondenz" sondern kann sich auch über das „Recht auf Achtung des Privatlebens". In den Entscheidungen *Copland*[173] und *Kennedy*[174] sah der EGMR beide Rechte des Art 8 Abs 1 EMRK als parallel einschlägig an.[175]

Befindet sich der entsprechende Sachverhalt zudem im Anwendungsbereich des Unionsrechts (EU-Vertrag, AEUV und EU-GRC) greift zusätzlich Art 7 EU-GRC, welcher die „Kommunikation" (iSv. jegliche individuelle Kommunikation, die an bestimmte Adressaten und nicht an die Öffentlichkeit gerichtet ist[176]) umfassend schützt und vom Regelungsinhalt weitgehend Art 8 Abs 1 EMRK entspricht. *Jarass* hält die bisherige Judikatur des EGMR zu Art 8 EMRK direkt auf Art 7 EU-GRC übertragbar.[177] Zudem bestimmt Art 52 Abs 3 Satz 1 EU-GRC, dass die EMRK als wichtigste Rechtserkenntnisquelle der Unionsgrundrechte anzusehen ist. Sobald ein in der EMRK garantiertes Recht einem Recht der EU-GRC entspricht, soll das Unionsgrundrecht die gleiche Bedeutung und Tragweite haben wie das entsprechende EMRK-Grundrecht.[178]

---

169 VfGH 29.06.2012, B 1031/11 = VfSlg. 19.657; VfGH 29.11.2017, G 223/2016; VwGH 24.04.2013, 2011/17/0293 = VwSlg 18612 A/2013.

170 *Chadoian*, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung (2015) 48 f.

171 *Chadoian*, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung (2015) 76 f.

172 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 21 ff; *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1438.

173 EGMR Urteil v. 03.04.2007, Az. 62617/00 (Copland gegen Vereinigtes Königreich).

174 EGMR, 18.05.2010, Az. 26839/05 (Kennedy gegen Vereinigtes Königreich).

175 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 13 ff; 32 ff.

176 *Jaras*s in Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016) Art 7 Rn 6; Rn 25 – 26.

177 *Jaras*s in Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016) Art 7 Rn 39.

178 *Kingreen* in Calliess/Ruffert (Hrsg), EUV/AEUV[5] (2016) Art 7 Rn 2; Art 52 Rn 21; Rn 31.

Hinsichtlich des Anwendungsbereichs stellt sich noch die Frage, ob Art 8 Abs 1 EMRK bzw. Art 7 iVm. Art 52 Abs 3 EU-GRC – entsprechend der Judikatur des deutschen BVerfG zu Art 10 Abs 1 GG[179] – auch bereits „empfangene" und „gelesene" Kommunikation nach abgeschlossenem Übermittlungsvorgang schützen (z.B. eingegangene eMail bleibt weiter im Account beim Provider gespeichert)?[180] Nach EGMR Judikatur erstreckt sich der Schutz der „Korrespondenz" gemäß Art 8 Abs 1 EMRK auch auf bereits empfangene bzw. bereits angekommene Nachrichten, die weiter aufbewahrt werden und nicht vernichtet bzw. gelöscht wurden. Der EGMR kam in zwei Urteilen zum Schluss, dass die Beschlagnahme von elektronischen Daten einen Eingriff in die durch Art 8 Abs 1 EMRK geschützte „Korrespondenz" darstelle. Im Fall *Bernh Larsen Holding AS*[181] befanden sich die Daten auf einem externen angemieteten Server, im Fall *Wieser and Bicos Beteiligungen GmbH*[182] waren die Daten vor Ort gesichert. Daraus kann gefolgert werden, dass es für den EGMR grundsätzlich keine Rolle spielt, wo die Daten konkret gespeichert sind, sondern es wird ausschließlich geprüft ob elektronisch gespeicherte „Korrespondenz" vorliegt oder nicht. „Elektronische Korrespondenz" ist also solange durch Art 8 Abs 1 EMRK geschützt, solange sie gespeichert ist. Der Ort der Speicherung (eigener Computer, externer Server, E-Mail Account, etc.) ist insofern irrelevant.[183]

An den Voraussetzungen ist zusammenfassend zu beachten, dass Art 10a StGG 1867 ein formelles Gesetz zur Beschränkung des Fernmeldegeheimnisses verlangt. Art 8 EMRK und Art 7 EU-GRC folgen bei Eingriffen in die „Korrespondenz" bzw. „Kommunikation" dem materiellen Gesetzesbegriff iSv. „law" (z.B. ungeschriebenes Richterrecht im Common Law-Rechtsystem bzw. auch reine Rechtsverordnungen, etc.).[184] Daraus ergibt sich:

- das Abfangen von Inhaltsdaten (§ 92 Abs 1 Z 5 TKG 2003) bzw. der Zugriff darauf direkt beim Provider bedarf eines Gesetzes im formellen Sinn und eines richterlichen Befehls je Einzelfall in Gemäßheit bestehender Gesetze (Art 10a StGG 1867). Eingriffsbefugnisse zum Abfangen von Nachrichten finden sich in den §§ 134 ff StPO (Richtervorbehalt).[185].
- das Abfangen von reinen Verkehrsdaten (§ 92 Abs 1 Z 4 TKG 2003) bzw. der Zugriff darauf direkt beim Provider bedarf nur einer gesetzlichen Ermächtigung iSv. „law" (materieller Gesetzesvorbehalt) gemäß Art 8 Abs 2 EMRK bzw. Art 7 EU-GRC. Nach hM kommt aber aufgrund der damit verbundenen Verarbeitung personenbezogener Daten auch das Grundrecht auf Datenschutz (§ 1 DSG [2000]) parallel zur Anwendung (vgl.

179 BVerfG Beschluss v. 16.06.2009, Az. 2 BvR 902/06 Rn 42 ff.
180 *Chadoian*, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung (2015), 48 f; BVerfG Beschluss v. 16.06.2009, Az. 2 BvR 902/06 Rn 42 ff.
181 EGMR Urteil v. 14.03.2013, Az. 24117/08 (Bernh Larsen Holding AS u.a. gegen Norwegen).
182 EGMR Urteil v. 16.10.2007, Az. 74336/01 (Wieser and Bicos Beteiligungen GmbH gegen Österreich).
183 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 19 ff.
184 *Chadoian*, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung (2015), 77.
185 §§ 135 Abs 3 iVm. § 137 Abs 1 Satz 2 StPO iVm. Art 10a StGG 1867.

Kapitel 2.3.4), welches gemäß § 1 Abs 2 DSG [2000] wieder ein formelles Gesetz verlangt,[186] sowie auch der ganz allgemeine Art 18 B-VG.[187] Gesetzliche Zugriffsbefugnisse auf Verkehrsdaten ohne richterlichen Vorbehalt iSd. VfGH und VwGH Judikatur[188] bei Betreibern öffentlicher Telekommunikationsdienste finden sich in § 76a StPO[189], § 53 Abs 3a und Abs 3b SPG[190,] § 11 Abs 1 Z 5 und Z 7 PStSG[191] und in § 22 Abs 2a und Abs 2b MBG[192].

Sowohl beim Abfangen von Inhaltsdaten (Art 10a StGG 1867, Art 8 Abs 1 EMRK u. Art 7 EU-GRC) als auch beim Abfangen von Verkehrsdaten (Art 8 Abs 1 EMRK, Art 7 EU-GRC) bzw. beim Zugriff darauf beim Provider, muss diese gesetzliche Ermächtigung die Voraussetzungen des Art 8 Abs 2 EMRK erfüllen. Das heißt der gesetzliche[193] Eingriff muss eine Maßnahme darstellen, die in einer demokratischen Gesellschaft notwendig ist:

- für die nationale Sicherheit,
- für die öffentliche Ruhe und Ordnung,
- für das wirtschaftliche Wohl des Landes,
- für die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen,
- zum Schutz der Gesundheit und der Moral oder
- zum Schutz der Rechte und Freiheiten anderer.[194]

Eingriffe außerhalb des Rahmens des Art 8 Abs 2 EMRK sind somit verfassungswidrig.

Hinsichtlich der gleichzeitig aus Art 8 EMRK, Art 7 EU-GRC und Art 10a StGG 1867 resultierenden staatlichen Schutzpflichten[195] im sensiblen Telekommunikationsbereich, kommt der österreichische Staat diesen – trotz enorm hoher Risiken – mA nicht ausreichend nach: Die österreichischen Telekom-spezifischen §§ 119, 119a StGB (Abfangen von Nachrichten bzw. von Daten) enthalten Strafdrohungen von max. 6 Monaten Freiheitsstrafe. Der

---

186 VfGH 15.06.2007, G147/06; ErläutRV 1613 BlgNr 20 GP 35; *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 2/57; *Ennöckl*, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014) 196 f.

187 *Bresich/Riedl* in Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl (Hrsg), DSG (2018) § 61 Rn 2.

188 VfGH 29.06.2012, B 1031/11 = VfSlg. 19.657; VfGH 29.11.2017, G 223/2016; VwGH 24.04.2013, 2011/17/0293 = VwSlg 18612 A/2013.

189 § 76a Strafprozessordnung 1975 idF. BGBl. I Nr. 33/2011.

190 § 53 Sicherheitspolizeigesetz idF. BGBl. I Nr. 29/2018.

191 § 11 Polizeiliches Staatsschutzgesetz idF. BGBl. I Nr. 5/2016.

192 § 22 Militärbefugnisgesetz idF. BGBl. I Nr. 102/2019 (Wehrrechtsänderungsgesetz 2019).

193 bei „Inhaltsdaten" ist ein Gesetz im formellen Sinn gem. Art 10a StGG 1867 zwingend; bei „Verkehrsdaten reicht nach Art 8 EMRK „law", also ein Gesetz im materiellen Sinn – allerdings verlangt § 1 Abs 2 DSG [2000] für Eingriffe in das Grundrecht auf Datenschutz wieder ein Gesetz im formellen Sinn, womit in den meisten Fällen ein formelles Gesetz erforderlich bleibt (vgl. **Kapitel 2.3.4**).

194 Art 8 Abs 2 EMRK; VfGH 29.06.2012, B 1031/11 = VfSlg. 19.657; VfGH 29.11.2017, G 223/2016; VwGH 24.04.2013, 2011/17/0293 = VwSlg 18612 A/2013; *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491.

195 *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017) Art 1 Rn 8; Art 8 Rn 2; *Mayer/Kucsko-Stadlmayer/Stöger,* Bundesverfassungsrecht[11] (2015) Rn 1333; *Siemen*, Datenschutz als Europäisches Grundrecht (2006) 177 f; *Wiederin* in Merten/Papier/Kucsko-Stadlmayer (Hrsg), Handbuch der Grundrechte in Deutschland und Europa, Band VII/1 Grundrechte in Österreich[2] (2014) § 10 Rn 127.

an die Telekom-Provider adressierte § 108 TKG 2003 enthält eine Strafandrohung von 3 Monaten, sollten österreichische Telekom-Provider oder deren Mitarbeiter vorsätzlich das Kommunikationsgeheimnis (§ 93 Abs 1 TKG 2003) verletzen. Wird ein Abhörgerät und/oder Tonaufnahmegerät zur Aufzeichnung von Telefongesprächen verwendet, droht eine Strafe von bis zu 1 Jahr gemäß § 120 Abs 1 StGB. Bei vorsätzlicher jahrelanger Nichtlöschung von sensiblen Verkehrsdaten (§ 92 Abs 1 Z 4 TKG 2003) tausender Betroffener entgegen § 99 Abs 1 Satz 1 TKG 2003 (Art 6 Abs 1 ePrivacy-RL) droht dem Management eines Telekom-Providers in Österreich eine gesamte maximale Verwaltungshöchststrafe von € 218. Mangels Verwaltungsstrafbestimmung in § 109 TKG 2003 bei Verstößen gegen die Löschpflicht von Verkehrsdaten stellt § 99 Abs 1 Satz 1 TKG 2003 eine fast sanktionslose Löschungsverpflichtung für sensible Verkehrsdaten dar, denn im Fall einer rechtswidrigen Nichtlöschung von Verkehrsdaten muss auf § 10 Abs 2 VStG[196] zurückgegriffen werden (vgl. Art 95 DSGVO), welcher folgendes bestimmt: „*Soweit für Verwaltungsübertretungen* (…) *keine besondere Strafe festgesetzt ist, werden sie mit Geldstrafe bis zu 218 Euro* (…) *bestraft.*“[197] In Deutschland drohen bei Verletzungen der vergleichbaren Telekom-spezifischen §§ 206, 202a, 202b dStGB Strafandrohungen zwischen 2 – 5 Jahren Freiheitsstrafe. Wird über ein Abhörgerät das nichtöffentlich gesprochene Wort (z.B. Telefongespräche) eines anderen abgehört und/oder auf einen Tonträger aufgezeichnet, droht in Deutschland eine Strafe von bis zu drei Jahren (§ 201 Abs 1 dStGB). Bei nicht unverzüglicher Löschung der Verkehrsdaten pro Verbindung durch deutsche Telekom-Provider gemäß § 96 Abs 1 Satz 3 dTKG 2004 drohen Bußgelder iHv. € 300.000 (§ 149 Abs 1 Nr 17 iVm. Abs 2 Nr. 2 dTKG 2004; ausgenommen z.B. erforderliche Abrechnungsdaten[198], erforderliche Störungens- Verfügbarkeits- bzw. Missbrauchserkennung[199], gesetzliche Vorratsdatenspeicherung[200]). Zusätzlich zu den Schutzpflichten aus Art 8 EMRK[201] verlangt auch die Europäische Union, dass die EU-Mitgliedsstaaten in Umsetzung der ePrivacy-Richtlinie 2002/58/EG Sanktionen – einschließlich strafrechtlicher Sanktionen – festlegen müssen, welche bei einem Verstoß gegen die nationalen Vorschriften zur Umsetzung der Richtlinie zu verhängen sind und dabei *„wirksam“*, *„verhältnismäßig“* und *„abschreckend“* sind (vgl. Art 15a ePrivacy-RL 2002/58/EG). Die vorgesehenen österreichischen Sanktionen werden diesen europarechtlichen Anforderungen mA nicht gerecht. Würde jemand z.B. anlasslos österreichische Telekommunikation speichern, wie dies der ehemalige österreichische Inlandsgeheimdienstchef *Gert René Polli* stark vermutet (*„Gesamte Telekommunikation in Österreich wird gespeichert* (…) *Schon bei meinem ersten Amtsbesuch in Großbritannien wollte der MI5 sämtlichen österreichischen Daten spiegeln, heute ist das*

196 *Sokolov* in heise.de (12.03.2018), Jahrelange Datenschutzverletzung: Telekom Austria drohen 218 Euro Strafe, abrufbar unter: https://www.heise.de/newsticker/meldung/Jahrelange-Datenschutzverletzung-Telekom-Austria-drohen-218-Euro-Strafe-3990676.html?seite=all (zuletzt abgerufen am 20.06.2019); Datenschutzbehörde Bescheid Beschwerde v. 28.05.2018 DSB-D216.471/0001-DSB/2018.

197 § 10 Abs 2 VStG idF. BGBl. I Nr. 5/2008 (Verwaltungstrafgesetz 1991).

198 § 97 iVm. § 96 Abs 1 dTKG 2004.

199 § 100 dTKG 2004.

200 §§ 113a ff dTKG 2004.

201 *Mayer/Kucsko-Stadlmayer/Stöger,* Bundesverfassungsrecht[11] (2015) Rn 1333; *Siemen*, Datenschutz als Europäisches Grundrecht (2006) 177 ff.

Fakt“)[202], hätte diese Person oder Stelle – soweit sie dadurch nicht explizit ein österreichisches Staatsgeheimnis (§ 254 StGB) oder ein Geschäfts- oder Betriebsgeheimnis (§§ 123 f StGB; § 11 Abs 2 UWG) sich verschaffen will bzw. konkret unmittelbar im österreichischen Inland einen militärischen Nachrichtendienst für einen fremden Staat bzw. – unabhängig vom Ort – nachweisbar einen solchen Nachrichtendienst zum Nachteil der Republik Österreich betreiben bzw. unterstützen will (iSv. Risiko für die Sicherheit, Ansehen, Prosperität Österreichs; vgl. § 256 bzw. § 319 StGB) – lediglich eine maximale Freiheitsstrafe von 3 – 6 Monaten zu befürchten (§§ 119, 119a StGB, § 108 TKG 2003), zusätzlich vorausgesetzt, dass das StGB überhaupt anwendbar wäre (vgl. §§ 62 ff. StGB).

2.3.2 Unverletzlichkeit des Hausrechts (Art 9 StGG 1867 iVm. HausrechtsG 1862) und Recht auf Achtung der Wohnung (Art 8 Abs 1 EMRK und Art 7 EU-GRC)

In Österreich dienen Art 9 StGG 1867 und das Gesetz vom 27. October 1862 zum Schutze des Hausrechtes (HausrechtsG 1862) als Grundrechte zur Wahrung der persönlichen Intimsphäre. Einen vergleichbaren Schutz gewähren Art 8 Abs 1 EMRK und Art 7 EU-GRC mit dem jedermann zustehenden Anspruch auf Achtung der Wohnung.[203] Art 9 StGG 1867 iVm. mit dem HausrechtsG 1862 verlangt als verfassungsgesetzlich gewährleistete Rechte eine prinzipielle Bindung von „Hausdurchsuchungen“ an einen „richterlichen Befehl“. Die nach hM in der Literatur strengeren rein österreichischen Grundrechte zum Hausrechtsschutz aus dem 19. Jahrhundert würden dann den europäischen Grundrechten aus dem 20. Jhdt. und 21. Jhdt vorgehen (vgl. Art 53 EMRK, Art 52 Abs 3 Satz 2 EU-GRC;). Im Zentrum der Diskussion steht dabei der Begriff der „Hausdurchsuchung“ gemäß Art 9 StGG 1867 iVm. HausrechtsG 1862. Eine solche „Hausdurchsuchung“ verlangt in jedem Fall einen „richterlichen Befehl“. In der österreichischen Lehre wird der Begriff „Hausdurchsuchung“ der Wohnung bzw. von Geschäfts- oder Betriebsräume[204] weiter definiert, so würden auch Ermittlungen iSv. „Spähangriffen“ von außen darunter fallen.[205] Dies wären bspw. akustische oder optische Wohnraumüberwachungen, Messung der elektromagnetischen Abstrahlungen zur Überwachung eines rein „offline“ arbeitenden IT-Systems oder das Eindringen durch Beamte in eine Wohnung um ein dort befindliches informationstechnisches System physisch zu manipulieren, um entsprechende Überwachungsmaßnahmen anschließend u.a. in der Wohnung bzw. in den Geschäftsräumen durchführen zu können.[206] *Raschhofer* lehnt diese hM der Lehre mit Verweis auf die bisherige VfGH Rechtsprechung strikt ab, denn diese aus Deutschland kommenden Überlegungen (Art 13 Abs 1 GG) wären zum größten Teil nicht auf die österreichische Rechtsordnung im HausrechtsG 1862 übertragbar. Spähangriffe bzw. Online-Durchsuchungen, wo nie eine Wohnung oder Räumlichkeit tatsächlich betreten wird, wären nach *Raschhofer* nicht als „Hausdurchsuchungen“ iSd. österreichischen Art 9 Abs 2 StGG 1867 iVm. HausrechtsG 1862 zu verstehen. Wird für die

202 *Kesssler* in futurezone.at (24.02.2015), “Gesamte Telekommunikation in Österreich wird gespeichert”, abrufbar unter: https://futurezone.at/netzpolitik/gesamte-telekommunikation-in-oesterreich-wird-gespeichert/116.081.559 (zuletzt abgerufen am 20.06.2019).

203 *Jarass* in Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016) Art 7 Rn 39.

204 *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1428.

205 *Wiederin*, Privatssphäre und Überwachungsstaat (2003) 228 ff; *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1431.

206 BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07 Rn 192 ff.

Kompromittierung des IT-Systems zwar die Wohnung betreten, ist das IT-System in der betretenen Wohnung aber „frei sichtbar“ und nicht irgendwo versteckt (z.B. in einem Schrank) und kann das IT-System somit „ohne systematische Besichtigung“ im Sinne einer „Durchsuchung der Wohnung bzw. der Räumlichkeit“ sofort von den Beamten wahrgenommen werden, liege nach *Raschhofer* mit Verweis auf die Judikatur des VfGH – trotz Betretens der Wohnung durch Beamte – noch immer keine unter Richtervorbehalt stehende „Hausdurchsuchung“ iSd. Art 9 Abs 2 StGG 1867 iVm. HausrechtG 1862 vor. Folgt man der Interpretation des HausrechtsG 1862 in Sinne von *Raschhofer* und der bisherigen VfGH Judikatur, wäre – im reinen Betretungsfall zur Kompromittierung eines „frei sichtbaren“ IT-Systems bzw. bei Spähangriffen durch Beamte – das „Recht auf Achtung der Wohnung“ gemäß Art 8 Abs 1 EMRK bzw. Art 7 EU-GRC das strengere Grundrecht und insofern vorrangig anwendbar. Für das reine Betreten der Wohnung ist dann nur ein „law“ iSd. Art 8 Abs 2 EMRK erforderlich. Mangels „systematischer Besichtigung“ iSv. „Hausdurchsuchung“ bestünde kein unmittelbarer Richtervorbehalt aus Art 9 StGG 1867.[207]

Eingriffsbefugnisse zu Durchsuchungen von Orten (§§ 117 ff StPO) und die optische und akustische Überwachung von Personen (§§ 136 f StPO) stehen unter Richtervorbehalt.

Der österreichische Gesetzgeber kommt seinen Schutzpflichten[208] durch strafrechtliche Bestimmungen nach. Strafrechtlicher Schutz besteht – neben den nicht-IT-relevanten § 109 StGB (Hausfriedensbruch; jedoch „Gewalt“ iSv. Türschloss aufbrechen bzw. Türe eintreten vorausgesetzt[209]), § 125 StGB (Sachbeschädigung), etc. – durch § 126a StGB (Datenbeschädigung), § 126b StGB (Störung der Funktionsfähigkeit eines Computersystems), § 120 Abs 1 StGB (Missbrauch von Tonaufnahmen und Abhörgeräten), § 119a StGB (Abfangen von Daten aus einer elektromagnetischen Abstrahlung eines Computersystems), § 63 DSG 2018 (Strafbestimmung bei Datenschutzverletzungen), § 123 StGB (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses), § 124 StGB (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands) und § 11 UWG (Verletzung von Geschäfts- oder Betriebsgeheimnissen).

2.3.3 Recht auf Achtung des Privatlebens (Art 8 Abs 1 EMRK und Art 7 EU-GRC)

Der völkerrechtliche und in Österreich zugleich im Verfassungsrang als Grundrecht stehende Art 8 Abs 1 EMRK gewährleistet den Schutz des Privatlebens. Die Rechtsprechung und die Ansichten zu Art 8 EMRK sind nach hA umfassend auf Art 7 EU-GRC übertragbar (vgl. Art 52 Abs 3 Satz 1 EU-GRC).[210] Der Begriff des „Privatlebens“ iSd. Art 8 Abs 1 EMRK (Art 7 EU-GRC) wird dabei umfassend verstanden. „Privatleben“ iSd. EMRK ist nicht auf die Gewährleistung eines privaten Rückzugsraums beschränkt, dies wird bereits vom „Recht auf Achtung der Wohnung“ in Art 8 Abs 1 EMRK umfassend garantiert. Das

207 *Raschhofer* in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 222 f.

208 *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017) Art 1 Rn 8; Art 8 Rn 2; *Mayer/Kucsko-Stadlmayer/Stöger,* Bundesverfassungsrecht[11] (2015) Rn 1333; *Siemen*, Datenschutz als Europäisches Grundrecht (2006) 177 f.

209 *Fabrizy*, StGB[13] (2018) § 109 Rn 3.

210 *Jaras*s in Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016) Art 7 Rn 39; *Kingreen* in Calliess/Ruffert (Hrsg), EUV/AEUV[5] (2016) Art 7 Rn 2; Art 52 Rn 21; Rn 31.

bedeutet, dass das „Privatleben" im Verständnis der EMRK insofern keiner abschließenden Definition zugänglich ist. Wesentlich für die EMRK-konforme Auslegung des Begriffs des „Privatlebens" ist die Autonomie eines jeden Menschen. Dem folgend steht im Zentrum der Garantien des Art 8 Abs 1 EMRK zum „Privatleben" das „Recht auf Selbstbestimmung". Unter „Selbstbestimmung" wird eine geschützte Sphäre verstanden, in der eine Person ihr Leben nach ihrer Wahl lebt und ihre Persönlichkeit entwickeln kann.[211] Damit soll die Möglichkeit der Entwicklung und Verwirklichung jedes Einzelnen sichergestellt werden, weshalb sich hier auch eine gewisse Nähe zum deutschen Allgemeinen Persönlichkeitsrecht nach Art 2 Abs 1 iVm Art 1 Abs 1 GG in seinen unterschiedlichen Ausprägungen[212] zeigt. Denn auch das deutsche BVerfG gibt für das Allgemeine Persönlichkeitsrecht gemäß Art 2 Abs 1 iVm. Art 1 Abs 1 GG keine abschließende Umschreibung bzw. keine Definition seines Schutzbereichs.[213] Es ist im Einzelnen schwierig zu bestimmen, (ab) wann eine geschützte Sphäre des „Privatlebens" konkret betroffen wird, insbesondere wenn es sich um Maßnahmen außerhalb des häuslichen Bereichs handelt. Bei der „Privatsphäre" iSd. EMRK handelt es sich folglich um einen Bereich, der frei von Beobachtung, Überwachung und Ausforschung ist. Das Recht auf Privatsphäre iSd. EMRK umfasst insofern das Recht jedes Einzelnen sich grundsätzlich ohne Beobachtung (durch staatliche Organe) im öffentlichen Raum zu bewegen. Mit Hinblick auf die Persönlichkeitsentfaltung haben heute virtuelle Räume im Internet häufig die gleiche Bedeutung wie reale Räume, denn mittlerweile findet ein großer Teil dessen, was früher an Persönlichkeitsentfaltung in realen Räumen stattfand, „online" als Persönlichkeitsentfaltung im Internet statt. Virtuelle Räume können folglich im Einzelfall zur Privatsphäre eines Einzelnen zählen, ein Eingriff wird damit durch Art 8 EMRK geschützt. Für den EGMR ist bei der Prüfung, ob ein solcher Eingriff in das Privatleben vorliegt, u.a. aber auch von Bedeutung – aber nicht allein entscheidend – ob ein Betroffener im Einzelfall die Achtung seiner Privatsphäre erwarten kann („reasonable expectation of privacy"). Das Problem mit dem Abstellen auf eine „reasonable expectation of privacy" besteht nun insofern darin, dass ein Betroffener sich häufig nicht mehr auf den Schutz des Privatlebens berufen kann, sobald bei einem Betroffenen dieses Vertrauen in einen Privatsphärenschutz offensichtlich nicht mehr bestehen kann. Denn gibt jemand seine Daten freiwillig preis – sei es explizit oder schlicht durch die Nutzung der Online-Dienste und Sozialen Netzwerke –, kann er nicht mehr schlüssig behaupten, eine „reasonable expectation of privacy" hinsichtlich seiner Daten zu haben. Anders als in der realen Welt, ist es in der Online-Welt die Regel, dass Online-Aktivitäten elektronische Spuren hinterlassen und diese gespeichert und analysiert werden. Ein Nutzer muss insofern davon ausgehen, dass jeder der beteiligten Online-Dienste seine Daten speichert. Eine begründete Erwartung in Achtung der Privatsphäre kann im virtuellen Raum häufig gar nicht mehr erfolgreich argumentiert werden. Demgemäß würde in dieser Konstellation, wo primär auf eine „reasonable expectation of privacy" des Betroffenen abgestellt wird, nur noch der Schutz der Individualkommunikation durch das „Recht auf Achtung der Korrespondenz" (siehe

211 *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017) Art 8 Rn 7.

212 z.B. Recht auf Privatsphäre, Recht auf informationelle Selbstbestimmung, Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme, etc.

213 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 25.

oben) greifen. Mangels eines nicht mehr begründbaren Vertrauens in einen Privatsphärenschutz besteht nach *Paefgen* „online" kein umfassendes „Recht auf Achtung der Privatsphäre" iSd. EMRK.[214]

Stellt man bei der Betrachtung des Schutzbereichs des Art 8 Abs 1 EMRK auf die Verarbeitung von personenbezogenen Daten ab, fällt die Sammlung personenbezogener Daten in den Schutzbereich des „Recht auf Achtung des Privatlebens" gemäß Art 8 Abs 1 EMRK.[215] Der EGMR unterscheidet aber – der Einstufung der realen Welt folgend (siehe oben) – zwischen geschützten „privaten" Daten, sowie Daten, die keinen engen Bezug zum Privatleben haben und „öffentlichen" Daten, welche grundsätzlich nicht unter den Schutz des Art 8 Abs 1 EMRK fallen.[216] Der EGMR differenziert insofern zwischen Daten, die einen besonders engen Bezug zum Privatleben haben, hier stellt bereits die „Erhebung" dieser Daten einen Eingriff in Art 8 Abs 1 EMRK dar. Hinsichtlich von Daten, die keinen engen Bezug zum Privatleben haben – bis hin zu (teil-)öffentlichen Daten – nimmt der EGMR einen Eingriff in Art 8 Abs 1 EMRK erst dann an, wenn diese Daten systematisch gesammelt und gespeichert werden, also eine umfangreiche Sammlung von Daten über eine bestimmte Person erfolgt, die in der Art oder im Ausmaß über das normalerweise Vorhersehbare hinausgeht (iSv. „reasonable expectation of privacy"). Nach *von Grafenstein* folgt der EGMR dabei folgendem Kriterienbündel: **1.** Wurden die Daten unter Verstoß einer besonderen Vertraulichkeitserwartung erlangt (z.B. Betroffener war zu Hause; oder Betroffener benutzte TK-Dienste)? **2.** Liegt ein privater oder öffentlicher Anlass vor? **3.** Werden die Daten nur eingeschränkt genutzt oder veröffentlicht? **4.** Ist bzw. war der Betroffene überhaupt in der Lage, die Erhebung seiner Daten durch entsprechendes Verhalten zu vermeiden (abgelehnt im Fall eines gesetzlichen Durchsuchungsrechts für die Polizei im öffentlichen Raum)?[217]

Während die Grenze zwischen öffentlichem und privatem Bereich im realen Leben mit gewissen Abgrenzungsschwierigkeiten durchaus erfolgreich gezogen werden kann, gibt es in der „virtuellen Welt" noch keinen definierten Bereich, wie bspw. eine „digitale Wohnung" bzw. „digitale Büros" oder ähnlichem, wo ein umfassender Schutz vor Online-Zugriffen bestünde (bzw. die es ermöglichen würden „private" Daten klar zu definieren). Demgemäß müsste – vergleichbar zum Hausrecht – der heimische Computer bzw. ein eigengenutztes informationstechnisches System rechtlich vor Eingriffen, die direkt über öffentliche Kommunikationsnetze erfolgen (z.B. „Online-Durchsuchung", „Quellen-TKÜ"), geschützt werden. Der Privatsphärenschutz des Art 8 Abs 1 EMRK greift mangels der Möglichkeit erfolgreich eine „reasonable expectation of privacy" als Betroffener zu behaupten in der Online Welt hier nicht umfassend. Eine Darlegung, dass man sich „online" in einem privaten Bereich befinde, wo man umfänglich vertrauen dürfe, dass das Verhalten nicht beobachtet werde bzw. nicht ausgelesen wird, wird nur schwer gelingen. Der Einzelne ist zu seiner

214 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 26; 32 f; *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017) Art 8 Rn 31 f.

215 *Raschhofer* in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 211.

216 *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017) Art 8 Rn 31 f.

217 *von Grafenstein*, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit, DuD 12/2015, 789 (793).

Persönlichkeitsentwicklung heute aber auf die Nutzung von informationstechnischen Systemen angewiesen und muss dabei – gewissermaßen zwangsweise – einem solchen System persönliche Daten anvertrauen bzw. liefert durch die Nutzung des IT-Systems solche Daten. Das deutsche „IT-Grundrecht" des BVerfG hängt – anders als das Recht auf informationelle Selbstbestimmung – daher nicht vom fallbezogenen Einverständnis des Betroffenen bzw.einer präzisen verhältnismäßigen rechtlichen Grundlage für eine konkrete zweckgebundene Datenerhebung, -verarbeitung und -nutzung ab, sondern es wird die Vertraulichkeit eines ganzen IT-Systems vor Gesamtzugriffen von außen gewährleistet, dem sich ein Grundrechtsträger anvertraut hat, ohne dass gleichzeitig erwartet werden kann, dass der Grundrechtsträger das IT-System selbst beherrschen kann.[218] Die Judikatur des EGMR kennt sprachlich noch kein „IT-Grundrecht"; heimliche Online-Durchsuchungen von privaten oder geschäftlichen IT-Systemen über öffentliche Kommunikationsnetze stellen einen Eingriff in das „Recht auf Achtung der Privatsphäre" bzw. des „Rechts auf Achtung der Korrespondenz" gemäß Art 8 Abs 1 EMRK („Recht auf Achtung der Kommunikation" iSd. Art 7 EU-GRC) dar und sind geschützt.[219] Jeder Eingriff erfordert eine gesetzliche Ermächtigung (materiellen Gesetzesbegriff – „law"), die in einer demokratischen Gesellschaft notwendig sein muss (Art 8 Abs 2 EMRK):

- für die nationale oder öffentliche Sicherheit,
- für das wirtschaftliche Wohl des Landes,
- zur Aufrechterhaltung der Ordnung,
- zur Verhütung von Straftaten,
- zum Schutz der Gesundheit oder der Moral oder
- zum Schutz der Rechte und Freiheiten anderer.220

Offen ist, ob aus Art 8 EMRK bzw. Art 7 EU-GRC („demokratischen Gesellschaft notwendig") ein Richtervorbehalt für den Einsatz der Schadsoftware „Bundestrojaner" begründet wird. In Österreich wird der Einsatz von Schadsoftware „Bundestrojaner" für Quellen-TKÜs (nicht für Online Durchsuchungen) zur Aufklärung bestimmter Delikte ab dem Jahr 2020 erlaubt und unter Richtervorbehalt gestellt (§§ 135a, 137 Abs 1 Satz 3 StPO).[221]

2.3.4 Grundrecht auf Datenschutz (§ 1 DSG [2000] und Art 8 EU-GRC)

Das Grundrecht auf Datenschutz gemäß § 1 DSG [2000] gewährt – viel konkreter als Art 8 Abs 1 EMRK – einen verfassungsrechtlichen Anspruch auf Geheimhaltung von personenbezogenen Daten. § 1 DSG [2000] überschneidet sich zwar mit dem zugleich verfassungsrechtlich gewährleistetem Recht auf Achtung des Privatlebens und der Korrespondenz gemäß Art 8 Abs 1 EMRK, das Grundrecht auf Datenschutz ist aber detaillierter und geht

218 *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017) Art 8 Rn 41 f; *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 52 f; 81; 85 ff; 102 ff.

219 *Raschhofer* in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 214 ff; *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 104 f.

220 Art 8 Abs 2 EMRK.

221 ErläutRV 17 BlgNr 26. GP 2; 8 ff; Strafprozessrechtsänderungsgesetz 2018 BGBl. I Nr. 27/2018.

über Art 8 EMRK hinaus. § 1 DSG [2000] stellt hinsichtlich seiner Anwendbarkeit alleine auf die „Verwendung" (§ 4 Z 8 DSG 2000 aF)[222] von personenbezogenen Daten ab. Darüber hinaus ist das Grundrecht auf Datenschutz seit dem Jahr 1978 mit unmittelbarer Drittwirkung ausgestaltet, das heißt es gilt auch unmittelbar zwischen Privaten. Das geschützte Geheimhaltungsinteresse an personenbezogenen Daten nach § 1 DSG [2000] ist nur dann ausgeschlossen, wenn die personenbezogenen Daten einem solchen Geheimhaltungsanspruch gar nicht zugänglich sind (z.B. allgemeine Verfügbarkeit oder nicht auf den Betroffenen rückführbar).[223]

Eingriffe in das Grundrecht auf Datenschutz gemäß § 1 DSG [2000] sind nur rechtmäßig:

- mit des Zustimmung des/der Betroffenen
- im lebenswichtigen Interesse des/der Betroffenen oder
- zur Wahrung „überwiegender berechtigter Interessen" eines anderen (im Anwendungsbereich der DSGVO europarechtskonform „berechtigte Interessen"[224]).

Durch eine staatlichen Behörde dürfen Eingriffe in das Grundrecht auf Datenschutz nur auf Grund von formellen Gesetzen, die aus den in Art 8 Abs 2 EMRK genannten Gründen notwendig sind, erfolgen.[225] Beschränkungen bzw. Eingriffe in das Grundrecht auf Datenschutz müssen dabei „notwendig" und „verhältnismäßig" sein. Ein solcher gemäß § 1 Abs 2 DSG [2000] zulässiger Eingriff muss im Hinblick auf den Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Ein Eingriff in das Grundrecht auf Datenschutz darf jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.[226]

Der Schutz personenbezogener Daten wird gleichzeitig durch Art 8 EU-GRC als EU-Primärrecht garantiert. Art 8 EU-GRC formuliert einerseits ein klassisches Abwehrrecht gegen staatliches Handeln (*status negativus*) in Durchführung des Unionsrechts als auch andererseits staatliche Schutzpflichten (*status positivus*) zur Gewährleistung, dass für jede Person im Anwendungsbereich des Unionsrechts das Recht auf Schutz der sie betreffenden personenbezogenen Daten entsprechend sichergestellt wird.[227] Art 8 Abs 2 Satz 1 EU-GRC normiert Anforderungen an eine rechtskonforme Datenverarbeitung. Personenbezogene Daten dürfen im Anwendungsbereich des Unionsrechts (Art 51 EU-GRC) gemäß Art 8 Abs 2 Satz 1 EU-GRC nur unter folgenden Bedingungen verarbeitet werden:

- Verarbeitung nach Treu und Glauben (Fairness und Transparenz)

---

222 § 4 Z 8 DSG 2000 idF. BGBl. I Nr. 133/2009: „*jede Art der Handhabung von Daten* (…)". **aA** nach AA-10 v. 20.04.2018 zu IA 189/A 26. GP 4 (DatenschutzDeregulierungs-Gesetz 2018): *„Das Grundrecht auf Datenschutz wurde bisher im Sinne der Begriffsbestimmungen des § 4 DSG 2000 ausgelegt* (…). *Nunmehr muss es im Sinne der Begriffsbestimmungen der DSGVO ausgelegt werden."*

223 *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1439.

224 EuGH Rs. 6/64, Slg. 1964, S. 1251, 1269 – Costa/ENEL iVm. Art 2 iVm. Art 6 Abs 1 lit f DSGVO.

225 ErläutRV 1613 BlgNr 20 GP 34 f; *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 2/57; *Ennöckl*, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014) 196 f.

226 *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1442 ff; AB 98 BlgNR 26. GP 3 (Bericht Verfassungsausschuss – Datenschutz-Deregulierungs-Gesetz 2018).

227 *Gersdorf* in Gersdorf/Paal (Hrsg), BeckOK Informations- und Medienrecht[24. Edition] (Stand: 01.05.2019) EU-GRCharta Art. 8 Rn 12.

- Verarbeitung für festgelegte Zwecke (Zweckbindung)
- Rechtsgrundlage
  - Einwilligung der betroffenen Person oder
  - sonstige gesetzlich geregelte legitime Rechtsgrundlage (z.B. DSGVO, etc.).

Nach Art 8 Abs 2 Satz 2 EU-GRC hat jede Person – wieder vorausgesetzt der Sachverhalt der Datenverarbeitung befindet sich im Anwendungsbereich des Unionsrechts – unmittelbar unionsprimärrechtlich:

- das Recht auf Auskunft, und
- das Recht, die Berichtigung der sie betreffenden personenbezogenen Daten zu erwirken.

Eine legitime gesetzliche Grundlage iSd. Art 8 Abs 2 Satz 1 EU-GRC muss „*klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahmen vorsehen*“, damit die Adressaten ihr Verhalten darauf einrichten können und es muss der Zweck der Verarbeitung darin klar festgelegt werden.[228] Es ist insofern der zentrale Grundsatz des europäischen Datenschutzrechts, dass eine Datenverarbeitung gesetzlich legitimiert sein muss. Das heißt im Rahmen des Art 8 EU-GRC gilt nicht der allgemeine Grundsatz für Lebenssachverhalte „*Alles, was nicht verboten ist, ist erlaubt*“, sondern der datenschutzrechtliche Grundsatz des Art 8 EU-GRC lautet „*Alles, was nicht erlaubt ist, ist verboten*“.[229]

Zu beachten ist, dass „gesetzlich“ iSd. österreichischen § 1 DSG [2000] ein formelles Gesetz verlangt[230] (vgl. zusätzlich Art 18 B-VG[231]), der EuGH für „gesetzlich“ iSd. Art 8 EU-GRC auch ein materielles Gesetz als mit der EU-Grundrechte Charta konforme Erlaubnisnorm ansieht (z.B. Durchführungsverordnungen der EU-Kommission ohne Beteiligung des EU-Parlaments).[232] Der österreichische § 1 DSG [2000] enthält aktuell mA insofern strengere Garantien als der europäische Art 8 EU-GRC. Gemäß Art 8 Abs 3 EU-GRC hat die Einhaltung der Vorschriften zum Datenschutz im Rahmen der Durchführung des Unionsrechts (Art 51 EU-GRC) von einer unabhängigen Stelle überwacht zu werden.[233]

Der VfGH hat die EU-GRC gesamt als „verfassungsgesetzlich gewährleistete Rechte“ mit selbstständiger Justiziabilität anerkannt.[234] Zu Art 8 EU-GRC im Verhältnis zu § 1 DSG [2000] sprach der VfGH im Jahr 2012 aus, dass Art 8 EU-GRC keinen über die Verfassungsbestimmung des § 1 DSG [2000] hinausgehenden Schutzgehalt hat und damit eine Prüfung beider Bestimmungen zum selben Ergebnis führt.[235] Der *Verfassungsausschuss des*

228 *Jarass* in Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016) Art 8 Rn. 11 ff.

229 *Forgó* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil I. Kapitel 2. Rn 18.

230 VfGH 15.06.2007, G147/06; ErläutRV 1613 BlgNr 20 GP 35; *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 2/57; *Ennöckl*, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014) 196 f.

231 *Bresich/Riedl* in Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl (Hrsg), DSG (2018) § 61 Rn 2.

232 EuGH Urteil v. 09. 11. 2010 C-92/09, C-93/09 („Schecke“) Rn 56 ff; *Jarass* in Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016) Art 52 Rn. 23 ff.

233 *Gersdorf* in Gersdorf/Paal (Hrsg), BeckOK Informations- und Medienrecht[24. Edition] (Stand: 01.05.2019) EU-GRCharta Art. 8 Rn 39 f.

234 VfGH 14.03.2012, U 466/11 = VfSlg 19.632/2012; *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rn 1317; Rn 1347.

235 VfGH 29.09.2012, B54/12.

Nationalrats sieht eine parallele Anwendbarkeit von § 1 DSG [2000] und Art 8 EU-GRC im Rahmen des Anwendungsbereichs des Unionsrechts als gegeben.[236]

Rein „private Daten" werden zusätzlich auch von Art 7 EU-GRC bzw. Art 8 EMRK geschützt (vgl. **Kapitel 2.3.3**).[237]

Es stellt sich nun noch abschließend die Frage, wie sich § 1 DSG [2000] bzw. Art 8 EU-GRC zu Online Durchsuchungen und Quellen-TKÜs mittels staatlicher Schadsoftware „Bundestrojaner" verhalten, denn das österreichische Recht kennt kein „IT-Grundrecht"? Nach hM ist eine Online-Durchsuchung ein Eingriff in das Recht auf Achtung des Privatlebens und der Korrespondenz gemäß Art 8 Abs 1 EMRK und zugleich ein Eingriff in das Grundrecht auf Datenschutz gemäß § 1 DSG [2000]. Da eine Online-Durchsuchung bzw. Quellen-TKÜ nicht im lebenswichtigen Interesse des Betroffenen stattfindet bzw. auch nicht mit dessen Zustimmung, sind die Voraussetzungen des § 1 Abs 2 Satz 2 DSG [2000][238] iVm. Art 8 Abs 2 EMRK umfassend einzuhalten.[239] Eine „Online-Durchsuchung" bzw. Quellen-TKÜ ist ein schwerer Eingriffe in das Grundrecht auf Datenschutz und sollte nach *Raschhofer* nur zur Bekämpfung schwerer oder organisierter Kriminalität und mit Richtervorbehalt vorgesehen werden.[240] § 135a StPO erlaubt in Österreich ab dem Jahr 2020 den Einsatz von Schadsoftware „Bundestrojaner" für Quellen-TKÜs („Überwachung verschlüsselter Nachrichten") und stellt den Einsatz dieser Schadsoftware unter Richtervorbehalt (§ 137 Abs 1 StPO). Für Online Durchsuchungen existiert aktuell allerdings keine Rechtsgrundlage in Österreich.[241]

Der österreichische Gesetzgeber kommt seinen Schutzpflichten im Bereich des „Grundrechts auf Datenschutz" (§ 1 Abs 1 DSG [2000] / Art 8 EU-GRC) [242] u.a. durch strafrechtliche (§ 63 DSG, §§ 118 ff StGB, § 11 UWG), verwaltungsstrafrechtliche (Art 83 DSGVO, § 62 DSG) und zivilrechtliche (§ 29 DSG iVm. Art 82 DSGVO; §§ 16, 1328a ABGB; §§ 26a ff UWG) Bestimmungen nach.

236 AB 98 BlgNR 26. GP 3 (Bericht Verfassungsausschuss – Datenschutz-Deregulierungs-Gesetz 2018).
237 *Johannes* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 2 Rn 57.
238 bzw. ähnliches Ergebnis gemäß Art 8 iVm. Art 52 Abs 3 EU-GRC.
239 *Raschhofer* in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 215 f.
240 *Raschhofer* in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 214 f.
241 ErläutRV 17 BlgNr 26. GP 2; 8 ff; Strafprozessrechtsänderungsgesetz 2018 BGBl. I Nr. 27/2018.
242 *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017) Art 1 Rn 8; Art 8 Rn 2; *Mayer/Kucsko-Stadlmayer/Stöger,* Bundesverfassungsrecht[11] (2015) Rn 1333; *Siemen*, Datenschutz als Europäisches Grundrecht (2006) 177 f.

2.4 Ergebnis

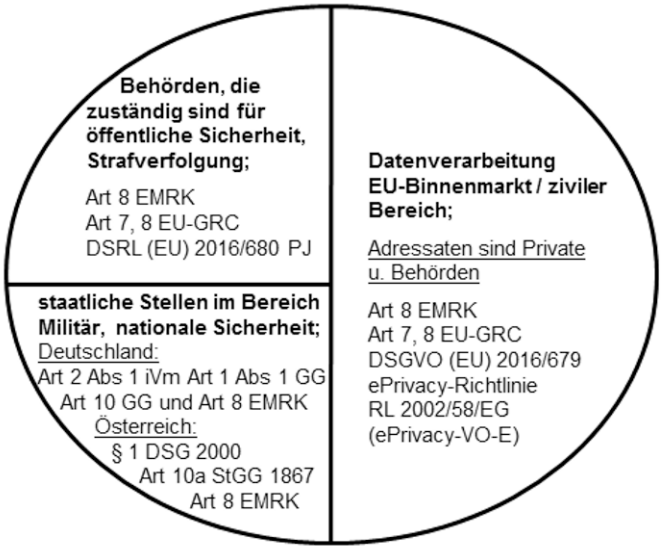


Abbildung 1: Anwendbare Regelungen im Datenschutz je Politikbereich in Deutschland und Österreich

3 Europäisches Datenschutzrecht und IT-gestützter Arbeitsplatz

3.1 Einordnung gemäß OSI Modell[243]

Das neue sekundärrechtliche Datenschutzrecht der Europäischen Union stellt sich für den deutschsprachigen EU-Raum Deutschland und Österreich im privatwirtschaftlichen Bereich seit dem 25. Mai 2018 im Wesentlichen wie folgt dar:

- Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) als unmittelbar anwendbarer auf Art 16 AEUV gestützter Sekundärrechtsakt der Europäischen Union sowie dazu:
  - §§ 1 – 44 BDSG idF. 2. DSAnpUG-EU als deutsches Ausführungsgesetz.
  - §§ 4 – 30 DSG[244] idF. BGBl. I Nr. 14/2019 für Österreich.
- Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (ePrivacy-RL) mit Ergänzung durch die Citizens' Rights Richtlinie 2009/136/EG (Cookie-RL) als nicht-unmittelbar anwendbarer auf Art 114 AEUV[245] gestützter Sekundärrechtsakt der Europäischen Union:
  - umgesetzt in Deutschland in den §§ 88 ff TKG 2004 für geschäftsmäßig Telekommunikationsdienste u. -netze. (§§ 11 ff TMG nach hA keine Umsetzung der ePrivacy-RL 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG[246]).
  - umgesetzt in Österreich in den §§ 92 ff TKG 2003 für Betreiber von öffentlichen Kommunikationsdiensten bzw. -netzen und § 96 Abs 3 TKG 2003[247] (idF. BGBl. I Nr. 78/2018) zusätzlich für Dienste der Informationsgesellschaft.

Mit (möglichem) Inkrafttreten der geplanten unmittelbar anwendbaren Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-VO) ab dem Jahr (tbd.) würde sich folgendes Bild ergeben:

- Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) sowie
  - §§ 1 – 44 BDSG idF. 2. DSAnpUG-EU Deutschland.
  - §§ 4 – 30 DSG[248] idF. BGBl. I Nr. 14/2019 Österreich.
- Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-VO) sowie
  - Ergänzende Bestimmung in den nationalen TKGs in Deutschland u. Österreich.

---

243 Open Systems Interconnection Model (Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur).
244 mit BGBl. I Nr. 120/2017 (Datenschutz-Anpassungsgesetz 2018) an die DSGVO angepasst.
245 ex Art 95 EGV Vertrag von Amsterdam.
246 *European Commission*, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report (2015) 63.
247 mit BGBl. I Nr. 102/2011 erfolgte die Umsetzung des Art 5 Abs 3 ePrivacy-RL 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG in § 96 Abs 3 TKG 2003.
248 BGBl. I Nr. 120/2017 (Datenschutz-Anpassungsgesetz 2018).

C. Jaksch, *Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes*,
AutoUni – Schriftenreihe 143, https://doi.org/10.1007/978-3-658-29450-2_3

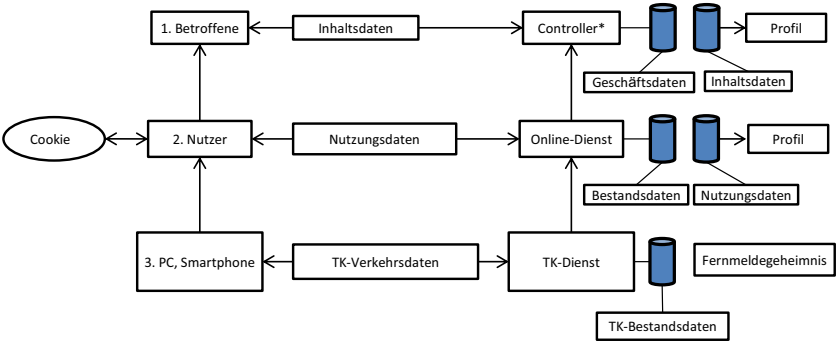
Bevor eine datenschutzrechtliche Analyse der neuen Anforderungen an den IT-gestützten Arbeitsplatzes erfolgen kann, ist es aufgrund der Komplexität des Europäischen Datenschutzrechts erforderlich den sachlichen Anwendungsbereich der ggf. jeweils unterschiedlich anwendbaren Datenschutznormen zu identifizieren.

Zur richtigen Einordnung der sachlichen Anwendungsbereiche der einzelnen Datenschutznormen für private Stellen hat sich das sogenannte 3-Schichten-Modell, welches sich am ISO/OSI Referenzmodell bzw. am TCP/IP-Referenzmodell orientiert, in der datenschutzrechtlichen Literatur etabliert. Damit wird es möglich die unterschiedlichen Anwendungsbereiche der verschiedenen datenschutzrechtlichen Normen voneinander abzugrenzen. Ein Verständnis des 3-Schichten-Modells ist die absolute Voraussetzung für die zutreffende Anwendung der datenschutzrechtlichen Vorschriften, denn Schichtenmodelle machen Modelle und komplexe Gebilde erst sinnvoll überschaubar.[249]

- Schicht 3 (Telekommunikationsebene): Zum Transport der Inhalte wird ein Kommunikationsdienst benötigt, der es möglich macht, beliebige Informationen in beide Richtungen zu transportieren. Die Telekommunikationsebene stellt den Informationstransport sicher, ohne sich um den Inhalt und die Bedeutung der übertragenen Informationen und Daten zu kümmern (Fernmeldegeheimnis).
- Schicht 2 (Interaktionsschicht): Ein Internetnutzer ruft eine Homepage auf, welche Informationen (Bilder, Texte) und Bedienelemente (Buttons, Menüs, Eingabefelder, Links, etc.) enthält. Der Internetnutzer interagiert mit der Homepage in dem er/sie Menüs auswählt, Buttons drückt oder Eingaben in Eingabefeldern durchführt. Alles mit dem was der Internetnutzer auf einer Homepage interagiert, gehört zur Schicht 2 (gesamte Interaktion wie bspw. eingegebenen URLs, die Mausklicks, die gedrückten Buttons, die ausgefüllten Eingabefelder, zeitliche Abfolge einer Interaktion, etc.).
- Schicht 1 (Inhaltsebene): Es geht hier um den konkreten Inhalt, also den Inhalt einer transportierten Nachricht, Datensatz, etc. und nicht um den Informationstransport oder die Interaktion mit einem Dienst der Informationsgesellschaft. Auf der Inhaltsebene der 3. Schicht ist nur der abstrakte Inhalt bzw. die Bedeutung einer Kommunikation interessant.

Die drei Schichten spielen in der Form zusammen, dass jede Schicht die nötigen Mittel bereitstellt, die die darüber liegende Schicht zur Umsetzung ihrer eigenen Leistung braucht. Es ist auch möglich, dass Schicht 3 (Telekommunikationsebene) unmittelbar auf Schicht 1 (Inhaltsebene) aufbaut (z.B. Versand einer E-Mail über einen klassischen E-Mail Dienst).[250]

249 *Schleipfer*, Das 3-Schichten-Modell des Multimediadatenschutzrechts, DuD 2004, 727 ff.
250 *Schleipfer*, Das 3-Schichten-Modell des Multimediadatenschutzrechts, DuD 2004, 727 ff.



* Verantwortlicher gemäß Art 4 Nr 7 Datenschutz-Grundverordnung (EU) 2016/679

Abbildung 2: *Schleipfer*, Das 3-Schichten-Modell des Multimediadatenschutzrechts, DuD 2004, 727 (732).

Auf Schicht 3 (Telekommunikationsebene) fallen folgende Daten an[251]:

- *Telekommunikationsbestanddaten*: Hierbei handelt es sich um Daten eines Teilnehmers, die für die Begründung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden wie bspw. Name bei natürlichen und juristischen Personen, Adresse, Rufnummer, Anschrift, etc.
- *Telekommunikationsverkehrsdaten*: Hierbei handelt es sich um Daten, die zum Zwecke der Weiterleitung einer Nachricht verarbeitet werden (Wer hat wann, wo, mit wem kommuniziert?). Verkehrsdaten dürfen grundsätzlich nicht länger als technisch erforderlich gespeichert werden und sind sofort zu löschen. Sie unterliegen dem (einfachgesetzlichen) Fernmeldegeheimnis.[252] Nach BGH (mA auf Österreich übertragbar) dürfen bei Vorliegen einer Flatrate die entsprechenden Verkehrsdaten eines Teilnehmers maximal 7 Tage zu IT-Sicherheitszwecken vorratsgespeichert werden[253] bzw. wenn keine Flatrate vorliegt, dürfen (nur) die für die Abrechnung erforderlichen Verkehrsdaten für 3 Monaten bis max. 6 Monaten[254] weitergespeichert werden. Jede andere Form von Vorratsdatenspeicherung ist im Anwendungsbereich der EU-GRC und des Unionsrechts (ePrivacy-Richtlinie) nach Rechtsprechung des EuGH[255] rechtswidrig.
- *Telekommunikationsinhaltsdaten*: Es handelt sich um die übertragenen Inhalte.

Unter Schicht 2 (Interaktionsschicht): fallen alle Daten im Rahmen der Nutzung von Informations- und Kommunikationsangeboten an (Dienste der Informationsgesellschaft):

- *Bestandsdaten* z.B. Benutzername, Kennwort, Name, Adresse, Rufnummer, etc.

---

251 *Schleipfer*, Das 3-Schichten-Modell des Multimediadatenschutzrechts, DuD 2004, 727 ff.
252 Vgl. § 88 dTKG 2004 bzw. § 93 öTKG 2003.
253 BGH Urteil v. 13.01.2011, Az. III ZR 146/10 Rn 28; BGH Urteil v. 03.06.2014, Az. III ZR 391/13; OLG Köln Urteil v. 14.12.2015, 12 U 16/13.
254 vgl. § 97 Abs 3 Satz 2 dTKG 2004 bzw. vgl. § 99 Abs 2 öTKG 2003.
255 EuGH Urteil v. 21.12.2016, C-203/15, C-698/15.

- *Nutzungsdaten* sind alle Daten, die bei einer dynamischen Nutzung von Internetdiensten anfallen (z.B. Mausklicks, Mausbewegungen, Tastatureingaben, Seitenabrufe, URLs inkl. Parameter, Cookie Werte, Konfigurationsdaten wie bspw. Betriebssystem, Sprache, Version, Auslesen der MAC Adresse, etc., Session ID, Session Kontext, Zeitpunkte aller Nutzungsvorgänge;).

Unter Schicht 1 (Inhaltsschicht) fallen alle Inhaltsdaten:

- Sämtliche Daten (*Inhaltsdaten*) über die ein Nutzer oder Unternehmen verfügt und die nicht den Schichten 2 und Schicht 3 zuzuordnen sind (bei einem Nutzer angekommene E-Mails, abgespeicherte Dateien, Fotos, etc.).

Das Schichten-Modell erfordert ein Denken iSv. „sowohl als auch" und nicht ein Denken iSv. „entweder oder". Denn ein und die gleichen Daten können auf verschiedenen Schichten verschiedene Rollen spielen, bspw. je nach datenschutzrechtlicher Rolle der konkret handelnden Akteure. Daten wandern dabei durch die Schichten und werden damit juristisch jeweils unterschiedlich eingestuft. Nach *Greve* ist im Rahmen einer datenschutzrechtlichen Prüfung wie folgt vorzugehen:

- Feststellung welche Dienstleistung datenschutzrechtlich geprüft werden soll.
- Feststellung welche Protokolle der IT-Technologie dafür benötigt werden.
- Feststellung welche Daten in den jeweiligen Protokollen verarbeitet werden.
- Ablesen aus der Tabelle, welcher technischen Schicht und damit datenschutzrechtlicher Ebene (3-Schichten-Modell) diese Daten zuzuordnen sind.
- Ausarbeiten wie diese Daten gemäß DSGVO und nationalem TKG bzw. ePrivacy-VO datenschutzrechtlich zu behandeln sind.[256]

Das bedeutet bspw. konkret: Wenn ein Nutzer eine Online Registrierung durchführt, werden seine Daten zuerst beim TK-Provider als Verkehrs- und Inhaltsdaten durch die TK-Infrastruktur übertragen (Schicht 3); → Anschließend werden diese Daten zunächst zu Nutzungsdaten (z.B. Agieren auf der Homepage) und nach der Registrierung bei einem Online-Dienst werden die Daten anschließend zu Bestandsdaten (Schicht 2). → Bei einem Vertragsabschluss werden die Daten zu konkreten Bestandteilen eines Vertragsverhältnisses und damit zu sogenannten Inhaltsdaten (Schicht 1).[257]

Hinsichtlich der Datenverarbeitung von IT-gestützt arbeitenden Beschäftigten ist dieses Modell von Relevanz, da zu prüfen ist, welche (EU-)Normen für den IT-gestützten Arbeitsplatz überhaupt zur Anwendung gelangen können und welche nicht.[258]

256 *Greve*, Datenschutz in der Unternehmenskommunikation. Eine technologiebasierte rechtliche Zuordnung (2006) 52.
257 *Schleipfer*, Das 3-Schichten-Modell des Multimediadatenschutzrechts, DuD 2004, 727 (732 f.).
258 *Greve*, Datenschutz in der Unternehmenskommunikation. Eine technologiebasierte rechtliche Zuordnung (2006) 48.

Tabelle 1: Einordnung OSI Modell

Datenschutz	**Rechtlich**			**Technische Beschreibung**		
3-Schichten	**DE**	**AT**	**DE / AT**	**ISO/OSI-Modell**	**TCP/IP-Modell**	**Internet**
	seit 25.05.2018		**ab *tbd***			
1. Inhaltschicht	DSGVO		DSGVO	Inhalt	Inhalt	Inhalt
2. Anwendungsschicht	***strittig*** nur DSGVO *oder §§ 12, 15 TMG ggf. Ausnahmen § 11 Abs 1 Nr 1 – 2 TMG*	§ 96 Abs 3 öTKG + DSGVO *nur DSGVO: – kein Dienst Inform. gesell. – kein öffentl. TK-Dienst*	Art 8 ff. ePrivacy-VO + DSGVO **bzw.** *bei öffentl. elektr. Komm – Diensten Art 5 ff. Privacy-VO*	7. Anwendungsschicht	4. Anwendungsschicht	HTTP 259 SMTP 260 DNS 261 FTP 262
				6. Darstellungsschicht	*im TCP/IP Modell nicht vorgesehen*	
				5. Sitzungsschicht		
3. Transportschicht	§§ 88 ff dTKG *nur DSGVO wenn kein geschäft. (öffentl.) TK-Dienst.*	§§ 92 ff öTKG *nur DSGVO wenn kein gewerb. öffentl. TK-Dienst.*	Art 5 ff ePrivacy-VO *nur DSGVO wenn kein öffentl. elektr. Komm – Dienst.*	4. Transportschicht	3. Transportschicht (TCP)	TCP 263
				3. Netzwerk- bzw. Vermittlungsschicht	2. Internetschicht (IP)	IP 264
				2. Sicherungs- bzw. Verbindungsschicht	1. Verbindungsschicht	LAN Ethernet Token Ring ISDN 265
				1. physikal- bzw. Bitübertragungsschicht		

259 HTTP: Hypertext Transfer Protocol.
260 SMTP: Simple Mail Transport Protocol.
261 DNS: Domain Name Service.
262 FTP: File Transfer Protocol.
263 TCP: Transmission Control Protocol.
264 IP: Internet Protocol.
265 ISDN: es handelt sich um ein digitales Telefonnetz für den Transfer von Daten über Telefonleitungen (Integrated Services Digital Netzwork).

3.2 Transportschicht

3.2.1 Europäische Union

Art 5 ff ePrivacy-RL 2002/58/EG (idF. RL 2009/136/EG):

Die aktuell in Kraft stehende ePrivacy-RL 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG (vgl. Art 3 ff) regelt primär die Vertraulichkeit der Daten auf der Transportebene (Fernmeldegeheimnis, Verkehrsdaten, Standortdaten, Sicherheit von TK-Diensten und Netzsicherheit, etc.), also die Schichten 1. – 4. des OSI/ISO Referenzmodels bzw. die Schichten 1. – 3. des TCP/IP Modells.

Nachfolgend zu prüfen ist ihre Anwendbarkeit auf Arbeitgeber und Beschäftigte in einem Unternehmen:

Die ePrivacy-Richtlinie 2002/58/EG hat ihren Ursprung im *„Vorschlag der Kommission für eine Europäische Richtlinie zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen"*[266] aus dem Jahr 1990. Im Rahmen der Liberalisierung und Privatisierung des Europäischen Telekommunikationsmarktes sollte allen europäischen Nutzern von öffentlich zugänglichen Telekommunikationsdiensten ein einheitliches Basisschutzniveau garantiert werden.[267] Gerade noch rechtzeitig für die eingeleitete europaweite TK-Liberalisierung Mitte/Ende der 1990er Jahre (Börsengang Deutsche Telekom AG in Frankfurt und New York mit 18. November 1996[268] bzw. Börsengang der Telekom Austria AG in Wien und New York mit 21. November 2000[269]) wurde die Europäische Datenschutzrichtlinie für die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation 97/66/EG (auch als „ISDN-Richtlinie" bezeichnet) mit 15. Dezember 1997 erlassen. Die nationale Umsetzung erfolgte in Deutschland schon vorab in den §§ 85, 89 TKG 1996[270] sowie der Telekommunikations-Datenschutzverordnung – TDSV[271] bzw. in Österreich in den §§ 87 ff TKG 1997[272]. Im Jahr 2002 wurde aufgrund der massiven technischen Veränderungen durch das Internet die bestehende ISDN-Richtlinie 97/66/EG durch die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (ePrivacy-Richtlinie) ersetzt. Sie musste an die Entwicklung der Märkte und Technologien für elektronische Kommunikationsdienste angepasst werden.[273] National wurde die ePrivacy-Richtlinie 2002/58/EG in Deutschland in den §§ 88 ff

266 KOM(90) 314 endg. 80 ff.
267 KOM(90) 314 endg. 7; KOM(87) 290 endg. 1 ff.
268 *Obertreis* in tagesspiegel.de (18.11.2016) 20 Jahre Telekom-Börsengang – Eine Aktie fürs Volk, abrufbar unter: http://www.tagesspiegel.de/wirtschaft/20-jahre-telekom-boersengang-eine-aktie-fuers-volk/14852362.html (zuletzt abgerufen am 20.06.2019).
269 *Standard.at* (19.11.2010), Telekom Austria ging vor 10 Jahren an die Börse, abrufbar unter: http://derstandard.at/1289608302892/Telekom-Austria-ging-vor-10-Jahren-an-die-Boerse (zuletzt abgerufen am 20.06.2019).
270 Telekommunikationsgesetz (BGBl. 1996 I. 1120).
271 Telekommunikations-Datenschutzverordnung – TDSV (BGBl. 2000 I. 1740).
272 BGBl. I Nr. 100/1997.
273 Erwägungsgrund 4 ePrivacy-Richtlinie 2002/58/EG.

TKG 2004[274] bzw. in Österreich in den §§ 92 ff TKG 2003[275] umgesetzt. Im Jahr 2009 erfolgte durch die Richtlinien 2009/136/EG (Citizen's Rights Directive)[276] und die Richtlinie 2009/140/EG (Better Regulation Directive)[277] nochmals eine starke Novellierung im Datenschutz (z.B. hinsichtlich „Cookies"), in der IT-Sicherheit und Netzsicherheit im TK-Bereich, was zu erhöhten Aktivitäten des deutschen[278] und österreichischen[279] Gesetzgebers in den jeweils nationalen TKGs führte.[280]

Normadressaten der ePrivacy-Richtlinie sind insofern „öffentlich zugängliche elektronische Kommunikationsdienste" (Art 3 ePrivacy-Richtlinie 2002/58/EG).

Bis zum 20. Dezember 2020 wird gemäß Art 125 Satz 3 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 iVm. Art 2 Satz 1 ePrivacy-RL 2002/58/EG der Begriff „elektronischer Kommunikationsdienst" im Sinne des Art 2 lit c TK-Rahmen-Richtlinie 2002/21/EG definiert als *„gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen;"* Der Tatbestand „öffentlich zugänglich" wird bis 20. Dezember 2020 in Art 2 lit d TK-Universaldienste Richtlinie 2002/22/EG als *„einen der Öffentlichkeit zur Verfügung gestellten Dienst"* definiert.

Ab 21. Dezember 2020 gelten dann Bezugnahmen auf die vier EG-Telekom-Richtlinien 2002/19/EG, 2002/20/EG, 2002/21/EG, 2002/22/EG als Bezugnahmen auf die Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972.[281] Der Begriff „elektronischer Kommunikationsdienst" wird ab 21. Dezember 2020 in Art 2 Nr 4 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 deutlich erweitert definiert als *„gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbrachte Dienste, die — mit der Ausnahme von Diensten, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben — folgende Dienste umfassen:*

a) „Internetzugangsdienste" im Sinne der Begriffsbestimmung des Artikels 2 Absatz 2 Nummer 2 der Verordnung (EU) 2015/2120,

b) interpersonelle Kommunikationsdienste und

c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden;"

---

274 Telekommunikationsgesetz (BGBl. 2004 I. 1190).
275 BGBl. I Nr. 70/2003.
276 Erwägungsgrund 3 Citizen's Rights Richtlinie 2009/136/EG.
277 Erwägungsgrund 3 Better Regulation Richtlinie 2009/140/EG.
278 Gesetz zur Änderung telekommunikationsrechtlicher Regelungen vom 09.05.2012 (BGBl 2012 I. 958); BT-Drs. 17/5707, 1 ff.
279 BGBl. I Nr. 102/2011; ErlRV 1389 BlgNR 24. GP 23 ff.
280 *Forgó/Otto*, Datenschutzrechtliche Neuerungen im TK-Recht, ecolex 2011,177; *Körber*, TKG-Novelle 2011, MMR 2011, 215.
281 Art 125 Satz 3 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 iVm. Art 2 Satz 1 ePrivacy-RL 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG.

Die Definition des Tatbestandsmerkmals „öffentlich zugänglich“ wird ähnlich wie bisher (Art 2 lit c TK-Universaldienste Richtlinie 2002/22/EG) im neuen Art 2 Nr 32 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 als *„einen der Öffentlichkeit zur Verfügung gestellten elektronischen Kommunikationsdienst“* definiert.

Erster Prüfschritt hinsichtlich der Anwendbarkeit der ePrivacy-Richtlinie ist folglich, ob ein der Öffentlichkeit zur Verfügung gestellter Dienst vorliegt (Art 3 ePrivacy-RL 2002/58/EG). Dies ist mA klar aus den folgenden Gründen zu verneinen:

Ein „elektronischer Kommunikationsdienst“ ist gemäß den europarechtlichen Definitionen[282] dann „öffentlich zugänglich“, wenn der Dienst einem unbeschränkten Personenkreis zur Verfügung gestellt wird, also nicht nur einem begrenzten Personenkreis wie Beschäftigten eines Unternehmens (geschlossene Benutzergruppe).[283] Ein „Telekommunikationsnetz“ ist „öffentlich zugänglich“, wenn das Netz einem unbestimmten offenen Personenkreis zur Verfügung steht. Firmennetzwerke sind demgemäß keine öffentlichen „Telekommunikationsnetze“, wenn sie lediglich den Firmenangehörigen zur Verfügung stehen (Corporate Networks).[284] *Lust* stellt mangels klarer europarechtlicher Definition der „öffentlichen Zugänglichkeit“ tendenziell weniger auf die physische Erreichbarkeit ab, sondern mehr auf die Zugänglichkeit in der Form, dass jedermann Verträge mit dem Kommunikationsdienst abschließen kann (iSv. Angebot an die Öffentlichkeit)[285]: *„Ein über das Netz erbrachter Kommunikationsdienst ist dann öffentlich zugänglich, wenn er der Allgemeinheit, dh einem unbestimmten Personenkreis angeboten wird.“*[286] Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen in Münster führte im Jahr 2002 zum Merkmal „öffentlich zugänglich“[287] aus: *„Steht fest, dass die Bereitstellung von Sprachtransport und -vermittlung nicht für beliebige natürliche oder juristische Personen erfolgt, liegt zwangsläufig ein Angebot für eine geschlossene Benutzergruppe* (…) *vor.* (…) *Denn auch soweit Sprachtransport und -vermittlung im Rahmen der Kommunikation nach außen erbracht wird, geschieht das "für" die Mitglieder der geschlossenen Benutzergruppe als Empfänger einer so gewollten zweckgerichteten Leistung. Die Sprachübertragung und -vermittlung wird nicht deshalb für beliebige ...* (sic!) *Personen bereit gestellt, weil Mitglieder der geschlossenen Benutzergruppe mit beliebigen Gesprächsempfängern im Außenverhältnis kommunizieren können. Denn die zu betrachtende vertragliche Leistung der Antragstellerin wird nicht für die Außenstehenden als Leistungsempfänger bereitgestellt.* (…) *Selbst zur Geltungszeit der Telekommunikations-Verleihungsverordnung*[288] *verlor eine geschlossene Gruppe von Benutzern nicht deshalb das Merkmal der Geschlossenheit, weil sie auch Au-*

282 Art. 2 lit. c TK-Universaldienste Richtlinie 2002/22/EG bzw. Art 2 Nr 32 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972.

283 *Fetzer* in Arndt/Fetzer/Scherer/Graulich (Hrsg), TKG^2 (2015) § 3 Rn 89 ff.

284 *Fetzer* in Arndt/Fetzer/Scherer/Graulich (Hrsg), TKG^2 (2015) § 3 Rn 89 ff.

285 *Lust* in Riesz/Schilchegger (Hrsg), TKG (2016) § 3 Rn 184; *Bräuer* in in Riesz/Schilchegger (Hrsg), TKG (2016) § 69 Rn 1.

286 *Lust* in Riesz/Schilchegger (Hrsg), TKG (2016) § 3 Rn 197.

287 § 3 Nr 15 dTKG 1996 (= Art 2 lit d TK-Universaldienste Richtlininie = heute § 3 Nr 17 dTKG 2004).

288 Verordnung zur Öffnung von Märkten für Dienstleistungen sowie zur Regelung von Inhalt, Umfang und Verfahren der Verleihung im Bereich der Telekommunikation (BGBl. 1995 I. 1434-1441).

ßenkommunikation betrieb (…) *Im Übrigen verlangte der Begriff der geschlossenen Benutzergruppe selbst zur Geltungszeit der Telekommunikations-Verleihungsverordnung bei wortlautorientiertem Verständnis keine Kommunikation allein innerhalb der Gruppe."*[289] Das bedeutet, dass bei der Bereitstellung für eine geschlossene Benutzergruppe auch im Rahmen deren Außenkommunikation Adressat und Leistungsempfänger nur allein die geschlossene Benutzergruppe bleibt, womit allein aus der Möglichkeit zur Außenkommunikation kein „öffentlich zugänglicher" Dienst entsteht.[290] Erwägungsgrund 55 der Citizens' Rights Richtlinie 2009/136/EG präzisierte den Anwendungsbereich der ePrivacy-Richtlinie nochmals im Jahr 2009: *„Im Einklang mit den Zielen des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste sowie den Grundsätzen der Verhältnismäßigkeit und Subsidiarität und im Bemühen um Rechtssicherheit und Effizienz für die europäischen Unternehmen wie auch für die nationalen Regulierungsbehörden stellt die Richtlinie 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation) auf öffentliche elektronische Kommunikationsnetze und -dienste ab und findet keine Anwendung auf geschlossene Benutzergruppen oder Unternehmensnetze."*

Demgemäß ist der europäische Datenschutzrechtsrahmen für die elektronische Kommunikation nicht auf einen Arbeitgeber von IT-gestützt arbeitenden Beschäftigten anwendbar, denn ein solches Unternehmen stellt nachvollziehbar keinen *„öffentlich zugänglichen Telekommunikationsdienst"* iSd. Art 3 ePrivacy-Richtlinie 2002/58/EG[291] bereit.[292] Das Tatbestandsmerkmal der *„öffentlichen Zugänglichkeit"* ist nicht erfüllt, wenn die Dienste nur einer geschlossenen Benutzergruppe (Beschäftigte) bzw. internen Unternehmensnetzen und eben nicht jedermann iSv. „öffentlich zugänglich" zur Verfügung gestellt (iSv. angeboten[293]) werden.[294] Eine Anwendbarkeit scheidet somit bereits nach dem ersten Prüfschritt mit der Festellung der mangelnden öffentlichen Zugänglichkeit aus.

Daran ändern auch die gemäß Art 2 Nr 4 lit a–c Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 geänderten Legaldefinitionen des „elektronischen Kommunikationsdienstes" nichts, auf welche Art 2 Satz 1 ePrivacy-RL 2002/58/EG gemäß Art 125 Satz 3 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 ab 21. Dezember 2020 verweisen wird.

---

289 Oberverwaltungsgericht für das Land Nordrhein-Westfalen, Beschluss v. 13. März 2002, Az. 13 B 32/02 Rn 7 ff; aA *Schütz* in Geppert/Schütz (Hrsg), Beck'scher TKG-Kommentar[4] (2013) § 6 Rn 52 – 53; *Lünenbürger/Stamm* in Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018) § 3 Rn 41.

290 Oberverwaltungsgericht für das Land Nordrhein-Westfalen, Beschluss v. 13. März 2002, Az. 13 B 32/02 Leitsatz 3; *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 f.

291 Art 3 ePrivacy-RL 2002/58/EG iVm. Art 2 lit c TK-Rahmen-Richtlinie 2002/21/EG iVm. Art 2 lit d TK-Universaldienste Richtlinie 2002/22/EG bzw. ab 21. Dezember 2020 Art 2 Nr 4 iVm. Nr 32 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972.

292 *Heun* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) vor § 88 TKG Rn 16 ff; *Heun/Assion* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) Art 95 Rn 10 ff; Rn 19; *Art 29 Datenschutzgruppe*, WP 36 (2000) 3; *Art 29 Datenschutzgruppe*, WP 126 (2006) 3.

293 *Lust* in Riesz/Schilchegger (Hrsg), TKG (2016) § 3 Rn 197.

294 ErwGr 55 Citizens' Rights Richtlinie 2009/136/EG; Art. 2 lit. c TK-Universaldienste Richtlinie 2002/22/EG bzw. Art 2 Nr 32 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972.

Zudem ergibt sich aus der jüngsten EuGH Rechtsprechung vom Juni 2019 die Schlussfolgerung, dass allein durch das Bereitstellen der Internetnutzung am Arbeitsplatz vom Arbeitgeber noch kein Dienst bereitgestellt wird, der „ganz oder überwiegend in der Übertragung von Signalen" besteht (Art 2 lit c TK-Rahmen-Richtlinie 2002/21/EG / Art 2 Nr 4 lit c Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972).[295]

Zwischenstand:

Aus rein europarechtlicher Sicht ist die ePrivacy-Richtlinie 2002/58/EG nicht auf Arbeitgeber anwendbar. Dies wird auch nach dem 21. Dezember 2020 mit der Anwendbarkeit der geänderten Begriffsbestimmungen des „elektronischen Kommunikationsdienstes" in Art 2 Nr 4 lit a – c Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 und dem Verweis darauf in Art 2 Satz 1 ePrivacy-RL 2002/58/EG iVm. Art 125 Satz 3 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 so bleiben. Auch bei erlaubter Privatnutzung der IKT Infrastruktur durch Beschäftigte (= geschlossene Benutzergruppen bzw. Unternehmensnetze) liegt aus europarechtlicher Sicht (Art 3 ePrivacy-RL) kein „öffentlich zugänglicher elektronischer Kommunikationsdienst" vor.[296] *Holländer* führt aus: *„Für geschlossene Benutzergruppen – wie beispielsweise rein innerbetriebliche Unternehmensnetze (bei der gestatteten Privatnutzung betrieblicher TK-Anlagen) – ist diese Richtlinie nicht anwendbar* (…). *In diesen Fällen muss auf die DS-GVO zurückgegriffen werden."*[297]

Im Verhältnis Arbeitgeber zu Beschäftigte – unabhängig davon ob den Beschäftigten die Privatnutzung der IKT Infrastruktur erlaubt ist oder nicht – ist auf der Transportebene aus europäischer Perspektive ausschließlich die DSGVO anwendbar. [298]

Art 5 ff ePrivacy-VO idF. EU-Kommission (Januar 2017):

Am 12. Oktober 2016 präsentierte die EU-Kommission den ersten Teil ihres neuen regulativen Konzepts für den Bereich der elektronischen Kommunikation. Dieser beinhaltet eine umfangreiche neue Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972, welche den bisherigen Rechtsrahmen der elektronischen Kommunikation (insbesondere Zugangsrichtlinie 2002/19/EG, Genehmigungsrichtlinie 2002/20/EG, Rahmenrichtlinie 2002/21/EG, Universaldienstrichtlinie 2002/22/EG, Citizens' Rights Richtlinie

295 EuGH Urteil v. 13.06.2019, C-193/18 („Google GMail") Rn 34 f.

296 ErwGr 55 Citizens' Rights Richtlinie 2009/136/EG*; Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht28. Edition (Stand: 01.05.2019) Art 95 Rn 4; *Nebel/Richter*, Datenschutz bei Internetdiensten nach der DS-GVO – Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD 2012, 407 (408); *Grussmann/Honekamp* in Geppert/Schütz (Hrsg), Beck'scher TKG-Kommentar4 (2013) B. Europarechtliche Grundlagen Rn 142; *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 ff.

297 *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4.

298 *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4. *Nebel/Richter*, ZD 2012, 407 (408); *Grussmann/Honekamp* in Geppert/Schütz (Hrsg), Beck'scher TKG-Kommentar[4] (2013) B. Europarechtliche Grundlagen Rn 142; *Brodil*, Die Registrierung von Vermittlungsdaten im Arbeitsverhältnis, ZAS 2004/01, 17 (19); *Art 29 Datenschutzgruppe*, WP 36 (2000) 3; *Art 29 Datenschutzgruppe*, WP 126 (2006) 3; *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 ff.

2009/136/EG und Better-Regulation Richtlinie 2009/140/EG) ab 21. Dezember 2020 ersetzt.[299] Hintergrund der Neugestaltung ist die gesellschaftliche Entwicklung, dass Verbraucher und Unternehmen zunehmend auf Daten- und Internetzugangsdienste setzen anstatt auf traditionelle Kommunikationsdienste (Telefon, SMS). Ziel dieses Reformvorhabens ist es, die seit dem Jahr 2009 stattgefundenen Veränderungen im Telekommunikationsbereich auch im Rechtsrahmen für die elektronische Kommunikation abzubilden.[300]

Am 10. Januar 2017 präsentierte die EU-Kommission den zweiten Teil ihres Reformvorhabens, nämlich die Ablösung der bisherigen ePrivacy-RL 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG durch eine unmittelbar anwendbare ePrivacy-VO. Bisher gibt es noch keiner finale Einigung zu diesem Reformvorhaben ePrivacy-VO. Ziel der ePrivacy-VO ist es, die europäischen ePrivacy Vorschriften gleichmäßig auf alle Anbieter funktional gleichwertiger Dienste (Telekom-Provider und OTT-Dienste[301]) anzuwenden. Die ePrivacy-VO regelt:

- die Verarbeitung elektronischer Kommunikationsdaten, die in Verbindung mit der Bereitstellung und Nutzung öffentlich zugänglicher elektronischer Kommunikationsdienste erfolgt (Art 5 – Art 7 iVm. ErwGr 13 letzer Satz iVm. Art 2 Abs 2 lit c ePrivacy-VO);
- die Verarbeitung von Informationen, die sich auf die Endeinrichtungen der Endnutzer beziehen oder von den Endeinrichtungen der Endnutzer verarbeitet werden (Art 8 ePrivacy-VO);
- das Inverkehrbringen von Software, die elektronische Kommunikation ermöglicht, darunter das Abrufen und Darstellen von Informationen aus dem Internet (Art 10 ePrivacy-VO);
- die Bereitstellung öffentlich zugänglicher Verzeichnisse der Nutzer elektronischer Kommunikation und die Anzeige von Rufnummern (Art 12 ff ePrivacy-Verordnung);
- die Übermittlung von Direktwerbung an Endnutzer mittels elektronischer Kommunikation (Art 16 ePrivacy-VO).

Nachfolgend zu prüfen ist ihre Anwendbarkeit auf Arbeitgeber und Beschäftigte in einem Unternehmen:

Gemäß Art 2 Abs 2 lit c ePrivacy-VO gilt die ePrivacy-VO nicht für elektronische Kommunikationsdienste, die nicht öffentlich zugänglich sind. Dies bekräftigt ErwGr 13: *„Diese Verordnung sollte dagegen keine Anwendung auf geschlossene Gruppen von Endnutzern (z. B. Unternehmensnetze) finden, bei denen der Zugang auf die Angehörigen des Unternehmens beschränkt ist."*[302] Daher bleibt es aus europarechtlicher Sicht wie bisher bei der Nichtanwendbarkeit der europäischen ePrivacy Normen zur Vertraulichkeit der Kommunikation auf Arbeitgeber – unabhängig davon ob sie die Privatnutzung erlauben oder nicht

299 COM(2016) 590 final., 2; Art 124, Art 125, Art 126 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972.

300 COM(2016) 590 final., 2; *Husemann* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 3 Rn 19 ff; *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 43 ff.

301 *Over-the-top content* (OTT) bezeichnet die Übermittlung und den Verkauf von Video- und Audioinhalten über Internetzugänge, ohne dass ein Internet-Service-Provider in die Kontrolle oder Verbreitung der Inhalte involviert ist.

302 ErwGr 13 letzter Satz iVm. Art 2 Abs 2 lit c ePrivacy-Verordnung.

(ErwGr 13 letzter Satz iVm. Art 2 Abs 2 lit c ePrivacy-Verordnung). Ein Arbeitgeber ist kein öffentlich zugänglicher elektronischer Kommunikationsdienst, da (auch bei erlaubter Privatnutzung) nur eine Bereitstellung an die geschlossene Benutzergruppe der Beschäftigten des Unternehmens erfolgt (siehe oben). Demgemäß scheidet gemäß ErwGr 13 letzter Satz iVm. Art 2 Abs 2 lit c ePrivacy-VO auf jeden Fall eine Anwendbarkeit der Art. 5 (*Vertraulichkeit elektronischer Kommunikationsdaten*), Art 6 (*Erlaubte Verarbeitung elektronischer Kommunikationsdaten*), Art 7 (*Speicherung und Löschung elektronischer Kommunikationsdaten*) ePrivacy-VO auf Arbeitgeber aus, da diese Bestimmungen die Verarbeitung elektronischer Kommunikationsdaten in Verbindung mit der Bereitstellung und Nutzung öffentlich zugänglicher elektronischer Kommunikationsdienste regeln (vgl. Art 2 Abs 1 Alt 1 iVm. Art 2 Abs 2 lit c ePrivacy-VO).[303]

Art 5 ff ePrivacy-VO idF. EU-Parlament (Oktober 2017):

Für das Europäische Parlament ist der Entwurf der EU-Kommission zu wenig weitgehend. Gemäß Art 4 Abs 3 lit aa) ePrivacy-VO idF. EU-Parlament[304] zählen nach Ansicht des Europäischen Parlaments zu den elektronischen Kommunikationsdiensten iSd. ePrivacy-VO idF. EU-Parlament auch solche, die zwar nicht öffentlich zugänglich sind, aber über die der Zugang zu einem öffentlich-zugänglichen elektronischen Kommunikationsnetz bereitgestellt wird (das heißt das EU-Parlament folgt hier offenbar nicht der Auslegung der „öffentlichen Zugänglichkeit" iSd. *Oberverwaltungsgericht für das Land Nordrhein-Westfalen*[305], *Lust*[306] bzw. ErwGr 55 Citizens' Rights Richtlinie 2009/136/EG). Trotz Ausnahme von öffentlich zugänglichen elektronischen Kommunikationsdiensten (Art 2 Abs 2 lit c ePrivacy-VO idF. EU-Parlament), wäre ein Arbeitgeber, der seinen Beschäftigten nicht nur ein Intranet bereitstellt (ErwGr 13 ePrivacy-VO idF. EU-Parlament), sondern gleichzeitig auch Zugang zum offenen Internet ermöglicht (Zugang zu einem öffentlich-zugänglichen elektronischen Kommunikationsnetz bereitgestellt) ggf. doch wieder im Anwendungsbereich der Art 5 – Art 7 ePrivacy-VO idF. EU-Parlament. Geschützt wären die „Nutzer" (Art 4 Abs 3 lit af ePrivacy-VO idF. EU-Parlament), also diejenigen, die den elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nehmen (Beschäftigte). Im Gegensatz zum bisherigen deutschen Telekommunikationsrecht, wo das „geschäftsmäßige Anbieten" in § 3 Nr 10 TKG 2004 legaldefiniert wird als *„das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht"*, fehlt im europäischen Telekommunikationsrecht in Art 2 lit c TK-Rahmenrichtlinie 2002/21/EG bzw.

303 *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 66; Rn 72; *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4; *Nebel/Richter*, ZD 2012, 407 (408); *Brodil*, ZAS 2004/01, 17 (19); *Grussmann/Honekamp* in Geppert/Schütz (Hrsg), Beck'scher TKG-Kommentar[4] (2013) B. Europarechtliche Grundlagen Rn 142; *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 ff.

304 *Europäisches Parlament*, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)).

305 Oberverwaltungsgericht für das Land Nordrhein-Westfalen Beschluss v. 13.03.2002, Az. 13 B 32/02 Rn 7 ff.

306 *Lust* in Riesz/Schilchegger (Hrsg), TKG (2016) § 3 Rn 197.

Art 2 Nr 4 lit b und lit c Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 das bisherige rein deutsche Tatbestandsmerkmal „Angebot für Dritte". In Extremauslegung könnten damit die Art 5 – Art 7 ePrivacy-VO idF. EU-Parlament auch gelten, wenn nicht nur die Privatnutzung erlaubt wäre, da die Begriffsbestimmung des „Nutzers"[307] gleichrangig auf die private oder geschäftliche Nutzung abstellt. In Deutschland erfolgt über das Tatbestandsmerkmal „Angebot für Dritte" (§ 3 Nr 10 TKG 2004) die Abgrenzung: Ist keine Privatnutzung erlaubt, liegt kein „Angebot an Dritte" vor; ist die Privatnutzung erlaubt, liege ein „Angebot an Dritte" (Beschäftigte) durch den Arbeitgeber vor.[308]

Bei Anwendbarkeit der ePrivacy-VO idF. EU-Parlament bei strengster Auslegung des „Nutzer"-Begriffs (Art 4 Abs 3 lit af ePrivacy-VO idF. EU-Parlament) dürfte ein Arbeitgeber – unabhängig von der Privatnutzung – Kommunikationsmetadaten (Protokolldaten) nur dann verarbeiten:

- zur Durchführung der Übermittlung der Kommunikation (Art 6 Abs 1 lit a ePrivacy-VO idF. EU-Parlament),
- zur Aufrechterhaltung und Wiederherstellung der Verfügbarkeit, Integrität, Vertraulichkeit und Sicherheit des jeweiligen Kommunikationsdienstes (Art 6 Abs 1 lit b ePrivacy-VO idF. EU-Parlament),
- zur Erkennung der betrügerischen Nutzung elektronischer Kommunikationsdienste (Art 6 Abs 2 lit b ePrivacy-VO idF. EU-Parlament),
- Einwilliung des jeweiligen Nutzers (Art 6 Abs 1 lit c ePrivacy-VO idF. EU-Parlament)

Kommunikationsinhaltsdaten dürfte ein Arbeitgeber nur dann verarbeiten:

- zur Durchführung der Übermittlung der Kommunikation (Art 6 Abs 1 lit a ePrivacy-VO idF. EU-Parlament),
- zur Aufrechterhaltung und Wiederherstellung der Verfügbarkeit, Integrität, Vertraulichkeit und Sicherheit des jeweiligen Kommunikationsdienstes (Art 6 Abs 1 lit b ePrivacy-VO idF. EU-Parlament),
- zum alleinigen Zweck der Bereitstellung eines bestimmten, vom Nutzer angeforderten Dienstes, wenn der jeweilige Nutzer seine Einwilligung zur Verarbeitung seiner elektronischen Kommunikationsinhalte gegeben hat und der Dienst ohne die Verarbeitung der Inhaltsdaten vom Anbieter nicht erbracht werden könnte (Art 6 Abs 3 lit a ePrivacy-VO idF. EU-Parlament),
- Einwilligung aller jeweiligen Nutzer (Art 6 Abs 3 lit b ePrivacy-VO idF. EU-Parlament);

Ein Arbeitgeber hätte nur eine Erlaubnis „Kommunikationsinhalte" und „Kommunikationsmetadaten" ohne Einwilligung der Beschäftigten zu verarbeiten: **1.** für die Zwecke der technischen Durchführung der Übertragung; **2.** für die IT-Sicherheit; und **3.** „Kommunikationsmetadaten" dürften zusätzlich durch den Arbeitgeber auch zur Aufdeckung einer

307 Art 4 Abs 3 lit af ePrivacy-VO idF. EU-Parlament bzw. Art 2 lit a ePrivacy-Richtlinie 2002/58/EG.

308 *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (2016), 4; *Elschner* in Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019) Teil 22.1 Elektronische Arbeitnehmerüberwachung Rn 76 ff.

betrügerischen Nutzung verarbeitet werden. Eine Einsicht in (dienstliche) eMails ohne Einwilligung des Nutzers wäre für den Arbeitgeber grundsätzlich nicht mehr möglich, was einen schweren Eingriff in sein Grundrecht auf Eigentum darstellen würde (Art 17 EU-GRC, Art 1 ZP. 1 EMRK, Art 14 dGG, Art 5 öStGG 1867).[309]

Zwischenstand:

Die Art 5 – Art 7 ePrivacy-VO idF. EU-Kommission (Januar 2017) würden auf Arbeitgeber keine Anwendung finden, es würde weiterhin nur die DSGVO und das jeweils anwendbare nationale Anpassungsgesetz zur DSGVO für Arbeitgeber gelten.[310]

Anderes gilt gemäß ePrivacy-VO idF. EU-Parlament (Oktober 2017), sie würde auch auf geschlossene Benutzergruppen zur Anwendung gelangen, wenn dabei auch der Zugang zu einem öffentlichen Kommunikationsnetz (Internet) ermöglicht wird, was am IT-gestützten Arbeitsplatz der Fall wäre (ErwGr 13 iVm. Art 4 Abs 3 lit aa) ePrivacy-VO idF EU-Parlament).

Die Art 12, Art 13, Art 14 und Art 15 ePrivacy-VO beider Entwürfe sind auf den Arbeitgeber nicht anwendbar, mangels Eigenschaft eines „Betreibers öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste" bzw. eines „Betreibers öffentlich zugänglicher Verzeichnisse" iSd. Richtlinie über den europäischen Kodex für die elektronische Kommunikation (EU) 2018/1972.

Die Frage ob weitere Bestimmungen der ePrivacy-VO (insb. Art 8, Art 10 u. Art 16) auf der Dienste-Ebene auf den Arbeitgeber anwendbar sind, wird an entsprechender Stelle (Diensteebene) weiter unten besprochen (siehe **Kapitel 3.3.1**).

3.2.2 Deutschland – §§ 88 ff TKG 2004

In Deutschland wurde die ePrivacy-Richtlinie 2002/58/EG überschießend in den §§ 88 ff TKG 2004 umgesetzt („gold plating").

Normadressat des Fernmeldegeheimnisses gemäß § 88 TKG 2004 ist nicht nur ein *„öffentlich zugänglicher Telekommunikationsdienst"* (vgl. Definition in § 3 Nr 17a TKG 2004) iSd. Art 3 ePrivacy-Richtlinie 2002/58/EG iVm. Art 2 lit c TK-Rahmen-Richtlinie 2002/21/EG iVm. Art 2 lit d TK-Universaldienste Richtlinie 2002/22/EG, sondern darüberhinausgehend *„jeder Diensteanbieter"* (§ 3 Nr 6 TKG 2004), der einen *„Telekommunikationsdienst"* (§ 3 Nr 24 TKG 2004) *„geschäftsmäßig"* – also im Sinne eines nachhaltigen Angebots von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht (§ 3 Nr 10 TKG 2004) – *„erbringt"* (§ 3 Nr 6 lit a TKG 2004) *„oder an der Erbringung solcher Dienste mitwirkt"* (§ 3 Nr 6 lit b TKG 2004). Der genaue Umfang des Anwendungsbereichs wird in der BT Drucksache 13/3609 S. 53 zum TKG 1996 und in der BT-Drs. 13/8016

309 *Europäisches Parlament*, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)).

310 *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 66; Rn 72; *Brodil*, ZAS 2004/01, 17 (19).

S. 29 zur Neufassung des § 206 StGB erläutert und sieben Jahre später in der BT Drucksache 15/2316 S. 87 zum TKG 2004 nochmals vollumfänglich bestätigt:

BT-Drs 13/3609 S. 53 im Jahr 1996 zu § 85 TKG 1996 (heute § 88 TKG 2004):

„(…) In Absatz 2 wird der Kreis der Verpflichteten bestimmt: Verpflichtet ist jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. (…) *Auch ein ohne Gewinnerzielungsabsicht erfolgendes, auf Dauer angelegtes Angebot von Telekommunikationsdiensten verpflichtet zur Wahrung des Fernmeldegeheimnisses. Dem Fernmeldegeheimnis unterliegen damit z. B. Corporate Networks, Nebenstellenanlagen in Hotels und Krankenhäusern, Clubtelefone und Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind. Nicht unter das Fernmeldegeheimnis fallen dagegen i. d. R. private Endgeräte, Haustelefonanlagen und hauseigene Sprechanlagen. Wegen der Komplexität und der Vielfalt denkbarer Konfigurationen bei Telekommunikationsanlagen, die künftig bestehen werden, ist eine enumerative Abgrenzung des Schutzbereichs des Fernmeldegeheimnisses nicht möglich. Im Einzelfall wird deshalb auf das schutzwürdige Vertrauen der Beteiligten abzustellen sein.“*[311]

BT-Drs 13/8016 S. 29 im Jahr 1997 zur Neufassung des § 206 StGB:
„(…) Die auf das „gèschäftsmäßige" Erbringen von Telekommunikationsdiensten abhebende Formulierung lehnt sich an § 3 Nr. 5 TKG [*1996*] *an. Mit ihrer Verwendung auch in dieser Sanktionsvorschrift wird die Dekkungsgleichheit des strafrechtlichen Adressatenkreises mit den gemäß § 85 Abs. 2 TKG* [*1996*] *zur Geheimhaltung verpflichteten Personen gewährleistet. Nach der Definition in § 3 Nr. 5 TKG* [*1996*] *ist „geschäftsmäßiges Erbringen von Telekommunikationsdiensten" das „nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht". Damit werden z. B. auch Telekommunikationsnetze für geschlossene Benutzergruppen (Corporate Networks), über die möglicherweise in Zukunft erhebliche Teile der geschäftlichen Telekommunikation abgewickelt werden, vom Schutzbereich der Vorschrift umfaßt. Die in Absatz 1 vorgeschlagene Bestimmung des Kreises der Normadressaten orientiert sich auch hinsichtlich des Postwesens an der (künftigen) bereichsspezifischen Regelung: Ein am 5. März 1997 vom Bundeskabinett beschlossener Regierungsentwurf für ein neues Postgesetz (PostG) unterwirft solche Personen der Geheimnispflicht, die Postdienste „geschäftsmäßig" erbringen oder daran mitwirken (§ 39 Abs. 2 i. V. m. § 38 PostG-E).“*[312]

BT-Drs 15/2316 S. 87 im Jahr 2004 zu § 88 TKG 2004:
„Die Vorschriften zum Fernmeldegeheimnis werden unverändert übernommen (…).[313]

Nach dem Willen des historischen deutschen Gesetzgebers soll damit eindeutig auch jeder Arbeitgeber in Deutschland, der seinen Beschäftigten die Privatnutzung erlaubt, dem Fernmeldegeheimnis gemäß § 88 TKG 2004 und der Strafbestimmung des § 206 StGB unterworfen sein. Das bedeutet, dass ein gewöhnlicher Arbeitgeber, der seinen Beschäftigten die Privatnutzung der IKT Infrastruktur gestattet, die Tatbestandsmerkmale *„geschäftsmäßiges*

311 BT-Drs. 13/3609, 53.
312 BT-Drs 13/8016, 29.
313 BT-Drs 15/2316, 87.

Erbringen von Telekommunikationsdiensten" erfüllen würde, also ein *„nachhaltige[s] Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht"* (§ 3 Nr. 10 TKG 2004) macht. Die bisher in Deutschland höchstgerichtlich ungeklärte Frage ist nun, ob bei der erlaubten privaten IKT Nutzung damit einem *„Dritten"* (= Beschäftigter, wenn er privat betriebliche IKT-Infrastruktur nutzt) *„nachhaltig"* (im Sinne von dauerhaft) Telekommunikationsdienste vom Arbeitgeber als „Diensteanbieter" bereitgestellt werden (?). Die deutschen Datenschutzaufsichtsbehörden (Düsseldorfer Kreis)[314] sehen wie die BT Drucksache 13/3609 S. 53 (§ 85 TKG 1996), BT-Drs 13/8016, S. 29 (§ 206 StGB) und BT Drucksache 15/2316 S. 87 (§ 88 TKG 2004) bei der erlaubten Privatnutzung eine nachhaltige dauerhafte geschäftsmäßige Bereitstellung von Telekommunikationsdiensten durch den Arbeitgeber als damit gleichzeitigen „Diensteanbieter" (§ 3 Nr 6 iVm. § 3 Nr 24 TKG 2004) an seine Beschäftigten als dann gleichzeitigen „Dritten" (§ 3 Nr 10 TKG 2004). Nach Ansicht der deutschen Datenschutzaufsichtsbehörden und *Elschners* wird der Arbeitgeber insofern eindeutig zum Telekommunikationsdienstanbieter.[315]

Dies soll nach *Graulich, Schmidt* und anderen Meinungen in der Literatur zum TKG 2004 hingegen nicht der Fall sein.[316] In der arbeitsrechtlichen Judikatur wird diese ablehnende Ansicht *Graulichs* von den Arbeitsgerichten bisher umfassend geteilt (vgl. LAG Niedersachsen Urteil v. 31.05.2010 12, Az. Sa 875/09; LAG Berlin-Brandenburg Urteil v. 16. Februar 2011, Az. 4 Sa 2132/10, LAG Hamm Urteil v. 10. Juli 2012, Az. 14 Sa 1711/10, LAG Berlin-Brandenburg Urteil v. 14. Januar 2016, Az. 5 Sa 657/15, ArbG Weiden Urteil vom 17.05.2017, 3 Ga 6/17). Der Arbeitgeber wurde in all diesen bisherigen arbeitsrechtlichen Entscheidungen nicht als ein „Diensteanbieter" iSd. § 88 TKG 2004 angesehen, auch wenn die Privatnutzung im Unternehmen erlaubt war.

Bestärkt wird die Ansicht der deutschen LAGs mit dem Blick auf die europarechtlichen Grundlagen der §§ 88 ff TKG 2004, nämlich der ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG (siehe oben). Dort gibt es kein Erfordernis das Fernmeldegeheimnis auch auf Arbeitgeber im Falle der Privatnutzung auszudehnen, denn die europäische ePrivacy-Richtlinie ist nur an „öffentlich zugängliche elektronische Kommunikationsdienste und -netze" adressiert[317] (Art 3 ePrivacy-Richtlinie), nicht aber an gewöhnliche Arbeitgeber, die die Privatnutzung erlauben.[318] Insofern stellen die §§ 88 ff TKG 2004

314 *Datenschutzkonferenz (Düsseldorfer Kreis),* Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (2016) 7 f.

315 *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (2016) 4; *Elschner* in Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019) Teil 22.1 Elektronische Arbeitnehmerüberwachung Rn 76 ff.

316 *Graulich* in *Arndt/Fetzer/Scherer/Graulich*, (Hrsg.), TKG[2], (2015) § 88 Rn. 81; *Schmidt,* Datenschutz für „Beschäftigte (2016) 106; *Herrmann/Soiné*, Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, NJW 2011, 2922 (2928).

317 ErwGr 55 Citizens' Rights Richtlinie 2009/136/EG; Art. 3 ePrivacy-Richtlinie 2002/58/EG.

318 ErwGr 55 Citizens' Rights Richtlinie 2009/136/EG; *Grussmann/Honekamp* in Geppert/Schütz (Hrsg), Beck'scher TKG-Kommentar[4] (2013) B. Europarechtliche Grundlagen Rn 142; *Brodil*, ZAS 2004/01, 17 (19).

eine überschießende Umsetzung der ePrivacy-Richtlinie dar[319] („gold plating"), welche auch mit der europarechtlichen Auslegung der Art 7 lit f DSRL 95/46/EG gemäß der Rechtsprechung des EuGH seit 2011 und der des Bundesarbeitsgerichts BAG seit 2017 in Konflikt tritt. Der EuGH hatte in den Entscheidungen C-582/14 („Breyer"), C-468/10 („ASNEF") und C-469/10 („FECEMD") festgestellt, dass pauschale Verarbeitungsverbote europarechtlich gegen Art 7 lit f DSRL 95/46/EG verstoßen. Ein solches pauschales Verabeitungsverbot stellt § 88 TKG 2004 – mangels europarechtlicher Grundlage – hinsichtlich der Ausdehnung seiner Anwendung auch auf Arbeitgeber dar. Dieser Rechtsprechung zu pauschalen Verarbeitungsverboten hat sich das BAG im Jahr 2017 angeschlossen und pauschale Verarbeitungsverbote im Arbeitsverhältnis (in diesem Fall bei § 32 Abs 1 Satz 2 BDSG idF. BGBl. 2009 I. 2814) als mit Art 7 lit f EG-Datenschutzrichtlinie 95/46/EG als unvereinbar angesehen. Damit ließ sich vor diesem Hintergrund dieser EuGH und BAG Rechtsprechung die Anwendung des unionsrechtlich nicht gedeckten pauschalen Verarbeitungsverbotes § 88 TKG 2004 im Arbeitsverhältnis entsprechend bereits vor Geltung der DSGVO nicht mehr halten (*Wybitul*).[320]

Aus der jüngsten EuGH Rechtsprechung vom Juni 2019 kann zudem schlussgefolgert werden, dass durch die Erlaubnis der Privatnutzung am Arbeitsplatz vom Arbeitgeber allein noch kein Dienst bereitgestellt wird, der „ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze" besteht (§ 3 Nr 24 TKG 2004).[321]

Seit 25. Mai 2018 genießt die DSGVO umfassenden Anwendungsvorrang. Ausgenommen werden gemäß Art 95 DSGVO nur natürliche oder juristische Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union. Diesen soll durch die DSGVO keine zusätzlichen Pflichten auflegt werden, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen (vgl. Art 95 DSGVO iVm. Art 3 ff ePrivacy-Richtlinie). Dies bedeutet, dass in Deutschland alle TK-Datenschutzvorschriften anwendbar bleiben, die auf der ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG beruhen und dasselbe Ziel wie die DSGVO verfolgen, was grundsätzlich auf die §§ 88 ff TKG 2004 zutrifft. Da aber die §§ 88 ff. TKG 2004 nicht nur an öffentlich zugängliche Telekommunikationsdienste adressiert sind, sondern zusätzlich auch jeden deutschen nicht-öffentlichen geschäftlichen Diensteanbieter erfassen, werden die §§ 88 ff TKG 2004 in diesem Rahmen hinsichtlich personenbezogener Daten vom Anwendungsvorrang der DSGVO verdrängt (vgl. Art 95

---

319 *Heun* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) vor § 88 TKG Rn 16 ff; *Heun/Assion* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) Art 95 Rn 10 ff; Rn 19; *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 66 ff; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 211 ff; *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4 f (*„deutsche Überregulierungen werden (…) von der DS-GVO verdrängt"*).

320 *Wybitul*, § 32 BDSG: Bundesarbeitsgericht klärt wichtige Fragen des Beschäftigtendatenschutzes, abrufbar unter: http://hoganlovells-blog.de/2017/09/03/%c2%a7-32-bdsg-bundesarbeitsgericht-klaert-wichtige-fragen-des-beschaeftigtendatenschutzes/# (zuletzt abgerufen am 20.06.2019); BAG Urteil v. 29.06.2017, Az. 2 AZR 597/16; *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer BDSG [aF][4] (2014) § 32 BDSG [aF] Rn 22.

321 EuGH Urteil v. 13.06.2019, C-193/18 („Google GMail") Rn 34 f.

DSGVO).[322] *Geminn/Richter* führen aus: *„Für ein Vertraulichkeitsgebot für nicht-öffentliche TK-Netze und -dienste bietet Art. 5 RL 2002/58/EG aber keine Grundlage. Insoweit unterliegt die Vorschrift dem Anwendungsvorrang der Verordnung."*[323] Diese Ansicht bestätigte im Juni 2018 auch die *Deutsche Bundesregierung*, dass für die Verarbeitung personenbezogener Daten im Rahmen von nicht-öffentlichen Telekommunikationsnetzen seit 25. Mai 2018 uneingeschränkt die DSGVO gilt.[324]

Im Referentenentwurf des BMI für das 2. DSAnpUG-EU vom 21. Juni 2018 fand sich eine gesetzliche Klarstellung zur Anpassung des TKG 2004 an die DSGVO (vgl. § 91 TKG 2004-E idF. Referentenentwurf 2. DSAnpUG-EU vom 21. Juni 2018). Der Anwendungsbereich des TKG 2004 sollte auch direkt im Gesetzestext des TKG 2004 auf öffentlich zugängliche Telekommunikationsdienste in öffentlichen Telekommunikationsnetzen reduziert werden:[325] „*§ 91 wird neu gefasst. § 91 Satz 1 beschreibt den Anwendungsbereich des telekommunikationsrechtlichen Datenschutzes. Da Abschnitt 2 zukünftig fachspezifische Datenschutzregelungen enthalten wird, die auf die Richtlinie 2002/58/EG zurückgehen, wird der Anwendungsbereich auf die in der Richtlinie allein adressierten öffentlichen Telekommunikationsnetze beschränkt. Für die bisher in § 91 Absatz 2 angesprochenen geschlossene Benutzergruppen öffentlicher Stellen der Länder findet sich keine Grundlage in der Richtlinie 2002/58/EG. Diese fallen daher zukünftig aus dem Anwendungsbereich dieses Abschnittes heraus.*"[326] Die im Referentenentwurf vom 21. Juni 2018 noch vorgesehene gesetzliche Anpassung direkt in § 91 TKG 2004-E idF. Referentenentwurf 2. DSAnpUG-EU[327] wurde in der BT-Drs. 19/4674 vom 01. Oktober 2018 zum 2. DSAnpUG-EU wieder herausgenommen, inhaltlich geht aber auch die BT-Drs. 19/4674 vom 01. Oktober 2018 weiterhin davon aus, dass das TKG 2004 nur noch auf öffentlich zugängliche elektronische Kommunikationsdienste anwendbar ist und, dass hinsichtlich nicht-öffentlich zugänglicher elektronischer Kommunikationsdienste seit 25. Mai 2018 ausschließlich die DSGVO gilt. Zur Novelle des § 9 Abs 1 Satz 1 BDSG idF. BT-Drs. 19/4674, S. 25 (2. DSAnpUG-EU), mit einer Klarstellung der Zuständigkeit des BfDI, wird erläutert:[328] *„Die Regelung trägt dem Umstand Rechnung, dass das Telekommunikationsgesetz (TKG) künftig nur noch Re-*

322 *Heun* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) vor § 88 TKG Rn 16 ff; *Heun/Assion* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) Art 95 Rn 10 ff; Rn 19; *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 68; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 211; Rn 224; *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4; *Kühling/Raab* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 95 Rn 11; *Nebel/Richter*, ZD 2012, 407 (408); *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 ff.

323 *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 220.

324 BT-Drs. 19/2653, 9 (Antwort BReg auf Frage 20).

325 *Bundesministeriums des Innern, für Bau und Heimat*, Referentenentwurf vom 21.06.2018, Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU, 180; 241; 491.

326 *Bundesministeriums des Innern, für Bau und Heimat*, Referentenentwurf vom 21.06.2018, Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU, 491.

327 *Bundesministeriums des Innern, für Bau und Heimat*, Referentenentwurf vom 21.06.2018, Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU, 180; 491.

328 BT-Drs. 19/4674, 25; 210.

gelungen zur Datenverarbeitung in Umsetzung der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) enthält. Bereiche, die durch die Verordnung (EU) 2016/679 unmittelbar geregelt werden, werden hingegen aus dem TKG gestrichen."[329] Das 2. DSAnpUG-EU wurde am 27. Juni 2019 gemäß dem oben besprochenen Gesetzentwurf der BT-Drs. 19/4674 und der Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung in der BT-Drs 19/5414 mit Maßgabe kurzfristiger kleinerer Anpassungen durch die BT-Drs. 19/11181, ohne konkrete gesetzestextliche Anpassung der §§ 91 ff TKG 2004 an die DSGVO, vom Bundestag verabschiedet.[330]

Die Diskussion über die Anwendbarkeit des §§ 88 ff TKG 2004 im Arbeitsverhältnis bei erlaubter Privatnutzung erledigt sich letztlich – mit oder ohne einer direkten gesetzlichen Klarstellung in § 91 TKG 2004 – auch in Deutschland seit Geltung der DSGVO durch ihren Anwendungsvorrang (Art 95 DSGVO) und der aktuellen EuGH Rechtsprechung.[331]

Der Anwendungsbereich des § 206 StGB (Verletzung des Fernmeldegeheimnisses) ist mA entsprechend der EuGH, BGH und BAG Judikatur zu pauschalen Verarbeitungsverboten[332] und der strafrechtlichen BGH Judikatur zur europarechtskonformen Auslegung von Datenschutzbestimmungen in Strafverfahren[333] – entgegen der anderslautenden BT-Drs 13/8016, S. 29 aus dem Jahr 1997 zu § 206 StGB – seit 25. Mai 2018 europarechtskonform[334] anzuwenden, also nur auf rein öffentlich zugängliche Telekommunikationsdienste und nicht auf Arbeitgeber, welche ihren Beschäftigten die Privatnutzung erlauben.[335]

Kommt man in europarechtskonformer Auslegung zum Ergebnis, dass die §§ 88 ff TKG 2004 iVm. § 206 StGB nicht auf Arbeitgeber anwendbar sind, auch wenn der Arbeitgeber die Privatnutzung erlaubt[336], haben deutsche Arbeitgeber auch in Zukunft bei der Kontrolle

---

329 BT-Drs. 19/4674, 210; *Bundesministeriums des Innern, für Bau und Heimat*, Referentenentwurf vom 21.06.2018, Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU, 241.

330 BGBl. 2019 I. 1626; *Bundestag.de* (27.06.2019), Bundestag stimmt zwei Gesetzen zum Datenschutzrecht zu, abrufbar unter: https://www.bundestag.de/dokumente/textarchiv/2019/kw26-de-datenschutz-649218 (zuletzt abgerufen am 27.06.2019); BT-Drs. 19/11181.

331 *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4 f; *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 68; Rn 72; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 211; Rn 224; *Nebel/Richter*, ZD 2012, 407 (408); *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 ff; EuGH Urteil v. 13.06.2019, C-193/18 („Google GMail") Rn 34 f.

332 EuGH Urteil v. 19.10.2016, C-582/14 („Breyer"); BGH Urteil v. 16.05.2017, Az. VI ZR 135/13; EuGH Urteil v. 24.11.2011, C-468/10 („ASNEF"), C-469/10 („FECEMD"); BAG Urteil v. 29.06.2017, Az. 2 AZR 597/16.

333 BGH Urteil v. 04.06.2013, Az. 1 StR 32/13, Rn 70 ff.

334 *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 219 ff; *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 ff.

335 Oberverwaltungsgericht für das Land Nordrhein-Westfalen, Beschluss v. 13.März 2002, Az. 13 B 32/02; *Schütz* in Geppert/Schütz (Hrsg), Beck'scher TKG-Kommentar[4] (2013) § 6 Rn 43 ff; aA *Lünenbürger/Stamm* in Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018) § 3 Rn 40 f.

336 LAG Niedersachsen Urteil v. 31.05.2010 12, Az. Sa 875/09; LAG Berlin-Brandenburg Urteil v. 16. Februar 2011, Az. 4 Sa 2132/10), LAG Hamm Urteil vom 10. Juli 2012, Az. 14 Sa 1711/10 und LAG Berlin-Brandenburg Urteil v. 14. Januar 2016, Az. 5 Sa 657/15; BAG Urteil v. 29.06.2017, Az. 2 AZR 597/16; EuGH Urteil v. 24.11.2011, C-468/10 („ASNEF"), C-469/10

der IKT Nutzung von Mitarbeitern weiterhin aber folgende Strafvorschriften im Zusammenhang mit elektronischer Kommunikation streng zu beachten:

- *§ 201 Abs 2 Nr 1 StGB (Verletzung der Vertraulichkeit des Wortes):* strafbar ist das unbefugte Abhören (z.B. Telefongespräch) das nicht zur Kenntnis des Abhörenden (Arbeitgeber) bestimmten nichtöffentlich gesprochenen Wortes eines anderen (Beschäftigten) mit einem Abhörgerät (Freiheitsstrafe bis zu drei Jahren).
- *§ 201 Abs 1 Nr 1 u. Nr 2 StGB (Verletzung der Vertraulichkeit des Wortes):* strafbar ist das unbefugte Aufnehmen des nichtöffentlich gesprochenen Wortes eines anderen auf einem Tonträger (Nr 1.) und sowie (Nr 2) ist das Gebrauchen bzw. das Zugänglichmachen der Aufnahme an einen Dritten (Freiheitsstrafe bis zu drei Jahren).
- *§ 202b StGB (Abfangen von Daten) ggf. iVm. § 202a StGB (Ausspähen von Daten):* strafbar ist das unbefugte Abfangen von nicht für den Abfangenden (Arbeitgeber) bestimmte Daten (z.B. Telefon, Fax, eMail, LAN Verbindungen, VPN-Verbindungen, etc.) aus einer nichtöffentlichen Datenübermittlung unter Anwendung von technischen Mitteln (*illegal interception* iSd. Art 3 Convention on Cybercrime 2001). Die Bestimmung § 202b StGB entspricht dabei beim unbefugten Abhören von Telefongesprächen der Strafbestimmung § 201 Abs 2 Nr 1 StGB, weil dies dort ebenso erfasst wird. Aufgrund der Subsidiaritätsklausel gelangt in einem solchen Fall § 202b StGB nicht zur Anwendung.[337] Die Abgrenzung zwischen § 202b StGB (*Abfangen von Daten*) mit § 202a StGB (*Ausspähen von Daten*), liegt konkret darin, dass bei § 202b StGB das Tatobjekt alle Daten einer nichtöffentlichen und auch nicht besonders gesicherten Datenübertragung sind, leitungsgebunden oder drahtlos und auch innerhalb von privaten Netzwerken, bei § 202a StGB geht es nur um gesicherte Daten („Zugangssicherung").[338] Daher hat die Norm § 202b StGB (Freiheitsstrafe bis zu zwei Jahre) gegenüber der strengeren Norm § 202a StGB (Freiheitsstrafe bis zu drei Jahre) nur ergänzende Funktion für jene Fälle nicht besonders gesicherter Datenübertragungen, die mangels „Zugangssicherung" (Verschlüsselung) nicht durch § 202a StGB geschützt wären (Subsidiaritätsklausel des § 202b StGB).[339]
- *§§ 148 Abs 1 Nr 1 iVm. 89 TKG 2004 (Empfang fremder Telekommunikationsvorgänge und die Weitergabe):* strafbar ist hier der unbefugte Empfang fremder Telekommunikationsvorgänge und die Weitergabe von Informationen hierüber an Dritte, soweit die Nachrichten nicht ausdrücklich für die empfangende Funkanlage (Arbeitgeber) bestimmt sind. Die Abhör- und Weitergabeverbote des § 89 TKG 2004 schützen nur Individualkommunikationsvorgänge mit Funkanlagen, also nicht Funkaussendungen, die für die Allgemeinheit oder einen unbestimmten Personenkreis sind.[340] Im Unterschied zu § 202b StGB gelten die §§ 148 Abs 1 Nr 1 iVm. 89 TKG 2004 nur für Funkanlagen

(„FECEMD"); EuGH Urteil v. 19.10.2016, C-582/14 („Breyer"); BGH Urteil v. 16.05.2017, Az. VI ZR 135/13; BGH Urteil v. 04.06.2013, Az. 1 StR 32/13, Rn 70 ff.

337 BT-Drs. 16/3656, 11; *Fischer* in Fischer (Hrsg), Strafgesetzbuch mit Nebengesetzen[66] (2019) § 202b Rn 10.

338 *Fischer* in Fischer (Hrsg), Strafgesetzbuch mit Nebengesetzen[66] (2019) § 202b Rn 2 f; *Gutmann/Knierim* in Müller/Schlothauer/Schütrumpf (Hrsg), MAH Strafverteidigung[2] (2014) § 51 Rn 38 ff.

339 BT-Drs. 16/3656, 18; *Fischer* in Fischer (Hrsg), Strafgesetzbuch mit Nebengesetzen[66] (2019) § 202b Rn 10.

340 *Bock* in Geppert/Schütz (Hrsg) Beck'scher TKG-Kommentar[4] (2013) § 89 Rn 1 ff.

einschließlich WLAN-Verbindungen, sie treten im Falle gleichzeitiger Anwendbarkeit gegenüber § 202b StGB (Abfangen von Daten) zurück.[341]

- *§ 42 BDSG* belegt besonders schwerwiegende Datenschutzverletzungen mit Kriminalstrafe:
  - § 42 Abs 1 BDSG bestraft die wissentliche gewerbsmäßige unberechtigte Übermittlung oder Zugänglichmachung von nicht allgemein zugänglichen personenbezogenen Daten.
  - § 42 Abs 2 BDSG bestraft die unrechtmäßige Verarbeitung oder Erschleichung von nicht allgemein zugänglichen personenbezogenen Daten gegen Entgelt oder in der Absicht sich oder einen anderen zu bereichern oder einen anderen zu schädigen.[342]

Zwischenstand:

Für deutsche Arbeitgeber werden die Bestimmungen der §§ 88 ff TKG 2004 iVm. § 206 StGB durch den Anwendungsvorrang der DSGVO umfassend und mA rechtssicher verdrängt. Arbeitgeber haben spätestens seit 25. Mai 2018 auf der Transportebene – auch bei erlaubter Privatnutzung – nur noch die DSGVO und das BDSG idF. 2. DSAnpUG-EU zu beachten inkl. der an jedermann adressierten Strafbestimmungen §§ 201, 202a, 202b StGB und § 42 BDSG.

3.2.3 Österreich – §§ 92 ff TKG 2003

In Österreich wurde die ePrivacy-Richtlinie in den §§ 92 ff TKG 2003 umgesetzt. Adressaten des österreichischen Kommunikationsgeheimnisses in § 93 TKG 2003 und den datenschutzrechtlichen Bestimmungen sind in europarechtskonformer Umsetzung *„öffentliche Kommunikationsdienste in öffentlichen Kommunikationsnetzen"* (vgl. § 92 Abs 1 Satz 1 TKG 2003).[343] Der Begriff „Kommunikationsdienst" ist gemäß § 3 Z 9 TKG 2003: *„eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht"*.

Die §§ 92 ff TKG finden auf einen Arbeitgeber, der seinen Mitarbeitern die betriebliche IKT-Infrastruktur auch zur privaten Nutzung zur Verfügung stellt, keine Anwendung, weil:

- der Arbeitgeber bietet keinen *„öffentlichen Kommunikationsdienst"* an, da sich die Bereitstellung der betrieblichen IKT-Infrastruktur nicht an die Öffentlichkeit richtet. Es wird durch die erlaubte Privatnutzung der IKT Infrastruktur nur an den abgegrenzten Nutzerkreis der Beschäftigten ein Kommunikationsdienst zur Verfügung gestellt (vgl. § 3 Z 16 – Z 19 TKG 2003; Art 3 ePrivacy-RL 2002/58/EG iVm. Erwägungsgrund 55 Citizens' Rights Richtlinie 2009/136/EG). Ein Kommunikationsdienst ist dann nicht-

341 *Fischer* in Fischer (Hrsg), Strafgesetzbuch mit Nebengesetzen[66] (2019) § 202b Rn 2; 11.

342 *Ehmann* in Gola/Heckmann (Hrsg), BDSG[13] (2019) § 42 Rn 5 ff.

343 ErlRV 1389 BlgNR 24. GP 24 (*„Zu § 92 Abs. 1: Mit dem eingefügten Satz 1 wird Art. 3 DatenschutzRL für elektronische Kommunikation umgesetzt. Dieser Zusatz soll verdeutlichen, dass auch die telekommunikationsrechtlichen Vorschriften betreffend Datenschutz den Schutz von personenbezogenen Daten gewährleisten sollen. Diese Frage stellt sich zB bei der Auslegung von § 93 TKG 2003, womit das Kommunikationsgeheimnis geschützt wird, oder § 96 TKG 2003, womit Regeln für den Betreiber festgelegt werden, nach welchen Stamm-, Inhalts-, Verkehrsund Standortdaten ermittelt, verarbeitetet oder übermittelt werden dürfen* (…)."

„öffentlich", wenn sich das Angebot nur an einen von vornherein begrenzten Benutzerkreis z.B. der Beschäftigen richtet bzw. in Unternehmensnetzen.[344]

- der Arbeitgeber bietet durch die Bereitstellung der IKT-Infrastruktur an Beschäftigte auch keine *„gewerbliche Dienstleistung"* (iSd. § 3 Z 9 TKG 2003 iVm. § 1 Abs 2 GewO 1994) an.[345]
- aus der jüngsten EuGH Rechtsprechung vom Juni 2019 kann zudem schlussgefolgert werden, dass durch die Erlaubnis der Privatnutzung am Arbeitsplatz vom Arbeitgeber allein noch kein Dienst bereitgestellt wird, der „*ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze* [*besteht*]*"* (§ 3 Z 9 TKG 2003).[346]

In Österreich entschied der Oberste Gerichtshof (OGH 8 ObA 288/01p) dem folgend früh, dass der Arbeitgeber auch dann nicht als Betreiber eines öffentlichen Telekommunikationsdienstes und damit als Normadressat des § 93 Abs 2 iVm. § 108 TKG 2003[347] (gerichtliche Strafbestimmung) anzusehen ist, wenn er den Dienstnehmern das Führen privater Telefongespräche auf seiner Telefonanlage – sei es auch gegen Entgelt – gestattet.[348] Arbeitgeber können damit in keiner Konstellation – auch wenn sie die Privatnutzung ihren Beschäftigten erlauben – dem § 93 Abs 2 TKG 2003[349] ausschließlich an öffentlich zugängliche TK-Betreiber adressierten Kommunikationsgeheimnis (§ 93 Abs 1 TKG 2003[350]) sowie der damit verbundenen Strafnorm (§ 108 TKG 2003[351]) unterliegen.

Arbeitgeber unterliegen folgend nur dem jedermann treffenden Verbot (vgl. § 93 Abs 3 TKG 2003; Art 3 Convention on Cybercrime 2001 – *illegal interception*) des Mithörens, Abhörens, Aufzeichnens, Abfangens oder sonstigen Überwachens von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer, welches durch die an jedermann adressierten Strafnormen in den § 119 StGB[352], § 119a StGB[353] sowie § 120 Abs 1 StGB[354] strafrechtlich sanktioniert wird. Wie in Deutschland[355] überschneiden sich auch in Österreich die beiden

344 *Riesz* in Riesz/Schilchegger (Hrsg), TKG (2016) § 92 Rn 31; *Lust* in Riesz/Schilchegger (Hrsg), TKG (2016) § 3 Rn 184; *Bräuer* in in Riesz/Schilchegger (Hrsg), TKG (2016) § 69 Rn 1. *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 6.34 ff; *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 7.56 f; *Rebhahn*, Mitarbeiterkontrollen am Arbeitsplatz (2009) 72 f; *Hattenberger,* Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 13 ff (20 ff); *Brodil*, ZAS 2004/01, 17 (19).

345 OGH 13.06.2002, 8 ObA 288/01p.

346 EuGH Urteil v. 13.06.2019, C-193/18 („Google GMail") Rn 34 f.

347 vgl. § 206 StGB iVm. § 88 TKG 2004 Deutschland.

348 OGH RIS-Justiz Rechtssatz RS0116693; *Wessely* in Riesz/Schilchegger (Hrsg), TKG (2016) § 93 Rn 7.

349 vgl. § 88 Abs 2 TKG 2004 Deutschland.

350 vgl. § 88 Abs 1 TKG 2004 (Fernmeldegeheimnis) Deutschland .

351 vgl. § 206 StGB (Verletzung des Fernmeldegeheimnisses) Deutschland.

352 vgl. § 201 Abs 2 Nr. 1 StGB (Abhören von Gesprächen) u. § 202b StGB (Abfangen von Daten) Deutschland.

353 vgl. § 202b StGB (Abfangen von Daten) Deutschland.

354 vgl. § 201 Abs 2 Nr. 1 StGB (Abhören von Gesprächen) Deutschland.

355 vgl. § 201 Abs 2 Nr 1 dStGB und § 202b dStGB.

Tatbestände § 119 StGB und § 120 Abs 1 StGB hinsichtlich Abhören von Telefongesprächen. § 119 StGB stellt auf das sich Kenntnisverschaffen vom Inhalt von Nachrichten als Vermittlung von Gedankeninhalten[356] im Wege einer Telekommunikation oder eines Computersystems ab, die durch Benutzen einer auf einer Telekommunikationsanlage oder an einem Computersystem angebrachten Vorrichtung abgefangen werden. § 120 Abs 1 StGB stellt auf das Abhören von nichtöffentlichen und nicht zur Kenntnisnahme des Abhörenden bestimmten Äußerungen durch Benutzen eines Abhörgeräts ab, wobei es sich bei einer „Äußerung" ausschließlich um das „gesprochene Wort" (z.B. Telefongespräche) handelt.[357] Echte Konkurrenz zwischen § 119 StGB und § 120 Abs 1 StGB besteht, wenn eine Abhörvorrichtung an eine Telekommunikationsanlage angebracht wird und darauf ein Tonaufnahmegerät angeschlossen wird, wodurch der Täter vom Inhalt der Nachricht (Telefongespräch[358]) Kenntnis erlangt.[359]

Aus § 120 Abs 2a StGB[360] iVm. § 93 Abs 4 TKG 2003[361] (*Empfang fremder Telekommunikationsvorgänge und die Weitergabe*) ergibt sich das jedermann treffende Verbot, bei unbeabsichtigt empfangenen und nicht für denjenigen/diejenige bestimmten Nachrichten, weder den Inhalt der Nachrichten noch die Tatsache ihres Empfanges aufzuzeichnen bzw. Unbefugten mitzuteilen und diese Kenntnisse auch nicht für irgendwelche Zwecke zu verwerten. Die Nachricht ist sofort zu löschen bzw. auf andere Art zu vernichten.

In § 63 DSG wird die Datenverarbeitung in Gewinn- oder Schädigungsabsicht sanktioniert. Bestraft wird, wer personenbezogene Daten, an denen ein schutzwürdiges Geheimhaltungsinteresse besteht (§ 1 Abs 1 DSG) und, die jemanden ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind, oder die sich jemand widerrechtlich verschafft hat, mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem Grundrecht auf Datenschutz (§ 1 Abs 1 DSG) zu schädigen, selbst benützt, einem anderen zugänglich macht oder veröffentlicht.[362]

Zwischenstand:
Die §§ 92 ff. iVm. § 108 TKG 2003 finden auf österreichische Arbeitgeber auch bei erlaubter Privatnutzung keine Anwendung.[363] Datenschutzrechtlich gilt für Arbeitgeber auf der Transportebene in jedem Fall ausschließlich allein die DSGVO und das DSG.[364] Österreichische Arbeitgeber haben die an jedermann addressierten Strafbestimmungen in den §§ 119, 119a, 120 StGB und § 63 DSG streng zu beachten.

---

356 *Fabrizy*, StGB[13] (2018) § 119 Rn 3.
357 *Tipold* in *Leukauf/Steininger* (Hrsg), Kommentar zum Strafgesetzbuch[4] (2017) § 120 Rn 2.
358 *Fabrizy*, StGB[13] (2018) § 119 Rn 3.
359 *Tipold* in *Leukauf/Steininger* (Hrsg), Kommentar zum Strafgesetzbuch[4] (2017) § 119 Rn 28.
360 vgl. § 148 Abs 1 Nr 1 iVm. § 89 TKG 2004 (Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen) Deutschland.
361 § 89 Satz 2 TKG 2004 Deutschland.
362 *Bresisch/Riedl* in Bresisch/Dopplinger/Dörnhöfer/Kunnert/Riedl (Hrsg), DSG (2018) § 63 Rn 1 ff.
363 OGH 13.06.2002, 8 ObA 288/01p.
364 *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 6.34 ff; *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Daten-

3.3 Diensteebene

3.3.1 Europäische Union

Art 5 Abs 3 ePrivacy-RL 2002/58/EG idF. RL 2009/136/EG

Gemäß der seit dem Jahr 2009 gültigen Fassung des Art 5 Abs 3 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG ist die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines „Teilnehmers" oder „Nutzers" gespeichert sind, nur gestattet, wenn der betreffende „Teilnehmer" oder „Nutzer" auf der Grundlage von klaren und umfassenden Informationen (Art 13 – 14 iVm. Art 94 Abs 2 DSGVO), dazu seine Einwilligung gegeben hat. Hauptanwendungsfall sind „Cookies" sowie „Spyware", „Web-Bugs" und „Hidden Identifiers".[365] Weiterhin ohne Einwilligung erlaubt ist eine technische Speicherung am Endgerät oder der Zugriff auf Informationen, die bereits im Endgerät eines „Teilnehmers" oder „Nutzers" gespeichert sind, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der „Anbieter eines Dienstes der Informationsgesellschaft" (Art 2 lit a E-Commerce-Richtlinie 2001/31/EG iVm. Art 1 Abs 1 lit b Richtlinie 2015/1535/EU), der vom „Teilnehmer"[366] oder „Nutzer"[367] ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.[368]

Die Pflicht aus Art 5 Abs 3 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG zur Einholung einer informierten Einwilligung des Teilnehmers bzw. des Nutzers trifft „jede Rechtsperson" (= öffentliche oder private Rechtsperson, einzelner Programmierer oder Großunternehmen, für die Verarbeitung Verantwortlicher, Auftragsverarbeiter oder Dritter[369]), der Informationen auf Endgeräten von „Teilnehmern" oder „Nutzern" übertragen oder auf diesen Geräten lesen will.[370] Damit wäre grundsätzlich auch jeder Arbeitgeber im Anwendungsbereich der Norm. Die *Art 29 Datenschutzgruppe* führt ein konkretes Anwendungsbeispiel – abseits der Cookie-Thematik – an: *„Eine Autovermietung installiert in ihren Leihwagen intelligente Fahrzeugortungsgeräte. Während die Autovermietung als Eigentümer des Geräts bzw. als Teilnehmer des Ortungsdienstes betrachtet*

---

schutz und Mitarbeiterkontrolle[2] (2018) Rn 7.56 f; *Rebhahn*, Mitarbeiterkontrollen am Arbeitsplatz (2009) 72 f; *Hattenberger* in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 20 ff; *Brodil*, ZAS 2004/01, 17 (19); *Art 29 Datenschutzgruppe*, WP 36 (2000) 3; *Art 29 Datenschutzgruppe,* WP 126 (2006) 3.

365 ErwGr 24 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG; ErwGr 65 Citizens' Rights Richtlinie 2009/136/EG.

366 Art 2 lit k Rahmen-RL 2002/21/EG.

367 Art 2 lit a ePrivacy-RL 2002/58/EG.

368 Art 5 Abs ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights 2009/136/EG; ErwGr 65 Citizens' Rights Richtlinie 2009/136/EG.

369 *Art 29 Datenschutzgruppe*, WP 223 (2014) 16; *Art 29 Datenschutzgruppe*, WP 224 (2014) 8; *Art 29 Datenschutzgruppe*, WP 202 (2013) 9; *Art 29 Datenschutzgruppe*, WP 171 (2010) 10 ff; *Art 29 Datenschutzgruppe*, WP 148 (2008) 14.

370 *Art 29 Datenschutzgruppe*, WP 223 (2014) 16; *Art 29 Datenschutzgruppe*, WP 224 (2014) 8; *Art 29 Datenschutzgruppe*, WP 202 (2013) 9; *Art 29 Datenschutzgruppe*, WP 171 (2010) 10 ff; *Art 29 Datenschutzgruppe*, WP 148 (2008) 14.

wird, gilt die das Fahrzeug mietende Person als der Nutzer des Geräts. Artikel 5 Absatz 3 schreibt vor, dass der Gerätehersteller (mindestens) die Einwilligung des Nutzers (d.h. in diesem Fall der das Fahrzeug mietenden Person) einholt. Darüber hinaus unterliegt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten der das Fahrzeug mietenden Person den besonderen Anforderungen von Artikel 7 der Richtlinie 95/46/EG [= Art 6 Abs 1 DSGVO] "[371]. Dieses Beispiel würde sich auch auf das Arbeitgeber – Beschäftigten-verhältnis bei Dienstfahrzeugen übertragen lassen.

Geschützt werden durch Art 5 Abs 3 ePrivacy-Richtlinie idF. Citizens' Rights Richtlinie:

- „Teilnehmer" (Art 2 lit k Rahmen-RL 2002/21/EG): „*jede natürliche oder juristische Person, die mit einem Anbieter öffentlich zugänglicher elektronischer Kommunikations-dienste einen Vertrag über die Bereitstellung derartiger Dienste geschlossen hat*;"
- „Nutzer" (Art 2 lit a ePrivacy-RL 2002/58/EG): „*eine natürliche Person, die einen öf-fentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäft-liche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben*;"

Weder in Deutschland noch in Österreich wurde diese Bestimmung mit diesem weiten Anwendungsbereich „jede Rechtsperson"[372] (= betrifft auch Arbeitgeber ggü. Beschäftigten als die geschützten „Nutzer") so in nationales Recht umgesetzt. Es erfolgte jeweils entweder nur eine eingeschränkte Umsetzung auf „öffentliche Kommunikationsdienste" und „Dienste der Informationsgesellschaft" wie in Österreich[373] (von EU-Kommission akzeptiert[374]) bzw. gar keine Umsetzung wie in Deutschland.[375]

Von Art 5 Abs 3 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG eindeutig bisher nicht erfasst ist die Erhebung von Informationen, die von den Endgeräten selbst ausgesendet werden (z.B. Daten über das Endgerät selbst, der Typ und Version bzw. Unterversionsidentifikation des Browsers und die ausgewählte Sprache, Betriebssystem und Version, Informationen über installierte Anwenderprogramme, Daten über die Konfiguration des anfragenden Endgeräts, etc.). Die Erhebung solcher von Endgeräten selbst ausgesendeten Informationen unterliegt allein der DSGVO, vorausgesetzt es handelt sich dabei überhaupt um „personenbezogene Daten" (vgl. EuGH[376] und BGH[377]).

Art 5 – Art 7 ePrivacy-VO Entwurf EU-Kommission (Januar 2017)

Gemäß Art 4 Abs 2 ePrivacy-VO idF. EU-Kommission wären auf der Diensteebene nun auch „interpersonelle Kommunikationsdienste" (Art 2 Nr 4 lit b iVm. Nr 7 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972) vom Fernmeldegeheimnis erfasst, die eine interpersonelle oder interaktive Kommunikation lediglich als untrennbar mit einem

371 *Art 29 Datenschutzgruppe*, WP 225 (2014) 17.
372 *Art 29 Datenschutzgruppe,* WP 202 (2013) 9; *Art 29 Datenschutzgruppe*, WP 223 (2014) 16; *Art 29 Datenschutzgruppe*, WP 224 (2014) 8; *Art 29 Datenschutzgruppe*, WP 171 (2010) 10 ff; *Art 29 Datenschutzgruppe*, WP 148 (2008) 14.
373 § 96 Abs 3 TKG 2003 idF. BGBl. I Nr. 102/2011 (aktuell idF. BGBl. I Nr. 78/2018).
374 European Commission, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report (2015) 63 ff.
375 European Commission, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report (2015) 63.
376 EuGH Urteil v. 19.10.2016, C-582/14 („Breyer").
377 BGH Urteil v. 16.05.2017, Az. VI ZR 135/13.

anderen Dienst verbundene Nebenfunktion ermöglichen (OTT-Dienste). Insofern wären die Art 5 – Art 7 ePrivacy-VO idF. EU-Kommission – in Erweiterung ihres Anwendungsbereichs auf OTT-Dienste – ggf. auch hier auf der Diensteebene relevant. Gemäß Art 2 Abs 2 lit c ePrivacy-VO idF. EU Kommission gilt dies aber nur für „öffentlich zugängliche elektronische Kommunikationsdienste" und damit insofern nicht für den Arbeitgeber und unternehmensinterne elektronische Kommunikationsdienste.[378]

Art 5 – Art 7 ePrivacy-VO idF. EU-Parlament (Okotber 2017)

Wie oben ausgeführt, wären auf der Diensteebene auch „interpersonelle Kommunikationsdienste" (Art 2 Nr 4 lit b iVm. Nr 7 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972) erfasst, die eine interpersonelle oder interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene Nebenfunktion ermöglichen (OTT-Dienste).[379] Nach Art 4 Abs 3 lit aa) ePrivacy-VO idF. EU-Parlament zählen zu den elektronischen Kommunikationsdiensten iSd. ePrivacy-VO idF. EU-Parlament auch solche, die zwar nicht öffentlich zugänglich sind, aber über die der Zugang zu einem öffentlich-zugänglichen elektronischen Kommunikationsnetz bereitgestellt wird. Trotz Ausnahme von öffentlich zugänglichen elektronischen Kommunikationsdiensten gemäß Art 2 Abs 2 lit c ePrivacy-VO, wäre ein Arbeitgeber, der seinen Beschäftigten Zugang zum offenen Internet bietet ggf. doch wieder im Anwendungsbereich der Art 5 – Art 7 ePrivacy-VO. Dies könnte auch interpersonelle Kommunikationsdienste (z.B. Chats, Messenger) des Arbeitgebers auf der Dienstebene (OTT-Dienste) erfassen.

Art 8 ePrivacy-VO Entwurf EU-Kommission (Januar 2017)

Die Bestimmung Art 8 ePrivacy-VO ist eine Weiterentwicklung des bisherigen Art 5 Abs 3 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG. Sie behandelt den zweiten Regelungsgegenstand der zukünftigen ePrivacy-VO. Es geht um den Schutz von Informationen in Bezug auf die Endeinrichtungen der Endnutzer (Art 2 Abs 1 Alt 2 ePrivacy-VO). Dieser Regelungsgegenstand betrifft dabei die Schicht 2 (Anwendungsschicht) im 3-Schichten Modell.[380] Art 8 Abs 1 ePrivacy-VO untersagt allgemein jede vom betreffenden Endnutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware soweit nicht einer der dort genannten Erlaubnistatbestände greift (technische Erforderlichkeit, informierte Einwilligung, zur Bereitstellung eines vom Endnutzer gewünschten Dienstes, Messung des Webpublikums). Art 8 Abs 1 ePrivacy-VO orientiert sich am Anwendungsbereich des bisherigen Art 5 Abs 3 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG, welcher bisher grundsätzlich für „jede Rechtsperson", die Informationen auf

378 *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 3 Rn 19 ff; § 8 Rn 47 ff; Rn 68; Rn 72; Rn 118 ff.

379 *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 3 Rn 19 ff; § 8 Rn 47 ff; Rn 118 ff.

380 *Schleipfer*, Das 3-Schichten-Modell des Multimediadatenschutzrechts, DuD 2004, 727 ff.

Endgeräte von Teilnehmern oder Nutzern überträgt oder auf diesen Geräten liest, umfassend gilt (öffentliche oder private Rechtsperson, einzelner Programmierer oder Großunternehmen, für die Verarbeitung Verantwortlicher, Auftragsverarbeiter oder Dritter).[381]

Offen ist die Anwendbarkeit des Art 8 ePrivacy-VO auf Endgeräte am IT-gestützten Arbeitsplatz im Verhältnis Arbeitgeber und Beschäftigte, denn der Anwendungsbereich des Art 8 ePrivacy-VO ist nicht auf öffentlich zugängliche elektronische Kommunikationsdienste beschränkt.[382] Der Anwendungsbereich des Art 8 ePrivacy-VO wird durch die Betroffenengruppe bestimmt: Von Art 8 ePrivacy-VO idF. EU-Kommission wird die Betroffenengruppe der „Endnutzer" (Art 2 Nr 14 Richtlinie Kodex für die elektronische Kommunikation 2018/1972) [383] geschützt. Ein „Endnutzer" wird definiert als „*ein Nutzer, der keine öffentlichen Kommunikationsnetze oder öffentlich zugänglichen elektronischen Kommunikationsdienste bereitstellt."* Nach dem bisherigen Verständnis der Rahmen-Richtlinie 2002/21/EG (in der Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972 werden diese Definitionen inhaltsgleich übernommen) sind „Endnutzer" (Art 2 lit n Rahmen-Richtlinie 2002/21/EG bzw. Art 2 Nr 14 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972) eine Teilgruppe der „Nutzer" (Art 2 lit h Rahmen-Richtlinie 2002/21/EG bzw. Art 2 Nr 13 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972).[384] „Endnutzer" sind bisher diejenige Teilgruppe der „Nutzer" von öffentlich zugänglichen Kommunikationsdiensten (Art 2 lit c Rahmen-Richtlinie 2002/21/EG iVm. Art 2 lit d TK-Universaldienste Richtlinie 2002/22/EG bzw. Art 2 Nr 4 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972), die die Kommunikationsdienste als Endkunden in Anspruch nehmen. Dabei ist es egal, ob es sich um einen privaten Kunden („Verbraucher" iSd. Art 2 lit i Rahmen-Richtlinie 2002/21/EG bzw. Art 2 Nr 15 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972) oder einen geschäftlichen Kunden (Unternehmer, juristische Person) handelt, der die Kommunikationsdienste im Rahmen seiner geschäftlichen Tätigkeit nützt. Mit dem Begriff des „Endnutzers" sind also regelmäßig Personen (natürliche oder juristische) umschrieben, die sich – unabhängig ob als Unternehmen (Betrieb) oder Verbraucher (Privathaushalt) – in der Kundenrolle befinden und eine Leistung für den Eigengebrauch erhalten.[385] Der „Endnutzer" ist der Kunde am Ende der Leistungskette. Dass möglicherweise andere Personen an dem vom „Endnutzer" bezogenen Telekommunikationsangebot teilhaben (z.B. Internetzugang für

381 *Art 29 Datenschutzgruppe*, WP 202 (2013) 9; *Art 29 Datenschutzgruppe*, WP 223 (2014) 16; *Art 29 Datenschutzgruppe*, WP 224 (2014) 8; *Art 29 Datenschutzgruppe,* WP 171 (2010) 10 ff.

382 *Art 29 Datenschutzgruppe* WP 249 (2017) 5.

383 entspricht bisherigem Art 2 lit n Rahmen-Richtlinie 2002/21/EG.

384 **Anm.** – die ePrivacy-VO idF. Entwurf EU-Kommission verwendet nicht den „Nutzer"-Begriff des Art 2 lit a ePrivacy-Richtlinie 2002/58/EG; – anderer Nutzerbegriff als „Nutzer" iSd. Art 2 Nr 13 Richtlinie Kodex für die elektronische Kommunikation 2018/1972 = Art 2 lit h Rahmen-Richtlinie 2002/21/EG: „eine natürliche oder juristische Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst in Anspruch nimmt oder beantragt;"

385 *Lust* in Riesz/Schilchegger (Hrsg), TKG (2016) § 3 Rn 56 f; Rn 171 ff; *Stratil* in Stratil (Hrsg), TKG 2003[4] (2013) § 3 Anm. 8; *Fetzer* in Arndt/Fetzer/Scherer/Graulich, (Hrsg.), TKG[2], (2015) § 3 Rn. 35; *Ricke* in Spindler/Schuster (Hrsg), Recht der elektronischen Medien[3] (2015) § 3 Rn 10; *Eckhardt* in Geppert/Schütz (Hrsg), Beck'scher TKG-Kommentar[4] (2013) § 108 Rn 23.

eine Wohngemeinschaft), ändert an seiner Position als Endnutzer nichts.[386] Insoweit können auch juristische Personen (Unternehmen) „Endnutzer" darstellen, obwohl sie nachgeschaltet ein eigenes Firmennetzwerk, eine eigene unternehmensinterne Telekommunikationsnebenstellenanlage oder ein WLAN-Netz betreiben (= iSv. nicht-öffentlicher Kommunikationsdienst). Demgemäß ist der Endnutzer ein Nutzer, der keine öffentlichen Telekommunikationsnetze betreibt oder öffentlich zugängliche Telekommunikationsdienste bereitstellt (Art 2 Nr 14 Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972).[387] „Endnutzer" könnten insofern selbst nur nicht-öffentliche Telekommunikationsdienste betreiben (Geschlossene Benutzergruppen, Corporate Networks).[388] Die Nutzer eines vom Arbeitgeber (Endnutzer) bereitgestellten nicht-öffentlichen betrieblichen Kommunikationsdienstes wären somit die Mitarbeiter (der „Nutzer"-Begriff kommt folglich in der ePrivacy-VO idF. EU Kommission gar nicht vor).[389] Folgt man dem Entwurf der EU-Kommission, wäre Art 8 ePrivacy-VO idF. EU-Kommission insofern nicht direkt im Arbeitsverhältnis zwischen Arbeitgeber und Beschäftigten anwendbar, weil sie die entsprechenden Rechte ausschließlich an den „Endnutzer" adressiert und „Endnutzer" ist bei Firmensmartphones, Tablets, oder Laptops der Arbeitgeber und nicht der Beschäftigte. Insofern wäre auch eine juristische Person als Arbeitgeber „Endnutzer" iSd. ePrivacy-VO idF. EU-Kommission.[390] Verwendet ein Unternehmen ein betriebliches Endgerät müsste dem folgend ausschließlich die juristische Person (Geschäftsführung zugleich als Arbeitgeber) als „Endnutzer" über eine ePrivacy-VO Einwilligung entscheiden (ErwGr 3 ePrivacy-VO idF. EU-Kommission). Mangels Eigenschaft als „Endnutzer" wäre eine Einwilligung eines jeden einzelnen Beschäftigten gemäß Art 8 ePrivacy-VO idF. EU-Kommission nicht erforderlich.

Dies wird von der *Art 29 Datenschutzgruppe* kritisiert, denn der Arbeitgeber (als natürliche oder juristische Person) könne keine Einwilligung für seine Beschäftigten erteilen. Art 8 ePrivacy-VO idF. EU-Kommission enthalte insofern keine geeignete Regelung für das Arbeitsverhältnis z.B. wenn der Arbeitgeber das Diensttelefon des Arbeitnehmers aktualisieren möchte oder er über die Onboard Unit Standortdaten seiner betrieblichen Fahrzeuge auslesen will. Demgemäß bedürfe es nach der *Art 29 Datenschutzgruppe* einer Ausnahme für das Arbeitsverhältnis:

- Arbeitgeber stellt Endeinrichtungen iZh mit dem Arbeitsverhältnis zur Verfügung;
- Arbeitnehmer sind Nutzer der Endeinrichtung;
- Der Eingriff ist für das Funktionieren der Einrichtung unbedingt nötig (Grundsätze der Verhältnismäßigkeit und Subsidiarität in Bezug auf die Datenerhebung wären vom Arbeitgeber zu beachten).[391]

386 *Graf* in Graf (Hrsg), BeckOK StPO mit RiStBV und MiStra[33. Edition] (Stand: 01.04.2019) § 3 TKG Rn 10.

387 *Lünenbürger/Stamm* in Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018) § 3 Rn 19.

388 *Lünenbürger/Stamm* in Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018) § 3 Rn 37.

389 *Art 29 Datenschutzgruppe*, WP 247 (2017) 30; *Fetzer* in Arndt/Fetzer/Scherer/Graulich, TKG[2] (2015) § 3 Rn 86; *Lust* in Riesz/Schilchegger (Hrsg), TKG (2016) § 3 Rn 174; *Lünenbürger/Stamm* in Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018) § 3 Rn 37.

390 ErwGr 3 COM(2017) 10 final. 14; *Art 29 Datenschutzgruppe*, WP 247 (2017) 30; 34.

391 *Art 29 Datenschutzgruppe,* WP 247 (2017) 34 f; *Art 29 Datenschutzgruppe*, WP 249 (2017) 5.

Aus der oben dargestellten klaren Adressierung des Art 8 ePrivacy-VO idF. EU-Kommission ausschließlich an „Endnutzer" (= Arbeitgeber), scheint das Erfordernis eines von der *Art 29 Datenschutzgruppe* geforderten Erlaubnistatbestandes mA jedoch zweifelhaft. Ein Arbeitgeber z.B. als juristische Person dürfte nämliche eine Einwilligung iSd. ErwGr 3 ePrivacy-VO in seiner Rolle als „Endnutzer" nach Art 8 ePrivacy-VO idF. EU-Kommission ohnehin nur erteilen, wenn zuvor vom Arbeitgeber sichergestellt wird, dass für das Auslesen der Informationen am Endgerät (personenbezogene Beschäftigtendaten) eine datenschutzrechtliche Rechtsgrundlage für die damit verbundene gleichzeitige datenschutzrechtliche Offenlegung (Art 4 Nr 2 DSGVO) von Beschäftigtendaten an die auf das Endgerät zugreifende Stelle vorliegt (z.B. § 26 BDSG idF. 2. DSAnpUG-EU bzw. Art 6 Abs 1 lit a, b, f DSGVO[392]). Insofern würde in diesem Fall eine Einwilligung des Arbeitgebers als „Endnutzer" nach ePrivacy-VO nicht das Datenschutzrecht für Beschäftigte übersteuern, sondern wäre weiter vom Arbeitgeber streng zu beachten, wenn er anderen Stellen iSd. Art 8 ePrivacy-VO idF. EU-Kommission Zugriff auf seine betrieblichen Endgeräte gewähren lassen will.

Art 8 ePrivacy-VO idF. EU-Parlament (Okotber 2017)

Der Entwurf des Europäischen Parlaments enthält weitgehend die Empfehlungen der Art 29 Datenschutzgruppe („*Der Begriff Endnutzer sollte alle einzelnen Nutzer umfassen*")[393] und schützt sowohl „Endnutzer" als auch „Nutzer". Die ePrivacy-VO idF. EU-Parlament verwendet den bisherigen Begriff „Nutzer" im Sinne des Art 2 lit a ePrivacy-Richtlinie 2002/58/EG und übernimmt für die Definition des „Endnutzers" die bisherige Begriffsbestimmung des „Nutzers" aus der Rahmen-Richtlinie 2002/21/EG:

- „Nutzer" (Art 2 Abs 3 lit af ePrivacy-VO idF. EP[394]): „*eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt, ohne diesen Dienst zwangsläufig abonniert zu haben.*"
- „Endnutzer" (Art 2 Abs 3 lit ae ePrivacy-VO idF. EP[395]): „*eine juristische oder natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst in Anspruch nimmt oder beantragt*;"

Der Beschäftigte ist „Nutzer" (Art 2 Abs 3 lit af ePrivacy-VO idF. EP[396]), der Arbeitgeber der „Endnutzer" (Art 2 Abs 3 lit ae ePrivacy-VO idF. EP iSd. bisherigen Verständnisses des Begriffs „Nutzers" gemäß Art 2 lit h Rahmen Richtlinie 2002/21/EG). Da Art 8 ePrivacy-VO idF. EU-Parlament sowohl auf den „Endnutzer" als auch auf den „Nutzer" abstellt, wäre Art 8 ePrivacy-VO idF. EU-Parlament im Arbeitsverhältnis voll anwendbar. Das EU-Parlament möchte insofern einen Zugriff auf das dienstliche Endgerät durch den Arbeitgeber nur in folgenden Fällen erlauben, *„wenn dies im Rahmen von Arbeitsverhältnissen für die Erfüllung einer von einem Arbeitnehmer wahrzunehmenden Aufgabe technisch zwingend nötig [ist], sofern*

392 *Art 29 Datenschutzgruppe,* WP 249 (2017) 6 f.
393 *Art 29 Datenschutzgruppe*, WP 247 (2017) 30.
394 entspricht dem Begriff „Nutzer" gemäß Art 2 lit a ePrivacy-Richtlinie 2002/58/EG.
395 entspricht dem Begriff des „Nutzers" gemäß Art 2 lit h Rahmen-Richtlinie 2002/21/EG.
396 entspricht dem Begriff „Nutzer" gemäß Art 2 lit a ePrivacy-Richtlinie 2002/58/EG.

- *der Arbeitgeber die Endeinrichtung bereitstellt bzw. deren Nutzer ist,*
- *der Arbeitnehmer der Nutzer der Endeinrichtung ist und*
- *sie überdies nicht der Überwachung des Arbeitnehmers dient."*

Darüberhinaus wäre ein Arbeitgeberzugriff bzgl. IT-Sicherheit erlaubt, *„wenn dies nötig [ist], um Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Endeinrichtungen des Endnutzers zu wahren, und zwar durch Aktualisierungen und für den hierfür erforderlichen Zeitraum, sofern*

- *dadurch in keiner Weise die Funktionsweise der Hardware oder Software geändert wird oder die vom Nutzer festgelegten Einstellungen zum Schutz der Privatsphäre geändert werden,*
- *der Nutzer bei jeder Installation einer Aktualisierung im Voraus informiert wird und*
- *der Nutzer die Möglichkeit hat, die automatische Installation dieser Aktualisierungen zu verschieben oder auszuschalten"*[397]

Damit wäre aber der Zugriff des Arbeitgebers auf dienstliche Endgeräte massiv erschwert und unpraktikabel. Die politische Entwicklung der ePrivacy-VO idF.EU-Parlament wird zeigen, wie weit europäische Arbeitgeber von Art 8 ePrivacy-VO betroffen sein werden.

Art 10 ePrivacy-VO Entwurf (beide Fassungen)

Art 10 ePrivacy-VO enthält Anforderungen an die in Verkehr gebrachte Software, die elektronische Kommunikation erlaubt. Diese muss die Möglichkeit bieten zu verhindern, dass Dritte Informationen in der Endeinrichtung eines „Endnutzers" (EU-Parlament: „Nutzers") speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten. Der Entwurf der EU-Kommission zielt auf den Schutz des „Endnutzers" ab, der Entwurf des EU-Parlaments wider auf den Schutz des „Nutzers" (siehe Diskussion oben). Je nach finaler politischer Umsetzung („Nutzer" / „Endnutzer") kann Art 10 ePrivacy-VO auch als konkrete Anforderungen an die vom Arbeitgeber an den Arbeitnehmer zur Verfügung gestellten Software angesehen werden (z.B. wenn selbst vom Arbeitgeber programmiert).[398]

Art 16 ePrivacy-VO Entwurf EU-Kommission (Januar 2017)

Art 16 ePrivacy-VO enthält eine an jedermann adressierte Vorschrift für Werbekommunikation. Sie ist von Arbeitgebern bei Beschäftigten, die zugleich dessen Kunden sind, zu beachten. Art 16 ePrivacy-VO entspricht dabei weitgehend § 7 dUWG in Deutschland bzw. § 107 öTKG 2003 in Österreich (vgl. Art 13 ePrivacy-RL 2002/58/EG).

---

397 *Europäisches Parlament*, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)), 137 ff.

398 COM(2017) 10 final., 32 f; (Art 10 ePrivacy-VO-E idF. EU-Kommission); *Europäisches Parlament,* Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)) 141 f.

Die Herausforderung am IT-gestützten Arbeitsplatz liegt aber woanders. Ein Beschäftigter am IT-gestützten Arbeitsplatz ist weder „Kunde“ noch „Endnutzer“ iSd. Art 16 ePrivacy-VO idF. EU-Kommission. Willigt ein Arbeitgeber als „Endnutzer“ zu Werbeanrufen/Werbeemails Dritter ein und werden daraufhin dessen Beschäftigte an den vom Arbeitgeber als „Endnutzer“ bereitgestellten Endgeräten (Smartphone, etc.) angerufen oder erhalten Werbemails, scheint dies aufgrund des reinen Abstellens auf die Einwilligung des „Endnutzers“ nun erlaubt. Ist der einwilligende Arbeitgeber („Endnutzer“) zudem eine juristische Person, bleibt der Fall offen, also ob überhaupt eine Einwilligung des Arbeitgebers erforderlich wäre (Art 16 Abs 5 ePrivacy-VO idF. EU-Kommission). Die *Art 29 Datenschutzgruppe* verlangt, dass für natürliche Personen, die für juristische Personen („Endnutzer“) als Beschäftigte arbeiten, dasselbe Schutzniveau gelten müsse und eine Einwilligung nur dann bei juristischen Personen nicht erforderlich sei[399], wenn diese über öffentliche Kontaktdaten wie z.B. info@companyname.eu kontaktiert werden.[400] Allgemein verlangt die *Art 29 Datenschutzgruppe*, dass die ePrivacy-VO alle „Nutzer“ schützen sollte.[401] Art 13 ePrivacy-Richtlinie 2002/58/EG idF. Citizens‘ Rights Richtlinie 2009/136/EG schützt aktuell bei Werbekommunikation die „Teilnehmer“[402] (Arbeitgeber als natürliche Person) und „Nutzer“[403] (Beschäftigte). Nationales Recht schützt ggf. auch juristischen Personen.[404] Demgemäß würde aus heutiger Perspektive gemäß dem Entwurf der EU-Kommission die Möglichkeit Werbeanrufe zu tätigen und Werbeemails an Beschäftige eines Unternehmens zu schicken mA erleichtert, da nur mehr der Arbeitgeber als „Endnutzer“ iSd. ePrivacy-VO bei betrieblichen und zugleich personenbezogenen eMail-Accounts/Telefonnummern zustimmen müsste und nicht mehr jeder Mitarbeiter als konkreter „Nutzer“ (Art 13 ePrivacy-RL); bzw. in Deutschland bei Anrufen – je nach Zweck des Werbeanrufs – in der Rolle als „Verbraucher“ oder „sonstige Marktteilnehmer“ bzw. bei Werbemails als „Adressat“ (vgl. § 7 Abs 2 – Abs 3 dUWG); und in Österreich bei Anrufen in der Rolle als „Benutzer“ und bei Werbemails als „Empfänger“ (vgl. § 107 öTKG 2003).

In Deutschland stellt sich das oben beschriebene Problem nämlich bisher gar nicht: § 7 Abs 2 Nr 2 UWG unterscheidet bei Telefonanrufen zwischen „Verbrauchern“ (§ 13 BGB) und „sonstigen Marktteilnehmern“ (§ 2 Abs 1 Nr 1 UWG) als „*alle Personen, die als Anbieter oder Nachfrager von Waren oder Dienstleistungen tätig sind*“. Bei einem Anruf unter der Geschäftsnummer einer Person kommt es im jeweiligen Einzelfall darauf an, ob der Werbeanruf einem geschäftlichen Zweck („sonstige Marktteilnehmer) – „mutmaßliche Einwilligung“ iSd. § 7 Abs 2 Nr 2 Alt 2 UWG reicht aus – oder einem privaten Zweck („Verbraucher“) – ausdrückliche Einwilligung iSd. § 7 Abs 2 Nr 2 Alt 1 UWG erforderlich – dient. Anrufe auf Privatnummern werden immer als Werbeanrufe an Verbraucher angesehen und bedürfen der ausdrücklichen Einwilligung des Verbrauchers.[405] Hinsichtlich elektronischer Kommunikation (Werbeemails) stellt § 7 Abs 2 Nr 3 UWG ganz allgemein auf „Adressaten“ ab („Verbraucher“ und „sonstige Marktteilnehmer“) und verlangt immer die

399 Art 16 Abs 5 ePrivacy-VO idF. EU Kommission (COM(2017) 10 final.).
400 *Art 29 Datenschutzgruppe*, WP 247 (2017) 38.
401 *Art 29 Datenschutzgruppe*, WP 247 (2017) 30.
402 Art 2 lit k Rahmen-Richtlinie 2002/21/EG.
403 Art 2 lit a ePrivacy-Richtlinie 2002/58/EG.
404 Art 13 Abs 5 ePrivacy-Richtlinie idF. Citizens‘ Rights Richtlinie 2009/136/EG.
405 *Köhler* in Köhler/Bornkamm (Hrsg), UWG[37] (2019) § 7 Rn 140; Rn 160.

vorherige ausdrückliche Einwilligung, ausgenommen es liegen die Vorrausetzungen des § 7 Abs 3 Nr 1 – 4 UWG vor.[406]

In Österreich stellt § 107 Abs 1 TKG 2003 hinsichtlich Werbeanrufe auf den „Teilnehmer“[407] ab (z.B. Arbeitgeber) und löst das Einwilligungsproblem (klarer Einwilligungsvorbehalt) damit, dass *„ [d]er Einwilligung des Teilnehmers die Einwilligung einer Person, die vom Teilnehmer zur Benützung seines Anschlusses ermächtigt wurde, gleich [steht].“*[408] *Riesz* weist darauf hin, dass dies nur dann gelten könne, wenn der „Benutzer“[409] vom „Teilnehmer“ zu solchen Willenserklärung bevollmächtigt wurde bzw. ein solcher Anschein vorliege. Einwilligungen früherer Anschlussinhaber könnten nicht zustimmungslos auf diejenigen übertragen werden, die diesen nunmehr „benützen“.[410] Hinsichtlich der Zusendung elektronischer Post stellt § 107 Abs 2 TKG 2003 auf „Empfänger“ [411] ab. Darunter fallen sowohl natürliche als auch juristische Personen.[412] Bei einem persönlichen betrieblichen eMail-Postfach am IT-gestützten Arbeitsplatz wie bspw. „vorname.nachname@unternehmenxyz.at“ muss jeder betroffene Arbeitnehmer als „Empfänger“ (§ 107 Abs 2 TKG 2003) zustimmen und nicht nur der Arbeitgeber (der Arbeitgeber muss aber jedenfalls bei E-Mail Adressen des Unternehmens wie info@companyname.eu zustimmen). Eine Einwilligung bzgl. elektronischer Post ist nur dann nicht erforderlich, wenn die Voraussetzungen des § 107 Abs 3 TKG 2003 vorliegen.[413]

Art 16 ePrivacy-VO idF. EU-Parlament (Okotber 2017)

Das Europäische Parlament stellt in Art 16 ePrivacy-VO idF. EU-Parlament hinsichtlich Werbekommunikation wieder auf den „Nutzer“ (Art 4 Abs 3 lit af ePrivacy-VO idF. EU-Parlament) ab, also denjenigen, der den elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt (Beschäftigten). Damit gelten nach dem EU-Parlament die Einwilligungserfordernisse bzw. auch die Ausnahmeregelungen gemäß Art 16 Abs 2 ePrivacy-VO idF. EU-Parlament bzgl. „Kunden“ auch gegenüber jedem Beschäftigten hinsichtlich seines persönliches betriebliches eMail-Postfachs bzw. Telefons.[414]

Zwischenstand:

- Art 8 – Art 10 ePrivacy-VO sind gemäß Entwurf der EU-Kommission 2017 nicht direkt auf das Verhältnis Arbeitgeber – Beschäftigten anwendbar („Endnutzer“). Hingegen

406 *Köhler* in Köhler/Bornkamm (Hrsg), UWG[37] (2019) § 7 Rn 185.
407 § 3 Z 19 TKG 2003 = Art 2 lit k Rahmen-Richtlinie 2002/21/EG.
408 § 107 Abs 1 Satz 2 TKG 2003 idF. BGBl. I Nr. 102/2011.
409 § 92 Z 2 TKG 2003 = Art 2 lit a ePrivacy-Richtlinie 2002/58/EG.
410 *Riesz* in Riesz/Schilchegger (Hrsg), TKG (2016) § 107 Rn 66; 77 ff.
411 Art 2 lit g DSRL 95/46/EG = Art 4 Nr 9 iVm. Art 94 DSGVO.
412 *Riesz* in Riesz/Schilchegger (Hrsg), TKG (2016) § 107 Rn 69.
413 *Feiel/Lehofer*, Telekommunikationsgesetz 2003 Praxiskommentar (2004) 306 (zur alten Rechtslage § 107 Abs 2 u. Abs 4 TKG, welcher mit BGBl. I Nr. 133/2005 aufgehoben wurde; Kommentar weiter gültig).
414 *Europäisches Parlament*, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)); *Feiel/Lehofer*, Telekommunikationsgesetz 2003 Praxiskommentar (2004) 306.

wäre dies bei Art 8 – Art 10 gemäß dem Entwurf des EU-Parlaments sehr wohl der Fall („Nutzer“ und „Endnutzer“).[415]
- Art 12 bis 15 ePrivacy-VO sind denkmöglich nicht anwendbar (siehe oben).
- Art 16 ePrivacy-VO bereitet für den IT-gestützten Arbeitsplatz Schwierigkeiten: Ein Beschäftigter ist weder „Kunde“ noch „Endnutzer“. Art 16 Abs 1 ePrivacy-VO idF. EU-Kommission verlangt die Einwilligung zu Werbekommunikation nur von „Endnutzern“, wenn sie natürliche Personen sind (Arbeitgeber). Juristische Personen und ihre Mitarbeiter werden gemäß Art 16 Abs 5 ePrivacy-VO nicht direkt geschützt. Im Vergleich zu heute (§ 7 dUWG / § 107 öTKG 2003) sorgt Art 16 ePrivacy-VO idF. EU-Kommission mA wahrscheinlich für ein Herabsenken des Schutzniveaus von IT-gestützt arbeitenden Beschäftigten hinsichtlich an sie adressierter elektronischer Werbekommunikation, weil letztlich allein der Arbeitgeber als „Endnutzer“ entscheiden würde, ob Beschäftigte elektronische Werbekommunikation erhalten dürfen und nicht mehr jeder Beschäftigte selbst wie bisher als „Adressat“ iSd. § 7 Abs 2 Nr. 3 dUWG bzw. als „Empfänger“ iSd. § 107 Abs 2 öTKG 2003.[416]

3.3.2 Deutschland – §§ 11 ff TMG, § 7 UWG

In Deutschland wurde die E-Commerce-Richtlinie 2000/31/EG und die national dazu für erforderlich angesehenen datenschutzrechtlichen Spezialregelungen als Teilumsetzung der EG-Datenschutzrichtlinie 95/46/EG gemeinsam im Telemediengesetz (TMG) umgesetzt.

Die Thematik § 7 UWG im Beschäftigtenverhältnis wurde bereits in **Kapitel 3.3.1** zu Art 16 ePrivacy-VO-E besprochen (vgl. auch Art 13 ePrivacy-RL).

Die deutsche legistische Konzeption folgte seit Mitte der 1990er Jahre (ursprünglich TDG/TDDSG[417], seit 2007 TMG[418]) bis 24. Mai 2018 dem OSI-Schichtenmodell:

- Transportebene → §§ 88 ff TKG 2004 (Bestandsdaten u. Fernmeldegeheimnis),
- Diensteebene → §§ 11 ff TMG (Bestands-, Nutzungsdaten u. Nutzungsprofile),
- Inhaltsebene → §§ 1 – 11; 27 ff BDSG 2003 (Inhaltsdaten).

Telemedien (Homepage, Webshop, Social Media Plattform, etc.) sind Dienste, die sich auf der 2. Anwendungs-Schicht des 3-Schichten Modells des Datenschutzes bzw. auf den Schichten 5. – 7. des OSI/ISO Modell oder der Schicht 4. des TCP/IP Modells befinden.[419] Aus Datenschutzsicht ist ein Anbieter eines Telemediums zugleich Verantwortlicher iSd. Datenschutzrechts (Art 4 Nr 7 DSGVO).[420]

---

415 *Art 29 Datenschutzgruppe*, WP 247 (2017) 34 f; *Art 29 Datenschutzgruppe*, WP 249 (2017) 5; *Europäisches Parlament,* Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)) 137 f.

416 *Art 29 Datenschutzgruppe*, WP 247 (2017) 38.

417 Teledienstedatenschutzgesetz TDDSG (BGBl. 1997 I. 1870, 1871).

418 Telemediengesetz TMG (BGBl. 2007 I. 179, 251).

419 § 1 Abs 1 TMG.

420 *Schmitz* in Spindler/Schmitz (Hrsg), TMG^2 (2018) § 11 Rn 13 ff.

Gemäß § 11 Abs 1 TMG gelten die Datenschutzvorschriften des TMG nicht für die Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien, soweit die Bereitstellung solcher Dienste

1) im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder

2) innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

Bei erlaubter Privatnutzung der Beschäftigten ist nach hM das TMG auch im Arbeitgeber – Beschäftigten Verhältnis voll anwendbar.[421] *Schmidt* lehnt jedoch die Anwendung der §§ 12 ff TMG auch bei erlaubter Privatnutzung im Beschäftigtenverhältnis entgegen dem Wortlaut in § 11 Abs 1 TMG ab. Die Vorschriften „passen" nicht zum Beschäftigungsverhältnis.[422]

Die Hauptschwierigkeit in der aktuellen Diskussion um die §§ 11 ff TMG iZh mit der DSGVO und Art 5 Abs 3 ePrivacy 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG (bzw. Art 8 ePrivacy-VO) liegen darin, dass die §§ 11 ff. TMG und die europarechtlichen Vorgaben völlig andere Regelungsschwerpunkte verfolgen. Die §§ 11 ff. TMG enthalten ein umfassendes Regelwerk für legale pseudonyme Nutzerprofile zu konkret und final im TMG bestimmten Zwecken, aus denen der Anbieter eines Telemediums aber selbst nicht die Identität eines Nutzers ableiten kann (§§ 12, 13 Abs 1, 15 Abs 3 TMG). Identifizierte Nutzerprofile und auch pseudonyme Nutzerprofile zu anderen Zwecken, als in § 15 Abs 3 TMG genannt, sind nur nach vorheriger informierter, bewusster und eindeutiger Einwilligung des Nutzers (§§ 12, 13 TMG) erlaubt (= pseudonyme Nutzerprofile sind in Deutschland nur zu den in § 15 Abs 3 TMG genannten Zwecken ohne informierte Einwilligung zulässig). Um zu verhindern, dass bei einem Telemedium anfangs legale pseudonyme Nutzerprofile gemäß den in § 15 Abs 3 TMG genannten Zwecke, nachträglich durch Mustervergleich einer konkreten identifizierten Person (rechtswidrig) zugeordnet werden, enthält das TMG ein strenges, durch technische und organisatorische Maßnahmen sicherzustellendes, Zusammenführungsverbot (vgl. § 15 Abs 3 Satz 3 TMG; gemäß § 16 Abs 2 Nr 5 TMG mit Bußgeldrisiko iHv. € 50.000). Will ein Nutzer trotz dieser klaren Rechtslage das Risiko einer Zusammenführung bei einem Websitebesuch nicht eingehen, hat er gegenüber dem Anbieter ein „Opt Out"-Widerspruchsrecht (§ 15 Abs 3 Satz 1 TMG). Das TMG reguliert – anders als das ePrivacy-Europarecht – insofern keine technischen Details wie IP Adressen, Cookies oder Fingerprints, sondern regelt plattformunabhängig und technologieneutral das Erstellen von legalen pseudonymen (Opt out) und einwilligungsbedürftigen identifizierten (Opt in) Nutzerprofilen. Die DSGVO enthält keine solchen Spezialregelungen wie das TMG, sondern nur allgemeine Bestimmungen zur personenbezogenen Datenverarbeitung. Die darüberhinausgehende Spezialregelung in Art 5 Abs 3 ePrivacy 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG (als auch der Nachfolger Art 8 ePrivacy-VO) beschränken – anders als die §§ 11 ff TMG – ihren Reglementierungsbereich ausschließlich auf das Endgerät von (End-)Nutzern. Der Unterschied im Regelungsansatz

421 *Gola*, Datenschutz am Arbeitsplatz[5] (2014) Rn 261 ff; *Elschner* in Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019) Teil 22.1 Elektronische Arbeitnehmerüberwachung Rn 123.

422 *Schmidt,* Datenschutz für „Beschäftigte (2016) 107.

zeigt sich nun dadurch, dass bspw. ein Webtracking nur zu einem kleinen Teil am Endgerät eines (End-)Nutzers stattfindet, der überwiegende Teil erfolgt auf den Servern der Tracker. Die europäischen ePrivacy-Regelungen regulieren – anders als das TMG – in Form eines „alles oder nichts" Ansatzes alle Informationen, die aus den Endgeräten der (End-)Nutzer erhoben werden sollen. Sie regulieren – anders als das TMG – aber nicht das Tracking selbst. Dieses anschließende Tracking auf den Servern der Tracker unterliegt allein der DSGVO. Der Regelungsansatz der europäischen ePrivacy Normen besteht nun konkret darin, dass der (End-)Nutzer zwar durch den strengen Einwilligungsvorbehalt verhindern kann, dass überhaupt Trackingsdaten („Informationen") von seinem Endgerät an einen Tracker übertragen werden. Willigt der Endnutzer einmal in die Übertragung dieser „Informationen" aus seinem Endgerät an den Tracker ein, hat er dann aber keine effektive Kontrolle mehr über die weitere Verwendung dieser Trackingdaten. Trackingdaten dürfen im Falle von personenbezogenen Daten, gestützt auf Art 6 Abs 1 lit f DSGVO (ErwGr 47 – 49) durch den Tracker verarbeitet werden. Handelt es sich bei den ausgelesenen Informationen gar nicht um personenbezogene Daten[423] (z.B. Informationen über eine juristische Person) können sie – nach erteilter ePrivacy-Einwilligung des Nutzers – vom Tracker unbeschränkt verarbeitet werden, mangels Anwendbarkeit der DSGVO.[424]

Es gab nun eine lange politische Diskussion darüber, ob die im Jahr 2009 geänderte Bestimmung Art 5 Abs 3 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG tatsächlich bereits (vorab seit 2001) in den §§ 11 ff TMG (bis 2006 TDDSG) umgesetzt wurde. Hintergrund dazu ist, dass der Deutsche Bundestag nach Verabschiedung der Citizens' Rights Richtlinie 2009/136/EG in Brüssel anschließend keine Novelle des TMG einleitete und ein dazu bereits ausgearbeiteter Gesetzesvorschlag der SPD Fraktion vom Januar 2012 für eine dbzgl. TMG Novelle im Bundestag abgelehnt wurde.[425] Die EU-Kommission stellte im Jahr 2015 daher klar, dass sie Art 5 Abs 3 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG als im deutschen TMG nicht umgesetzt ansieht[426], leitete aber kein Vertragsverletzungsverfahren gegen Deutschland ein. In Deutschland war man aber spätestens seit dem Jahr 2011 (zumindest bis zum Bericht der EU-Kommission 2015[427]) davon ausgegangen, dass eine Umsetzung der Citizens' Rights Richtlinie 2009/136/EG im TMG erfolgt sei und als solche in Brüssel anerkannt wurde. [428]

423 EuGH Urteil v. 19.10.2016, C-582/14 („Breyer"); BGH Urteil v. 16.05.2017, Az. VI ZR 135/13.

424 *Schleipfer*, Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 2017, 460 ff; *Schleipfer*, Datenschutzkonformer Umgang mit Nutzungsprofilen – Sind IP-Adressen, Cookies und Fingerprints die entscheidenden Details beim Webtracking? ZD 2015, 399 ff; *Schleipfer*, Nutzungsprofile unter Pseudonym – Die datenschutzrechtlichen Bestimmungen und ihre Anwendung im Internet, RDV 4/2008, 143 ff; *Keppeler*, Was bleibt vom TMG-Datenschutz nach der DS-GVO? MMR 2015, 779 ff.

425 BT-Drs 17/8454 (Gesetzentwurf); BT-Drs 17/8814 (Beschlussempfehlung und Bericht); BT – 2. Beratung vom 8.10.2012 – BT-Plenarprotokoll 17/198, S. 23862C – 23862D.

426 *European Commission*, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report (2015) 63.

427 *European Commission*, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report (2015) 63.

428 *Schneider* in telemedicus.info (05.02.2014), EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt, abrufbar unter: https://www.telemedicus.info/article/2716-EU-Kommission-

Die pauschalen Verarbeitungsverbotsbestimmungen der §§ 12, 14, 15 TMG widersprachen aber bereits seit 2011 gemäß EuGH Rechtsprechung – aufgrund des oben beschriebenen völlig unterschiedlichem Regelungsansatzes zwischen europäischem Datenschutzrecht und deutschem TMG/TDDSG-Recht –, somit bereits vor Inkrafttretens der DSGVO, umfassend den europarechtlichen Vorgaben des Art 7 lit f DSRL 95/46/EG[429]; zudem sah der EuGH das TMG nie als Umsetzung der ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG an.[430] Diese Interpretation ergibt sich auch aus der BT-Drs. 13/7385, S. 22 zum alten TDDSG 1997 (es wird dort nur auf die EG-Datenschutzrichtlinie 95/46/EG Bezug genommen).[431] Das TDDSG wurde textlich im Jahr 2001 zur Anpassung an die E-Commerce-Richtlinie 2001/31/EG teilweise neu formuliert[432] und im Jahr 2007 ins TMG verschoben – die TDDSG-Bestimmungen wurden dabei in den §§ 11 ff TMG *„- abgesehen von erforderlichen redaktionellen Anpassungen – unverändert übernommen"*[433].

Das weitere Schicksal der §§ 11 ff TMG im Verhältnis zur DSGVO wurde im Mai 2018 durch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) und auch bereits zwei Mal durch die Deutsche Bundesregierung[434] (BT-Drs. 18/12356, S. 28; BT-Drs. 19/2653, S. 9.) selbst und der hM[435] geklärt. Am 26. April 2018 stellte die *Datenschutzkonferenz* abschließend klar: *„Die Vorschrift des Artikels 95 DSGVO findet keine Anwendung auf die Regelungen im 4. Abschnitt des TMG* [Anm. §§ 11 ff TMG]. *Denn diese Vorschriften stellen vorrangig eine Umsetzung der durch die DSGVO aufgehobenen Datenschutzrichtlinie [95/46/EG] dar und unterfallen – da sie auch nicht auf der Grundlage von Öffnungsklauseln in der DSGVO beibehalten werden dürfen –*

Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html (zuletzt abgerufen am 20.06.2019); CO-COM11-20, 04th October 2011, Questionnaire on the implementation of the Article 5(3) of the ePrivacy Directive, 2 ff.

429 EuGH Urteil v. 19.10.2016, C-582/14 („Breyer"); BGH Urteil v. 16.05.2017, Az. VI ZR 135/13; EuGH Urteil v. 24.11.2011, C-468/10 („ASNEF"), C-469/10 („FECEMD").

430 EuGH Urteil v. 19.10.2016, C-582/14 („Breyer").

431 BT-Drs. 13/7385, 22 (TDDSG); *Piltz* in Gola (Hrsg), DS-GVO[2] (2018) Art 95 Rn 19; *Schmitz* in Spindler/Schmitz/Gleis (Hrsg), TDG (2004) Einf TDDSG Rn 13 ff.

432 BT-Drs. 14/6098, 8 ff (Elektronischer Geschäftsverkehr-Gesetz – EGG); *Schmitz* in Spindler/Schmitz/Gleis (Hrsg), TDG (2004) Einf TDDSG Rn 10 ff.

433 BT-Drs. 16/3078, 15. (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG).

434 BT-Drs. 18/12356, 28. (Netzwerkdurchsetzungsgesetz – NetzDG): *„Eine Änderung der Sachlage wird nunmehr durch die anstehende Anpassung des Datenschutzrechts im TMG an die Datenschutz-Grundverordnung eintreten. Mit derAufhebung des bereichsspezifischen Telemediendatenschutzes werden für die Telemedien dann die Vorschriften der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes gelten* (…)."; BT-Drs. 19/2653, 9. (Antwort Frage 21): *„Die Bundesregierung weist darauf hin, dass die Datenschutzkonferenz (DSK) zur Nichtanwendbarkeit einiger Datenschutz-Regelungen des TMG hinischtlich Reichweitenmessung und Tracking-Mechanismen und zu der Frage der Anwendung der Verordnung (EU) 2016/679 bei Telemedien und beim Einsatz von Tracking-Mechainismen einen Beschluss gefasst hat, der für die Rechtsanwendung durch die einzelnen unabhängigen Datenschutzaufsichtsbehörden von Bedeutung ist. Der Vollzug des Datenschutzrechts obliegt den unabhängigen Datenschutzbehörden. Die Bundesregierung hat darauf keinen Einfluss."*

435 *Schulz* in Gola (Hrsg), DS-GVO[2] (2018) Art 6 Rn 32 ff; *Piltz* in Gola (Hrsg), DS-GVO[2] (2018) Art 95 Rn 18 ff; *Schmitz* in Spindler/Schmitz (Hrsg), TMG[2] (2018) Vorbemerkung: Überblick zum Datenschutz nach TMG und Ausblick auf DS-GVO und ePrivacy-VO, Rn 3; *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 f.

demgemäß dem Anwendungsvorrang der DSGVO. Hiervon betroffen sind damit auch etwaige unvollständige Umsetzungen der ePrivacy-Richtlinie in diesem Abschnitt, welche jedenfalls isoliert nicht mehr bestehen bleiben können. Damit können die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden. Eine unmittelbare Anwendung der ePrivacy-Richtlinie [Anm. Art 5 Abs 3] (…) *kommt nicht in Betracht (keine horizontale unmittelbare Wirkung von Richtlinien).*"[436]

Entgegen der Ansicht der *Datenschutzkonferenz* werden aber auch im Anwendungsbereich der DSGVO und trotz ihres Anwendungsvorrangs einige Bestimmungen der §§ 11 ff TMG nicht verdrängt und bleiben bei erlaubter Privatnutzung (vgl. § 11 Abs 1 TMG)[437] im Beschäftigtenverhältnis für Arbeitgeber beim IT-gestützten Arbeitsplatz anwendbar:

- § 13 Abs 4 Nr 1 TMG: „*Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer die Nutzung des Dienstes jederzeit beenden kann.*" Diese TMG-Anforderung unterliegt nicht dem Anwendungsvorrang der DSGVO (weil von der DSGVO nicht behandelt). Die Anforderung wird durch eine entsprechende Schaltfläche am Telemedium realisiert, mit der der Nutzer jederzeit die Verbindung zum Dienst unterbrechen können muss. Die Nichterfüllung dieser Anforderung wird gemäß § 16 Abs 2 Nr 3 TMG mit Bußgeld bis zu € 50.000 bestraft.[438]
- § 13 Abs 7 TMG (IT-Sicherheitsgesetz 2015, BGBl. 2015 I. 1324)[439] bleibt anwendbar, da diese Bestimmung zur IT-Sicherheit über den Schutz personenbezogener Daten hinausgeht und insofern nicht umfassend von Art 32 DSGVO verdrängt wird. Die Nichterfüllung der Anforderung durch einen Diensteanbieter eines Telemediums wird gemäß § 16 Abs 2 Nr 3 TMG mit Bußgeld bis zu € 50.000 bestraft.[440]
- § 15 Abs 4 Satz 2 TMG (Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen als faktische „Muss-Vorschrift"[441]) stellt eine rechtliche Verpflichtung iSd. Art 6 Abs 1 lit c iVm. Art 6 Abs 2 DSGVO dar.[442]

---

436 *Datenschutzkonferenz,* Positionsbestimmung (26.04.2018), Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf (zuletzt abgerufen am 20.06.2019).

437 *Gola*, Datenschutz am Arbeitsplatz[5] (2014) Rn 261 ff; *Elschner* in Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019) Teil 22.1 Elektronische Arbeitnehmerüberwachung Rn 123.

438 *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 135; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 281; Rn 302.

439 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) BGBl. 2015 I. 1324; BT-Drs. 18/4096, 34 f.

440 *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 143; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 289; Rn. 302.

441 *Schreibauer* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 15 Rn 32 ff.

442 *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 153; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 296.

- die Pflichten zur Herausgabe von Daten gemäß § 14 Abs 2 – Abs 5 TMG und § 15 Abs 5 Satz 4 TMG (erweitert gemäß NetzDG, BGBl. 2017 I. 3352)[443] stellen eine rechtliche Verpflichtung durch mitgliedstaatliches Recht gemäß Art 6 Abs 1 lit c iVm. Abs 2 und Abs 3 DSGVO dar.[444] Zusätzlich greift § 24 BDSG idF. DSAnpUG-EU.[445]

Es ergibt sich für die Datenverarbeitung auf der 2. Anwendungs-Schicht des 3-Schichten Modells seit 25. Mai 2018 folgendes Ergebnis gemäß DSGVO:

- für Verarbeitungen, die unbedingt erforderlich sind, damit der Anbieter den von den betroffenen Personen angefragten Dienst zur Verfügung stellen kann, gilt Art 6 Abs 1 lit b DSGVO (Vertragserfüllung) bzw. Art 6 Abs 1 lit f DSGVO (berechtigtes Interesse);
- weitere nicht unbedingt erforderliche Verarbeitungstätigkeiten bedürfen einer Interessenabwägung im Einzelfall gemäß Art 6 Abs 1 lit f DSGVO (berechtigtes Interesse);
- der Einsatz von Tracking-Mechanismen iZh mit Telemedien (Homepage, Webshop, Social Media Plattform, etc.), die das Verhalten von Betroffenen nachvollziehbar machen sollen, sowie für die Erstellung von Nutzerprofilen iZh mit Telemedien bedarf es nach Ansicht der *Datenschutzkonferenz* immer einer informierten Einwilligung in Form einer Erklärung oder sonstiger eindeutig bestätigender Handlungen.[446] Diese Klarstellung der *Datenschutzkonferenz* zu Telemedien entspricht der Kommentierung von *Schmitz*[447] und orientiert sich an Art 5 Abs 3 ePrivacy-Richtlinie idF. Citizens' Rights Richtlinie.
  Die *GDD* und *Schwartmann/Klein* kritisieren diese Ansicht und sehen weiterhin die Möglichkeit pseudonymisierte Nutzerprofile gestützt auf Art 6 Abs 1 lit f DSGVO zu machen, was – mangels Umsetzung des Art 5 Abs 3 ePrivacy-RL in Deutschland – damit auch (ebenso gestützt auf Art 6 Abs 1 lit f DSGVO) das Ablegen von Cookies am Endgeräten von Nutzern ohne vorherige informierte Einwilligung sowie den anschließenden Abruf von Informationen aus Endgeräten, umfassen soll. Die *GDD* und *Schwartmann/Klein* verlangen – wie bisher nach §§ 12, 15 Abs 3 TMG – nur die informierte Einwilligung, wenn keine Pseudonymisierung durch den Tracker erfolgt und begründen dies damit, dass Art 5 Abs 3 ePrivacy-Richtlinie 2002/58/EG idF. Citizens' Rights Richtlinie 2009/136/EG keine Vorschrift iSd. Art 95 DSGVO sei, denn Art 95

443 BT-Drs. 18/13013, 23 f; (Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss) NetzDG).

444 *Heun/Assion* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) Art 95 Rn 14 ff; *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 146 f; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 292.

445 BT-Drs. 18/12356, 28 (Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken); *Schmitz* in Spindler/Schmitz (Hrsg), TMG[2] (2018) § 14 Rn 61; 68.

446 *Datenschutzkonferenz,* Positionsbestimmung (26.04.2018), Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf (zuletzt abgerufen am 20.06.2019).

447 *Schmitz* in Spindler/Schmitz (Hrsg), TMG[2] (2018) § 15 Rn 36.

DSGVO spreche nur von „öffentlich zugänglichen elektronischen Kommunikationsdiensten in öffentlichen Kommunikationsnetzen“.[448] Dieser Ansicht folgte der EuGH im Urteil C-673/17 („Planet49 GmbH“) vom 01. Oktober 2019 aber nicht.[449]

Zwischenstand:

Auf nicht-öffentliche Arbeitgeber in Deutschland ist (auch) bei erlaubter Privatnutzung auf der Diensteebene – mit sehr geringen Ausnahmen (siehe oben) – die DSGVO und das BDSG idF. 2. DSAnpUG-EU alleine anwendbar.

Öffentliche Stellen in Deutschland, welche nicht von der DSGVO erfasst werden (vgl. Art 2 Abs 2 DSGVO), jedoch im Anwendungsbereich des § 1 Abs 1 Satz 2 iVm. § 11 Abs 1 TMG liegen (erlaubte Privatnutzung Bedienstete), können wie bisher unverändert ihre IKT Infrastruktur gemäß den Regelungen der §§ 11 ff TMG betreiben.[450] Hintergrund ist, dass die §§ 11 ff TMG nicht vom Deutschen Bundestag aufgehoben wurden, sondern nur (größtenteils) im Anwendungsbereich von der DSGVO (insb. bei nicht-öffentlichen Stellen) verdrängt werden.[451]

3.3.3 Österreich – § 96 Abs 3 TKG 2003, § 18 ECG, § 107 TKG 2003

In Österreich wurde die Neufassung des Art 5 Abs 3 ePrivacy-Richtlinie durch die Citizens‘ Rights Richtlinie 2009/136/EG im Jahr 2011 mit BGBl. I Nr. 102/2011 in § 96 Abs 3 TKG 2003 in österreichisches Recht transformiert und mit BGBl. I Nr. 78/2018 an die DSGVO angepasst. § 96 Abs 3 TKG verlangt eine Einwilligung des „Teilnehmers“ bzw. „Benutzers“ z.B. für das Setzen eines „Cookies“, subsidiär gelangt die DSGVO zur Anwendung. Eine Einwilligung iSd. § 96 Abs 3 TKG 2003 muss auf der Grundlage von klaren und umfassenden Informationen getroffen werden. Wenn technisch durchführbar, kann in Österreich diese Einwilligung auch über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung vom „Teilnehmer“ bzw. „Benutzer“ ausgedrückt werden.[452] § 96 Abs 3 TKG 2003[453] idF. BGBl. I Nr. 78/2018 ist adressiert an:

- „öffentliche Kommunikationsdienste“ (§ 3 Z 9 TKG 2003) als eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht.
- „Anbieter eines Dienstes der Informationsgesellschaft“ (§ 3 Z 1 E-Commerce-Gesetz) als „ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (§ 1 Abs. 1 Z 2 Notifikationsgesetz 1999);“

448 ErwGr 47 letzer Satz DSGVO; *Schwartmann/Klein* in Schwartmann/Jaspers/Thüsing /Kugelmann (Hrsg), Datenschutz-Grundverordnung mit Bundesdatenschutzgesetz (2018) Art 6 Rn 137 ff; *GDD* (08.05.2018), Zulässigkeit des Tracking nach der DS-GVO, abrufbar unter: https://www.gdd.de/aktuelles/startseite/zulaessigkeit-des-tracking-nach-der-ds-gvo (zuletzt abgerufen am 20.06.2019).

449 EuGH Urteil v. 01.10.2019, C-673/17 („Planet49 GmbH“) Rn 44 ff.

450 Art 2 Abs 2 lit a, lit b und lit d DSGVO iVm. § 1 Abs 1 Satz 2 TMG; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 270.

451 Art 2 Abs 1 DSGVO; EuGH, Rs. 6/64, Slg. 1964, S. 1251, 1269 – Costa/ENEL.

452 ErläutRV 1389 BlgNR 24. GP 25.

453 BGBl. I Nr. 102/2011.

Keine Anwendung auf Arbeitgeber:

Ein Arbeitgeber, der seinen Beschäftigten die Privatnutzung erlaubt, bietet weder eine gewerbliche noch öffentliche Kommunikationsdienstleistung an (§ 3 Z 9 TKG 2003).[454] Ein Arbeitgeber ist gegenüber seinen Arbeitnehmern auch kein Dienst der Informationsgesellschaft (§ 3 Z 1 E-Commerce-Gesetz). Die E-Commerce-Richtlinie 2000/31/EG und das österreichische E-Commerce-Gesetz (ECG) sind auf die vertraglichen Beziehungen zwischen Arbeitnehmern (arbeitnehmerähnlichen Personen) und Arbeitgebern nicht anzuwenden.[455] *Zankl* weist ausdrücklich daraufhin, dass Fragen zur privaten IT-Nutzung bzw. Überwachung des IT-gestützten Arbeitsplatzes durch den Arbeitgeber nicht vom ECG erfasst werden.[456] So stellt bspw. auch das Intranet der Mitglieder der WKÖ (= WKÖ-Beschäftigte und WKÖ-Pflichtmitglieder sind dort aktiv) auch noch keinen Dienst der Informationsgesellschaft dar.[457]

Hinsichtlich der Bestandsdaten von Nutzern bei Host-Providern (§ 16 ECG) existiert mit § 18 Abs 4 ECG eine eigene datenschutzrechtliche Erlaubnisnorm, die Adresse eines Nutzers ihres Dienstes, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen können, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.[458] Zusätzlich existieren Auskunftspflichten an staatliche Stellen gemäß § 18 Abs 2 – Abs 3 u. Abs 5 ECG. Ähnlich wie in Deutschland die §§ 14 Abs 2 – 5, 15 Abs 5 Satz 4 dTMG handelt es sich bei § 18 Abs 2 – 5 ECG um Verpflichtungen durch mitgliedstaatliches Recht (Art 6 Abs 1 lit c iVm. Abs 2 iVm. Abs 3 DSGVO), die weiter anwendbar bleiben.[459] § 18 ECG findet aber – anders als das dTMG bei erlaubter Privatnutzung – mangels „Diensteeigenschaft" eines österreichischen Arbeitgebers (vgl. § 3 Z 1 E-Commerce-Gesetz) keine Anwendung im Beschäftigtenverhältnis (z.B. Corporate Social Networks).[460]

Die Thematik § 107 TKG 2003 im Beschäftigtenverhältnis wurde bereits in **Kapitel 3.3.1** zu Art 16 ePrivacy-VO-E besprochen (vgl. auch Art 13 ePrivacy-RL).

Zwischenstand:

Die Anwendung der § 96 Abs 3 TKG 2003 und § 18 ECG scheidet im Arbeitsverhältnis mangels „Diensteeigenschaft" (§ 3 Z 1 ECG, § 3 Z 9 TKG 2003) aus. Auf Diensteebene gelangen allein die DSGVO und das DSG 2018 im Arbeitsverhältnis zur Anwendung.[461]

---

454 *Brodil*, ZAS 2004/01, 17 (19).

455 ErläutRV 817 BlgNR 21. GP 16 f; ErwGr 18 E-Commerce-Richtlinie 2000/31/EG; *Burgstaller/Minichmayr*, E-Commerce-Recht[2] (2011) 9; 13; 260.

456 *Zankl,* E-Commerce-Gesetz[2] (2016) § 2 Rn 44.

457 *Burgstaller/Minichmayr*, E-Commerce-Recht[2] (2011) 88 f.

458 ErläutRV 817 BlgNR 21. GP 39.

459 *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 292.

460 ErläutRV 817 BlgNR 21. GP 16 f; ErwGr 18 E-Commerce-Richtlinie 2000/31/EG; *Burgstaller/Minichmayr*, E-Commerce-Recht[2] (2011) 9, 13; 88 f; 260; *Zankl,* E-Commerce-Gesetz[2] (2016) § 2 Rn 44.

461 ErläutRV 817 BlgNR 21. GP 16 f; ErwGr 18 E-Commerce-Richtlinie 2000/31/EG; *Brodil*, ZAS 2004/01, 17 (19); *Zankl,* E-Commerce-Gesetz[2] (2016) § 2 Rn 44.

3.4 Zwischenergebnis

Für den IT-gestützten Arbeitsplatz – unabhängig ob Privatnutzung erlaubt ist oder nicht – zeigt sich nun zusammenfassend folgender Zwischenstand der geprüften europäischen und nationalen datenschutzrechtlichen Normen hinsichtlich ihrer Anwendbarkeit:

- Transportebene → DSGVO in D / Ö;
- Diensteebene → DSGVO in D* / Ö;
- Inhaltsebene → DSGVO in D / Ö.

Es konnte herausgearbeitet werden, dass für einen europäischen Arbeitgeber (am Bsp. D / Ö) auch bei erlaubter Privatnutzung am IT-gestützten Arbeitsplatz ausschließlich* nur mehr die DSGVO zur Anwendung gelangt.

***Ausgenommen** in Deutschland bei erlaubter Privatnutzung (vgl. § 11 Abs 1 TMG)[462] die Weitergeltung der einzelnen Bestimmungen § 13 Abs 4 Nr 1 (spezielle Schaltfläche = kein Regelungsbereich der DSGVO); § 13 Abs 7 (IT-Sicherheit – über Art 32 DSGVO hinausgehend); § 14 Abs 2 – Abs 5; § 15 Abs 5 Satz 4 und § 15 Abs 4 Satz 2 TMG (diverse rechtliche Verpflichtungen iSd. Art 6 Abs 1 lit c; Abs 2 und Abs 3 DSGVO).[463]

Wie weit die Art 5 ff, Art 8 und Art 10 ePrivacy-VO eine Rolle am IT-gestützten Arbeitsplatz im Verhältnis Arbeitgeber und Beschäftigte spielen werden, hängt davon ab, ob dem Entwurf der EU-Kommission vom Januar 2017 (nicht anwendbar)[464] oder dem Entwurf des EU-Parlaments vom Oktober 2017 (tlw. anwendbar)[465] gefolgt wird. Die Umsetzung der Entwurfs des EU-Parlaments in dieser intensiven Form ist eher unwahrscheinlich. Dies deuten die bisherigen Dokumente des Europäischen Rats an, die hinsichtlich dieser Punkte weitgehend den Vorstellungen der EU-Kommission folgen und Arbeitgeber und Beschäftigte eindeutig nicht im Anwendungsbereich sehen.[466]

462 *Gola*, Datenschutz am Arbeitsplatz[5] (2014) Rn 261 ff; *Elschner* in Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019) Teil 22.1 Elektronische Arbeitnehmerüberwachung Rn 123.

463 *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 265 ff.

464 COM(2017) 10 final.

465 *Europäisches Parlament,* Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)).

466 *Europäischer Rat*, Interinstitutional File:2017/0003(COD) vom 22. Februar 2019, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6771_2019_INIT&from=EN (zuletzt abgerufen am 20.06.2019).

3.5 Inhaltsebene

3.5.1 Überblick

Der primärrechtliche Art 8 Abs 2 Satz 1 EU-GRC und der sekundärrechtliche DSGVO-Grundsatz der „Rechtmäßigkeit" (Art 5 Abs 1 lit a DSGVO) verlangen vom Arbeitgeber als datenschutzrechtlich Verantwortlichen (Art 4 Nr 7 DSGVO), dass konkrete Rechtsgrundlagen für die Verarbeitung vorliegen. Die DSGVO selbst enthält Rechtsgrundlagen, die eine Beschäftigtendatenverarbeitung legitimieren können.

3.5.2 DSGVO-Erlaubnistatbestände für Beschäftigtendatenverarbeitung

Folgende allgemeine Erlaubnistatbestände der DSGVO kommen in Betracht:

Einwilligung (Art 6 Abs 1 lit a iVm. Art 4 Nr 11 iVm. Art 7 DSGVO): Der Beschäftigte willigt informiert in die Verarbeitung seiner Daten durch den Arbeitgeber ein. Gemäß Art 4 Nr 11 DSGVO ist eine datenschutzrechtliche Einwilligung eine Erklärung oder eine sonstige als eindeutige bestätigende Handlung abgegebene Willensbekundung, die freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben wird. Die betroffene Person gibt mit einer datenschutzrechtlichen Einwilligung zu verstehen, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Eine datenschutzrechtliche „saubere" (iSv. freiwillige) Einwilligung ist im Beschäftigtenverhältnis häufig schwer zu erreichen.[467] ErwGr 42 DSGVO führt zur Freiwilligkeit aus: *„Es sollte nur dann davon ausgegangen werden, dass [die betroffene Person] ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden."*[468] ErwGr 43 stellt abschließend klar: *„Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht* (…) *und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern."*[469]

Die *Art 29 Datenschutzgruppe* kommt letztlich zum Ergebnis, dass die Einwilligung der Beschäftigten in den meisten Fällen nicht die Rechtsgrundlage für Datenverarbeitungen durch den Arbeitgeber sein sollte. Hintergrund ist, dass schwer ausgeschlossen werden kann, dass eine Nichteinwilligung eines Beschäftigten nicht mit tatsächlichen oder potentiellen Nachteilen für den Beschäftigten später verbunden ist, womit es häufig an der Freiwilligkeit mangelt, mit der Folge, dass letztlich keine rechtskonforme Einwilligung und damit keine wirksame Rechtsgrundlage für den Arbeitgeber vorliegt. Werden personenbezogene Daten von Beschäftigten ohne bzw. auf Basis einer falschen oder unwirksamen Rechtsgrundlage verarbeitet, stellt dies einen Verstoß gegen Art 5 Abs 1 lit a DSGVO („Rechtmäßigkeit") iVm. Art 83 Abs 5 lit a DSGVO dar.[470] Eine Freiwilligkeit bei einer Einwilligung ist nur dann gegeben, wenn die betroffene Person tatsächliche eine

467 *Art 29 Datenschutzgruppe*, WP 249 (2017) 6 ff.
468 ErwGr 42 Datenschutz-Grundverordnung (EU) 2016/679.
469 ErwGr 43 Datenschutz-Grundverordnung (EU) 2016/679.
470 *Art 29 Datenschutzgruppe*, WP 249 (2017) 6.

Wahlmöglichkeit hat, also ohne Nachteile auf die Erteilung der Einwilligung verzichten kann.[471]

Vertragsverhältnis (Art 6 Abs 1 lit b DSGVO): Die Verarbeitung der Beschäftigtendaten ist für die Erfüllung des Arbeitsvertrages erforderlich (z.B. Gehaltszahlung). Dies ist der Fall, wenn der Arbeitgeber die personenbezogenen Daten eines Beschäftigten verarbeiten muss (Erforderlichkeit), um den vertraglichen Verpflichtungen mit dem Beschäftigten nachzukommen.[472] Darunter fallen sämtliche personenbezogenen Daten, die für den Abschluss, die Durchführung, die Änderung und die Beendigung der arbeitsvertraglichen Beziehungen erforderlich sind. Maßgeblich ist die Erforderlichkeit zur Vertragsdurchführung (unmittelbarer Zusammenhang zwischen Datenverarbeitung und Vertragsverhältnis). Deshalb dürfen mA gestützt auf Art 6 Abs 1 lit b DSGVO auch Daten verarbeitet werden, die die Verwirklichung des Vertragszwecks (Erfüllung vertraglich begründeter Haupt- und Nebenpflichten) gefährden könnten (z.B. konkrete Anhaltspunkte auf tatsächliche oder vermeintliche Verletzungen der den Vertragspartner obliegenden Verpflichtungen). Die allgemeine (präventive) Überwachung der IKT Nutzung von Beschäftigten ist nach Ansicht der *Art 29 Datenschutzgruppe* in den meisten Fällen aber nicht unmittelbar für die Erfüllung des Arbeitsvertrages erforderlich, eine solche Verarbeitung ist daher für den Arbeitgeber nur unter den Voraussetzungen des Art 6 Abs 1 lit f DSGVO (berechtigte Interessen des Arbeitgebers) zulässig.[473] Der Tatbestand der „Erforderlichkeit" in Art 6 Abs 1 lit b DSGVO bedeutet aber auch, dass eine Datenverarbeitung, die zwar durch einen Vertrag gedeckt ist, aber nicht „erforderlich" ist, nicht auf diesen Erlaubnistatbestand gestützt werden kann. Bspw. kann der Aufbau einer unternehmensweiten Mitarbeiterdatenbank mit dem Ziel, dass sich die Kollegen leichter miteinander in Verbindung setzen können, für die Erfüllung des Beschäftigtenvertrages erforderlich sein (Art 6 Abs 1 lit b DSGVO), wenn der Beschäftigte einer solchen Tätigkeit nachgeht, wo dies zur erfolgreichen Durchführung notwendig ist. Die Verarbeitung der Beschäftigtendaten in der Mitarbeiterdatenbank kann aber auch auf Art 6 Abs 1 lit f DSGVO gestützt werden, wenn der Arbeitgeber ein berechtigtes Interesse zusammen mit einem legitimen Zweck am Betrieb einer solchen Mitarbeiterdatenbank hat und die Interessen der Beschäftigten nicht überwiegen. Die korrekte Rechtsgrundlage wäre dann Art 6 Abs 1 lit f DSGVO, weil die Verarbeitung nicht unbedingt erforderlich ist zur Vertragsdurchführung des Beschäftigtenverhältnisses, sondern sich auf ein berechtigtes Interesse des Verantwortlichen stützt.[474]

Rechtliche Verpflichtung (Art 6 Abs 1 lit c DSGVO): Die Verarbeitung der Beschäftigtendaten wird hier durch rechtliche Verpflichtungen aus dem arbeitsrechtlichen, handels- und

471 *Brodil,* Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 4; *Brodil*, Arbeitnehmerdatenschutz und Datenschutz-Grundverordnung (DSGVO), ecolex 2018, 486 ff.

472 *Art 29 Datenschutzgruppe,* WP 249 (2017) 6 ff; *Art 29 Datenschutzgruppe*, WP 48 (2001) 16.

473 *Art 29 Datenschutzgruppe,* WP 217 (2014) 22; *Art 29 Datenschutzgruppe,* WP 249 (2017) 6 ff; *Art 29 Datenschutzgruppe*, WP 55 (2002) 17; *Art 29 Datenschutzgruppe*, WP 48 (2001) 16 f; *Gola* in Gola (Hrsg), DS-GVO[2] (2018) Art 6 Rn 27 ff; Rn 95 ff; *Pötters* in Gola (Hrsg), DS-GVO[2] (2018) Art 88 Rn 45 ff.

474 *Art 29 Datenschutzgruppe,* WP 217 (2014) 22.

steuerrechtlichen Vorschriften, etc. vorgeschrieben (z.B. Steuerberechnung, Gehaltsabrechnung, etc.).[475] Es muss sich bei dieser rechtlichen Verpflichtung allerdings um eine Rechtsvorschrift der Europäischen Union oder eines EU-Mitgliedsstaates handeln. Eine Rechtsvorschrift der bspw. USA oder aus Russland, etc. fällt nicht unter den Begriff „rechtliche Verpflichtung" iSd. Art 6 Abs 1 lit c DSGVO. Compliance mit ausländischen (Non-EU-Drittstaaten) rechtlichen Verpflichtungen kann aber ein berechtigtes Interesse iSd. Art 6 Abs 1 lit f DSGVO darstellen.[476]

Lebenswichtiges Interesse (Art 6 Abs 1 lit d DSGVO): Die Verarbeitung muss zum Schutz der lebenswichtigen Interessen eines Beschäftigten erforderlich sein (Arbeitsunfall – Datenübermittlung an Krankenhaus).[477]

Berechtigtes Interesse (Art 6 Abs 1 lit f DSGVO): Die Verarbeitung der Beschäftigtendaten stützt sich auf ein berechtigtes Interesse (und legitimer Zweck) des Arbeitgebers als datenschutzrechtlich Verantwortlichen und die gewählte Methode oder Technologie zur Datenverarbeitung muss für die Wahrung dieses berechtigten Interesses erforderlich sein. Zusätzlich dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person als Beschäftigter, die den Schutz personenbezogener Daten erfordern, nicht im konkreten Einzelfall den berechtigten Interessen des Arbeitgebers überwiegen.[478] Es geht also bei Art 6 Abs 1 lit f DSGVO um eine Prüfung der Ausgewogenheit der Interessen. Die Interessen des Verantwortlichen oder eines Dritten sind gegen die Interessen oder die Grundrechte und Grundfreiheiten des Betroffenen abzuwägen.[479]

Der europäische Gesetzgeber anerkennt unmittelbar in der DSGVO folgende berechtigte Interessen iSd. Art 6 Abs 1 lit f DSGVO:

- (ErwGr 47): Verarbeitung personenbezogener Daten zu Zwecken der Verhinderung von Betrug;
- (ErwGr 48): Verarbeitung personenbezogener Daten innerhalb einer Unternehmensgruppe zu internen Verwaltungszwecken von Kunden- und Beschäftigtendaten;
- (ErwGr 49): Verarbeitung personenbezogener Daten zu Zwecken der Verbesserung der Netz- und IT-Sicherheit.

Die *Art 29 Datenschutzgruppe* anerkennt folgende berechtigte Interessen iSd. Art 6 Abs 1 lit f DSGVO:

- Wirtschaftliche Interessen (Werbung, Effizienzsteigerung und Wettbewerbsfähigkeit);
- Durchsetzung von Rechtsansprüchen über außergerichtliche Verfahren;
- Verhütung von Betrug, Leistungsmissbrauch oder Geldwäsche;
- Überwachung von Arbeitnehmern aus Sicherheits- und Verwaltungsgründen;
- Regelungen zur Meldung mutmaßlicher Missstände (Hinweisgebersystem).[480]

475 *Art 29 Datenschutzgruppe*, WP 249 (2017) 6 ff; *Art 29 Datenschutzgruppe*, WP 48 (2001) 16 f.
476 *Art 29 Datenschutzgruppe,* WP 217 (2014) 24; 70.
477 *Art 29 Datenschutzgruppe,* WP 217 (2014) 26; *Gola* in Gola (Hrsg), DS-GVO[2] (2018) Art 6 Rn 100.
478 *Art 29 Datenschutzgruppe*, WP 249 (2017) 6 ff; *Art 29 Datenschutzgruppe,* WP 48 (2001) 17.
479 *Art 29 Datenschutzgruppe,* WP 217 (2014) 30 ff.
480 *Art 29 Datenschutzgruppe,* WP 217 (2014) 32.

Mit den berechtigten Interessen des Verantwortlichen müssen schließlich die Interessen oder die Grundrechte und Grundfreiheiten der Betroffenen abgewogen werden. Die Interessen oder die Grundrechte und Grundfreiheiten der Betroffenen dürfen nicht den berechtigten Interessen des Verantwortlichen überwiegen. Im Gesetzestext des Art 6 Abs 1 lit f DSGVO fällt auf, dass zwar auf die „berechtigten Interessen" des Verantwortlichen abgestellt wird (iSv. rechtmäßig und hinreichend tatsächlich und gegenwärtig vorliegend[481]) jedoch auf der Betroffenenseite auf die „Interessen oder Grundrechte und Grundfreiheiten" abgestellt wird. Das heißt, auf Betroffenenseite sind alle einschlägigen Interessen in Betracht zu ziehen, soweit damit das Interesse des Einzelnen an einer Wahrung der Privatsphäre und persönlichen Autonomie verbunden ist. Da auf Betroffenenseite das Adjektiv „berechtigt" – anders als bei den Interessen des Verantwortlichen – vom Gesetzgeber nicht benutzt wird, impliziert dies einen weit gefassten Schutzbereich durch Art 6 Abs 1 lit f DSGVO. Selbst Betroffene, die rechtswidrige Handlungen begehen, dürfen keinen unverhältnismäßigen Eingriffen in ihre Rechte und Interessen ausgesetzt werden.[482]

Fünf Prüfschritte sind im Rahmen einer Interessenabwägung nach Art 6 Abs 1 lit f DSGVO vom Verantwortlichen zu beachten:

- **Erster Schritt:** prüfen, ob die Interessensabwägung in Art 6 Abs 1 lit f DSGVO die für den Verarbeitungszweck passende Rechtsgrundlage ist.
- **Zweiter Schritt:** Einstufung des verfolgten Interesses des Verantwortlichen als „berechtigt" oder „nicht-berechtigt";
- **Dritter Schritt:** Feststellung, ob die Verarbeitung zum Erreichen des verfolgten berechtigten Interesses „erforderlich" ist. Das heißt es ist zu überlegen, ob andere, weniger stark in die Privatsphäre eingreifende Mittel zum Erreichens des genannten Zwecks der Verarbeitung gibt, die dem berechtigten Interesse des Verantwortlichen entsprechen.
- **Vierter Schritt:** Abwägung der Interessen, also ob die Grundrechte und Grundfreiheiten oder Interessen des Betroffenen die berechtigten Interessen des Verantwortlichen überwiegen.
- **Fünfter Schritt:** Herstellung eines letztendlichen Gleichgewichts der Interessen durch Berücksichtigung zusätzlicher Schutzmaßnahmen (Einsatz von Technologien und Maßnahmen zur Stärkung der Privatsphäre).

Die getroffene Interessensabwägung ist zu dokumentieren und der betroffenen Person und ggf. auch für die Aufsichtsbehörde als Dokumentation bereit zu halten. Betroffenen steht ein Widerspruchsrecht (Art 21 DSGVO) zu.[483]

Vom EGMR[484] wurde in der Entscheidung „Bărbulescu" ein „Sechs-Punkte-Katalog" zur Rechtmäßigkeit einer Beschäftigtenüberwachung nach Art 8 EMRK entwickelt. Gemäß Art 52 Abs 2 iVm. Art 7 und Art 8 EU-GRC hat der „Sechs-Punkte-Katalog" unmittelbar Auswirkungen auf die Anwendung des Art 6 Abs 1 lit f DSGVO bzgl. der Kontrolle der IT-Nutzung. Zu prüfen ist:

---

481 *Art 29 Datenschutzgruppe,* WP 217 (2014) 32.
482 *Art 29 Datenschutzgruppe*, WP 217 (2014) 38.
483 Art 13 Abs 1 lit d; Art 14 Abs 2 lit b, Art 5 Abs 2 DSGVO; *Art 29 Datenschutzgruppe*, WP 217 (2014) 70 ff.
484 EGMR Urteil v. 05.09.2017, Az. 61496/08 („Bărbulescu").

1. Ob der Arbeitnehmer über die Möglichkeit, dass der Arbeitgeber Maßnahmen zur Überwachung der Kommunikation ergreifen könnte, und über die Umsetzung solcher Maßnahmen informiert wurde. Die Verständigung der Beschäftigten sollte nach *EGMR* hinsichtlich der Art der Überwachung eindeutig sein und im Vorhinein erfolgen.
2. Das Ausmaß der Überwachung durch den Arbeitgeber und den Grad des Eindringens in die Privatsphäre ist zu prüfen, also ob eine Inhaltsüberwachung oder nur eine Kontrolle des Kommunikationsflusses erfolgt; ob die Überwachung nur zeitlich begrenzt ist und wie viele Personen Zugang zu den Ergebnissen der Überwachung haben.
3. Ob der Arbeitgeber legitime Gründe zur Rechtfertigung der Überwachung der Kommunikation und des Zugangs zu ihrem eigentlichen Inhalt vorbringen kann (Verhältnis schützenwerte Arbeitgeberinteressen zur Überwachungstiefe). Die Überwachung des Inhalts von Kommunikation erfordert nach *EGMR* jedenfalls eine gewichtigere Rechtfertigung.
4. Ob der Arbeitgeber die beabsichtigte Überwachungsmaßnahme nicht durch ein gleich wirksames aber eingriffsärmeres Mittel ersetzen kann.
5. Die nachträglichen Konsequenzen der Überwachung für den betroffenen Arbeitnehmer und die Verwendung der Resultate der Überwachungsoperation durch den Arbeitgeber sind zu prüfen, also ob die Ergebnisse der Überwachung dann auch tatsächlich verwendet wurden, um das erklärte Ziel der Maßnahme zu erreichen. Die gewonnen Erkenntnisse müssen für die Durchsetzung der legitimen und dokumentierten Überwachungsziele insofern konsequent verwertet werden, ansonsten fehlt der Überwachung rückblickend die erforderliche Ernsthaftigkeit.
6. Die innterbetrieblichen Datenschutzprozesse müssen „angemessene Garantien" für die Betroffenen Beschäftigten schaffen. Als Beispiel führt der *EGMR* aus, dass solche Sicherungen insbesondere gewährleisten sollten, dass der Arbeitgeber keinen Zugang zum eigentlichen Inhalt der betroffenen Kommunikation hat, solange der Arbeitnehmer nicht im Vorhinein über diese Möglichkeit informiert worden ist.[485]

Der EGMR folgt in der Entscheidung „Bărbulescu" der bisher im deutschsprachigen Raum u.a. von *Brodil* vertretenen Auffassung, dass sich der Umfang der Kontrollbefugnis des Arbeitgebers ausschließlich aus dem objektiven Recht ableitet. Die Intensität der Kontrollbefugnis hängt nicht vom Verbot oder der Zulassung von Privatnutzung ab. Verbietet der Arbeitgeber die Privatnutzung, darf der Arbeitgeber trotzdem nicht die gesamte damit rein formal „dienstliche" Kommunikation vollständig kontrollieren, sondern nur angemessene Mittel zur Überprüfung des Verbots der Privatnutzung einsetzen. Das heißt die vollständige

485 EGMR Urteil v. 05.09.2017, Az. 61496/08 („Bărbulescu") – die deutsche Übersetzung des Urteils „Bărbulescu" auf der Homepage des EGMR (hudoc.echr.coe.int) abrufbar unter: https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=001-185260&filename=CASE%20OF%20B%u0102RBULESCU%20v.%20ROMANIA%20-%20%5BGerman%20Translation%5D%20summary%20by%20the%20Austrian%20Institute%20for%20Human%20Rights%20%28%D6IM%29.pdf (zuletzt abgerufen 20.06.2019); *Hanloser* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 1. Rn 88.

Einsicht in den Inhalt einer unzulässigen aber offensichtlichen „privaten" Kommunikation ist – trotz verbotener Privatnutzug – idR. nicht erlaubt (private Daten).[486]

3.5.3 Deutschland – Beschäftigtendatenschutz IT-gestützter Arbeitsplatz

Überblick

Deutschland hat von der Öffnungsklausel in Art 88 DSGVO Gebrauch gemacht und in § 26 BDSG eine eigene nationale Beschäftigtendatenschutzbestimmung verankert. Mit dieser Bestimmung wird der bis 24. Mai 2018 gültige § 32 BDSG aF fortgeführt und der Terminologie der DSGVO angepasst.[487] Aufgrund des Umstandes, dass die Diskussion, ob §§ 88 ff TKG 2004 bei erlaubter Privatnutzung zur Anwendung gelangt oder nicht, durch den Anwendungsvorrang der DSGVO[488] endgültig final geklärt ist und §§ 88 ff TKG 2004 nicht mehr auf Arbeitgeber anwendbar sind, gilt auch bei erlaubter Privatnutzung alleine § 26 BDSG iVm. Art 88 DSGVO.[489] Bei der nunmehr alleinigen Anwendung des § 26 BDSG ist der „Sechs-Punkte-Katalog" des EGMR im Urteil „Bărbulescu" zur Rechtmäßigkeit der Beschäftigtenüberwachung bei der IT-Nutzung zu beachten (vgl. **Kapitel 3.5.2**). [490]

Der Anwendungsbereich des § 26 BDSG iVm. Art 88 DSGVO im Verhältnis zu den Erlaubnistatbeständen in Art 6 Abs 1 DSGVO ist noch nicht abschließend geklärt. So unterscheidet bspw. *Forst* bzgl. der für eine Verarbeitung von Beschäftigtendaten korrekt heranzuziehenden Rechtsgrundlage zwischen Art 6 Abs 1 lit f DSGVO oder § 26 Abs 1 BDSG hinsichtlich der Zweckbestimmung der getroffenen Maßnahme:[491]

- geht es dem Verantwortlichen (Arbeitgeber) darum, Fehlverhalten einzelner Beschäftigter aufzudecken und daraus arbeits- oder disziplinarische Konsequenzen zu ziehen gelte allein § 26 BDSG.
- geht es dem Verantwortliche (Arbeitgeber) darum, ausschließlich allgemein Schäden vom Unternehmen abzuwehren (z.B. Art 32 DSGVO), ohne dass die gewonnen Erkenntnisse Konsequenzen für die Beschäftigten nach sich ziehen sollen, gelten die allgemeinen Erlaubnistatbestände der DSGVO, weil keine Datenverarbeitung zu Zwecken des Beschäftigtenverhältnisses erfolge. Eine nachträgliche Weiterverarbeitung doch zu

---

486 *Brodil,* Eine nicht dem AN offengelegte Kommunikationsüberwachung am Arbeitsplatz verletzt das in Art 8 EMRK geschützte Recht auf Privatleben, ZAS 2018/33, 203 (207).

487 BT-Drs 18/11325, 96 ff.

488 Art 2 Abs 1 iVm. Art 95 DSGVO; EuGH, Rs. 6/64, Slg. 1964, S. 1251, 1269 – Costa/ENEL.

489 BT-Drs 19/2653, 9. (Antwort BReg Frage 20); *Heun* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) vor § 88 TKG Rn 16 ff; *Heun/Assion* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) Art 95 Rn 10 ff; Rn 19; *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 68; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 211; Rn 224; *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4; *Kühling/Raab* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) Art 95 Rn 11; *Nebel/Richter*, ZD 2012, 407 (408); *Schwichtenberg*, Datenschutz in drei Stufen (2018) 64 ff; *Maschmann* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) § 26 BDSG Rn 50.

490 *Hanloser* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 1. Rn 88.

491 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 Rn 18.

Zwecken des Beschäftigtenverhältnisses (Kontrolle, Leistungsbeurteilung) würde aber dann – trotz verfügbarer Rechtsgrundlage § 26 BDSG – höchstwahrscheinlich an der mangelnden Zweckkompatibiltität scheitern (Zweckkompatibilitätstest).[492]

- Dient eine Verarbeitung gleichzeitig beiden Zwecken und wird dies auch so den Beschäftigten kommuniziert, findet alleine § 26 BDSG Anwendung.[493]

Durchführung des Beschäftigtenverhältnisses (inkl. präventive Kontrollen)

Gemäß § 26 Abs 1 Satz 1 BDSG[494] dürfen personenbezogene Daten von Beschäftigten (ohne deren Einwilligung) für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung, für die Durchführung eines Beschäftigungsverhältnisses, oder dessen Beendigung „erforderlich" ist und die Beschäftigten in transparenter Form nach Treu und Glauben darüber informiert wurden (§ 26 Abs 5 BDSG iVm. Art 5 Abs 1 lit a iVm. Art 14 DSGVO). „Erforderlich" iSd. § 26 Abs 1 Satz 1 BDSG ist im Sinne der allgemein bekannten verfassungsrechtlichen Verhältnismäßigkeitsprüfung zu verstehen.[495] Das heißt bei Datenverarbeitungen für Zwecke des Beschäftigtenverhältnisses sind im Rahmen einer „Erforderlichkeitsprüfung" als allgemeine Verhältnismäßigkeitsprüfung die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen. Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt. § 26 Abs 1 Satz 1 BDSG ist dabei auch die Rechtsgrundlage für beabsichtigte präventive Kontrollen der Leistung oder des Verhaltens von Beschäftigten inklusive die Zulässigkeit von präventiven Maßnahmen zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen, die im Zusammenhang mit dem Beschäftigtenverhältnis stehen. Mit § 26 Abs 1 Satz 1 BDSG wird zugleich auch Art 10 DSGVO umgesetzt, womit Arbeitgeber auch Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln ihrer Beschäftigten verarbeiten dürfen.[496]

Ein Eingriff in die informationelle Selbstbestimmung im Sinne einer rechtskonformen Beschäftigtendatenverarbeitung gemäß § 26 Abs 1 Satz 1 BDSG bedarf der folgenden Verhältnismäßigkeitsprüfung:

- *Berechtigte Zwecke (Ziele) auf Seiten des Arbeitgebers im Zusammenhang mit der Durchführung des Beschäftigtenverhältnisses*

Darunter fallen – neben der für die eigentliche Durchführung des Beschäftigtenverhältnisses zu verarbeitenden Daten – bspw. auch präventive allgemeine Kontrollen der Erfüllung der geschuldeten Arbeitsleistung, ob die geschuldete Leistung ordnungsgemäß erbracht

492 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 Rn 18; *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff; *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff.

493 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 Rn 18.

494 bis 24. Mai 2018: § 32 Abs 1 Satz 1 BDSG idF. BGBl. 2009 I. 2814.

495 *Tinnefeld/Buchner/Petri/Hof,* Einführung in das Datenschutzrecht[6] (2018) 148 f.

496 BT-Drs 18/11325, 96 f; BT-Drs 16/13657, 20 f; ErwGr 155 iVm. Art 88 Abs 1 DSGVO; *Gräber/Nolden* in Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018) § 26 BDSG Rn 10 f.

wird, etc. Anlassloses Suchen von Seiten des Arbeitgebers nach belastendem Material gegen Mitarbeiter ohne Anhaltspunkte ist dagegen nicht von berechtigten Interessen getragen.[497]

- *Geeignetheit (Erheblichkeit)*

Die Verarbeitung muss geeignet sein, den berechtigten Zweck des Arbeitgebers zu fördern. Wenn die Maßnahme nicht dazu dient bzw. nicht dazu dienen kann den angestrebten Zweck zu erreichen bzw. die Zweckerreichung zumindest zu fördern, ist sie schlicht ungeeignet zur Zweckerreichung und datenschutzrechtlich nicht erlaubt.[498]

- *Erforderlichkeit im engeren Sinne*

Hier geht es darum zu prüfen, ob mehrere Maßnahmen gleicher Eignung bestehen, die jeweils weniger eingriffsintensiv sind. Die Erforderlichkeit im engeren Sinn einer Maßnahme eines Arbeitgebers ist dann gegeben, wenn sich bei gleicher Eignung keine milderen Mittel gegenüber dem Beschäftigten finden lassen, die die berechtigten Interessen des Arbeitgebers im gleichen Ergebnis sicherzustellen können. Der Arbeitgeber ist dabei nicht gezwungen, Maßnahmen, welche weniger effizient, organisatorisch aufwändiger oder schlicht unwirtschaftlich sind, den Vorrang einzuräumen.[499]

- *Angemessenheit (Verhältnismäßigkeit im engeren Sinn)*

Hier erfolgt eine Abwägung der widerstreitenden Interessen. Die eintretende Beeinträchtigung der Persönlichkeitsrechte des Arbeitnehmers darf nicht außer Verhältnis zu dem angestrebten Zweck stehen. Dabei sind einzubeziehen: der Ort, die Dauer, die Art und der Umfang sowie der Zeitpunkt des Eingriffs durch den Arbeitgeber. Stichprobenartige Kontrollen und zeitlich begrenzte Maßnahmen sind einer dauerhaften Maßnahme grundsätzlich vorzuziehen.[500]

§ 26 Abs 1 Satz 1 BDSG und die darin kodifizierte Verhältnismäßigkeitsprüfung verdrängt im Hinblick auf die Datenverarbeitung für Beschäftigtenverhältnisse sowohl Art 6 Abs 1 lit b DSGVO als auch Art 6 Abs 1 lit f DSGVO. Die Erlaubnistatbestände der Art 6 Abs 1 bzw. Art 9 Abs 2 DSGVO finden jedoch dann weiter parallel zu § 26 Abs 1 u. Abs 3 BDSG Anwendung, wenn die Verarbeitung für andere Zwecke als denen des Beschäftigtenverhältnisses dient („beschäftigungsfremde Zwecke"; vgl. den Umfang der Öffnungsklausel in ErwGr 155, Art 88 Abs 1 DSGVO).[501]

Bei einem arbeitgeberseitigen Zugriff auf dienstliche und private Daten gilt folgendes:

- Der Arbeitgeber darf dienstliche E-Mails bzw. bei dienstlichen elektronischen Daten und Nachrichten z.B. im Rahmen von Enterprise Social Media, innerbetrieblichen Chats sowohl die Verkehrsdaten als auch die Inhaltsdaten – bei entsprechender Sicherstellung

497 *Oberthür* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel B Rn 427 f.
498 *Oberthür* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel B Rn 429.
499 *Oberthür* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel B Rn 430.
500 *Oberthür* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel B Rn 431.
501 BT-Drs 18/11325, 96 f; BT-Drs 16/13657, 20 f; ErwGr 155 iVm. Art 88 Abs 1 DSGVO; *Gola* in Gola/Heckmann (Hrsg), BDSG[13] (2019) § 26 Rn 18; *Schulz* in Gola (Hrsg) DS-GVO[2] (2018) Art 6 Rn 95 ff; *Gräber/Nolden* in Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018) § 26 BDSG Rn 10 f.

der Verhältnismäßigkeit iSd. § 26 Abs 1 Satz BDSG (siehe oben) – einsehen und verarbeiten. Entsprechend seinem allgemein anerkannten Rechts als Arbeitgeber auf Offenlegung brieflicher Dienstkorrespondenz, steht dem Arbeitgeber im selben Ausmaß die Einsicht in dienstliche elektronische Kommunikation zu.[502] Klar unverhältnismäßig und damit rechtswidrig ist aber eine lückenlose Überwachung des Beschäftigten, auch wenn sich diese Überwachung nur auf rein dienstliche Daten beschränken würde, sie wäre dennoch völlig unverhältnismäßig iSd. § 26 Abs 1 Satz 1 BDSG.[503]

- Private Daten, E-Mails und private elektronische Nachrichten dürfen bei erlaubter Privatnutzung vom Arbeitgeber einerseits für das technische Funktionieren der Dienste verarbeitet werden. Wie oben festgestellt werden die §§ 88 ff TKG 2004 (Fernmeldegeheimnis) aufgrund des Anwendungsvorrangs umfassend für Arbeitgeber von der DSGVO verdrängt und sind nicht mehr anwendbar. Trotzdem darf der Arbeitgeber grundsätzlich keine Einsicht in den Inhalt von offensichtlich erkennbar privaten Nachrichten nehmen, denn es besteht sowohl kein berechtigtes Interesse und auch keine begründbare Verhältnismäßigkeit einer solchen Maßnahme zur Einsicht in private Daten von Beschäftigten. Ist der dienstliche oder private Charakter des E-Mails bzw. der Nachricht nicht eindeutig, sollte die dbzgl. Klärung des dienstlichen oder privaten Charakters der Information im ersten Schritt über eine Befragung des Beschäftigten oder über die Verkehrsdaten erfolgen. Deutet sich hier ein dienstlicher Charakter der elektronischen Nachricht an, darf die E-Mail vom Arbeitgeber eingesehen werden. Werden private E-Mails und Nachrichten jedoch verarbeitet, weil ihr privater Charakter irrtümlich nicht erkannt wurde, ist die Verarbeitung sofort vom Arbeitgeber zu beenden, sobald der private Charakter erkannt wird.[504]

In allen präventiven Kontrollfällen nach § 26 Abs 1 Satz 1 BDSG hat der Arbeitgeber aus strafrechtlicher Sicht § 202b StGB (Abfangen von Daten) weiter zu beachten.[505] § 206 StGB kommt mA mangels Eigenschaft eines öffentlich zugänglichen Telekommunikationsanbieters – auch bei erlaubter Privatnutzung – in europarechtskonformer Auslegung (Art 3 iVm. Art 15a ePrivacy-RL iVm. Art 95 DSGVO) nicht (mehr) zur Anwendung.[506] Der an jedermann adressierte § 202b StGB (Art 3 Cyber Crime Convention) schützt das Abfangen (unbefugte Verschaffen iSv. „interception") von (unverschlüsselten) Daten aus nicht-öffentlichen Datenübermittlungen im Sinne eines Übertragungsgeheimnisses. Werden dabei auch

502 *Gola*, Datenschutz am Arbeitsplatz[5] (2014) 47.

503 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 BDSG Rn 124; *Raffler/Hellich*, Unter welchen Voraussetzungen ist die Überwachung von Arbeit- nehmere-mails zulässig? NZA 1997, 862 (863 f.).

504 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 BDSG Rn 124; *Raffler/Hellich*, NZA 1997, 862 (863 f.).

505 *Gola*, Datenschutz am Arbeitsplatz[5] (2014) 47; *Petri* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel D Rn 74 ff; Kapitel D Rn 115 ff.

506 BT-Drs 19/2653, 9. (Antwort BReg Frage 20); *Heun* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) vor § 88 TKG Rn 16 ff; *Heun/Assion* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) Art 95 Rn 10 ff; Rn 19; *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 68; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 211; Rn 224; *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4.

verschlüsselte bzw. mit Passwortschutz versehene Daten abgefangen und anschließend unbefugt durch Überwindung der Zugangssicherung diese Daten ausgespäht, geht – trotz des eigentlichen vorhergehenden rechtswidrigen Abfangens der Daten gemäß § 202b StGB – nach Willen des deutschen Gesetzgebers § 202a StGB hier vor.[507] Das Filtern von elektronischer Kommunikation zum Erkennen von Viren und Spam und das Aufbrechen von (SSL/TLS)-Verschlüsselung durch Arbeitgeber zum Schutz des Unternehmens zum Zweck des Art 32 DSGVO ist durch die gesetzliche Verpflichtung an Verantwortliche geeignete technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung zu treffen gemäß Art 5 Abs 1 lit f iVm. Art 32 DSGVO grundsätzlich europarechtlich gedeckt, womit idR. keine Strafbarkeitsrisiken nach §§ 202a und 202b StGB drohen sollten.[508]

Ist die Privatnutzung erlaubt, werden im Rahmen der Filterung und Analyse auch besondere Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO) verarbeitet (z.B. angesurfte Homepage einer politischen Partei, Homepage eines Arztes, etc.). Aufgrund der besonderen Kategorien von Daten ist eine zusätzliche datenschutzrechtliche Rechtsgrundlage erforderlich. Es ergeben sich **vier** Möglichkeiten einer Lösung: **[1.]** man stützt sich auf die Rechtsgrundlage § 26 Abs 3 BDSG (zweistufige Prüfung: i. arbeitsrechtliche Erforderlichkeit der besonderen Kategorien personenbezogener Daten; ii. Interessensabwägung, ob die Interessen des Beschäftigten im konkreten Einzelfall nicht doch überwiegen.[509]) oder; **[2.]** es existiert zusätzlich zur arbeitsrechtlichen Erforderlichkeit eine ausführende Betriebsvereinbarung mit dort formulierten „geeigneten Garantien" (Art 9 Abs 2 lit b Alt 2. DSGVO) oder; **[3.]** es existiert eine autonome Art 88 Abs 1 DSGVO-Betriebsvereinbarung als eigenständiger Erlaubnistatbestand gemäß § 26 Abs 4 BDSG mit „geeigenten Garantien". Alternativ und praxisnahe bietet sich **[4.]** für den Arbeitgeber, welcher grundsätzlich seinen Beschäftigten die Privatnutzung erlauben will, aber trotzdem IT-Sicherheitsmaßnahmen mit hoher Intensität setzen will, an, im ersten Schritt allgemein die Privatnutzung im Unternehmen zu verbieten und im zweiten Schritt nur mehr solchen Beschäftigten die Privatnutzung wieder erlauben, die der informierten Überwachung ihres Internetverkehrs einschließlich Privatnutzung ausdrücklich zustimmen (§ 26 Abs 2 BDSG).[510] Die BT-Drs 18/11325, S. 97 zum DSAnpUG-EU bestätigt das Vorliegen von „Freiwilligkeit" einer solchen Arbeitnehmer-Einwilligung zur erlaubten Privatnutzung betrieblicher IT: *„[§ 26 Abs 2] Satz 2 [BDSG] legt fest, dass eine freiwillige Einwilligung insbesondere vorliegen kann, wenn die oder der Beschäftigte infolge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder Arbeitgeber und Beschäftigter gleichgerichtete Interessen verfolgen. Die Gewährung eines Vorteils liegt beispielsweise in* (…) *der Einführung der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen*."[511]

Die Strafbestimmung § 202b StGB (Abfangen von Daten) greift spätestens dann nicht mehr als Risiko für den Arbeitgeber, wenn die nicht-öffentlichen Datenübermittlungen beendet ist und der Empfänger (Beschäftigter) die Herrschaft über die übermittelten Daten erlangt

507 BT-Drs 16/3656, 11.

508 *Art 29 Datenschutzgruppe*, WP 118 (2006) 5 ff; *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff; *Raffler/Hellich*, NZA 1997, 862 (863 f.).

509 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 BDSG Rn 83.

510 *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff.

511 BT-Drs 18/11325, 97.

hat (Daten sind am Endgerät gespeichert). Für den Zugriff des Arbeitgebers auf Daten am Endgerät des Beschäftigten besteht kein Strafbarkeitsrisiko nach § 202b StGB. Ein Risiko besteht nur noch aus § 202a StGB, wenn verschlüsselte bzw. zumindest Passwort geschützte offensichtlich private Daten eines Beschäftigten durch Überwindung der Zugangssicherung durch den Arbeitgeber unberechtigt eingesehen werden (unbefugt Passwort überwinden oder Verschlüsselung aufbrechen).[512] Allerdings hat in der Regel der Arbeitgeber im Arbeitsverhältnis regelmäßig die faktische Verfügungsbefugnis (Arbeitsmaterial IT) an den privaten Daten unabhängig davon, ob eine private Nutzung erlaubt war oder nicht. Verfügungsbefugt iSd. § 202a StGB ist grundsätzlich (auch) derjenige, der das materielle Eigentums- oder Besitzrecht an dem Speichermedium bzw. am Endgerät hat und dies ist der Arbeitgeber, was das Strafbarkeitsrisiko stark reduziert.[513]

Repressive Kontrollen (interne Untersuchungen)

Der Tatbestand des § 26 Abs 1 Satz 2 BDSG bestimmt für Arbeitgeber sehr eng formulierte Eingriffsvoraussetzungen für heimliche interne Untersuchungen gegen Beschäftigte beim Verdacht einer im Beschäftigtenverhältnis begangenen Straftat. In diesem Zusammenhang gibt es jedoch bis heute keine Klarstellung, was unter „Straftaten" iSd. § 26 Abs 1 Satz 2 BDSG im Verhältnis zu Art 10 DSGVO genau zu verstehen ist. Nach *Hanloser* wird unter „Straftaten" iSd. Art 10 DSGVO nur auf das Sammeln von Daten über Verurteilungen oder sonst wie festgestellte Straftaten insbesondere in Registern abgestellt, nicht die vorgelagerte investigative Datenverarbeitung zur Aufklärung einer Straftat iSd. § 26 Abs 1 Satz 2 BDSG. Dies ergebe sich aus Art 10 Satz 2 DSGVO.[514] *Feiler/Forgó* sehen hingegen bereits solche Daten als Daten über Straftaten iSd Art 10 Satz 1 DSGVO an, wenn ein konkreter begründeter Verdacht über eine Straftat gegen eine bestimmte Person vorliegt, womit Daten im Rahmen von strafrechtlich relevanten Compliance-Untersuchungen gemäß § 26 Abs 1 Satz 2 BDSG zugleich Daten iSd. Art 10 DSGVO wären (vgl. § 4 Abs 3 Z 2 öDSG).[515] Völlig unabhängig von dieser Diskussion benennt § 26 Abs 1 Satz 2 BDSG[516] die gesetzlichen Voraussetzungen für die heimliche Verarbeitung personenbezogener Daten von Beschäftigten zur Aufdeckung von im Beschäftigungsverhältnis begangenen Straftaten. Ein Arbeitgeber hat vor Einleitung einer heimlichen repressiven Maßnahme folgendes konkret zu berücksichtigen:

- es muss ein durch tatsächliche Anhaltspunkte begründeter Verdacht auf eine Straftat vorliegen (liegen objektive Verdachtsmomente gegen den Mitarbeiter vor?);
- der mit tatsächlichen Anhaltspunkten begründete Verdacht auf eine Straftat beinhaltet dabei im Beschäftigungsverhältnis begangenen Straftaten (Straftat während der Arbeitszeit oder Straftat außerhalb der Arbeitszeit gegen den Arbeitgeber);

512 *Gola*, Datenschutz am Arbeitsplatz[5] (2014) 48 f; BT-Drs 16/3656, 10 ff; *Fischer* in Fischer (Hrsg), Strafgesetzbuch[66] (2019) § 202a Rn 9 ff; *Fischer* in Fischer (Hrsg), Strafgesetzbuch[66] (2019) § 202b Rn 3 ff.

513 *Petri* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel D Rn 119.

514 *Hanloser* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 1. Rn 86.

515 *Feiler/Forgó*, EU-DSGVO (2017) Art 10 Rn 1 (für Österreich relevant, da dies entscheidet ob Art 6 Abs 1 lit f DSGVO oder § 4 Abs 3 DSG die korrekte Rechtsgrundlage für eine Compliance Untersuchung ist).

516 bis 24. Mai 2018: § 32 Abs 1 Satz 2 BDSG idF. BGBl. 2009 I. 2814.

- das Handeln des Verantwortlichen (Arbeitgebers) erfolgt zum Zweck der internen Aufdeckung und Aufklärung dieses mit Anhaltspunkten begründeten Verdachts;
- die gesetzlich geforderte Dokumentationsobliegenheit wird vom Verantwortlichen (Arbeitgeber) beachtet;
- es liegt Erforderlichkeit der gesamten Datenverarbeitung hinsichtlich Art und Weise und Umfang vor (= *siehe oben*: „Erforderlichkeit im engeren Sinn"; es bestehen keine Maßnahmen gleicher Eignung mit geringerer Eingriffsintensität),
- es besteht kein überwiegendes entgegenstehendes schutzwürdiges Interesse des betroffenen Beschäftigten – insbesondere keine Unverhältnismäßigkeit von Art und Ausmaß der Verarbeitung im Hinblick auf den Anlassfall. Je dringender der Tatverdacht einer im Beschäftigtenverhältnis begangenen Straftat, desto eher müssen die Interessen des Arbeitnehmers zugunsten der Kontrollmaßnahme des Arbeitgebers zurücktreten.[517]

Damit ergibt es aus § 26 Abs 1 Satz 2 BDSG folgender gesetzlicher Ablauf der Einleitung einer repressiven Aufklärung: **[1.]** Es liegen dem Arbeitgeber tatsächliche Anhaltspunkte vor, die den Verdacht einer Straftat durch den Beschäftigten begründen. Diese tatsächlichen Anhaltspunkte hat der Arbeitgeber **[2.]** zu dokumentieren, bevor **[3.]** interne Ermittlungsmaßnahmen eingeleitet werden dürfen. Die Verarbeitung der Beschäftigtendaten im Rahmen der internen Ermittlung muss für die Aufdeckung der konkreten Straftat auch **[4.]** tatsächlich erforderlich sein. Die Art und das Ausmaß der Verarbeitung dürfen dabei **[5.]** nicht unverhältnismäßig sein und es dürfen **[6.]** keine überwiegenden schutzwürdigen Interessen der Betroffenen entgegenstehen.[518]

Für die heimliche Aufdeckung von „schweren Pflichtverletzungen" (schwere arbeitsrechtliche Verstöße ohne strafrechtliche Relevanz) gilt nach klarstellender Judikatur des BAG als Rechtsgrundlage § 26 Abs 1 Satz 1 BDSG (= bis 24. Mai 2018: § 32 Abs 1 Satz 1 BDSG idF. BGBl. 2009 I. 2814). Hintergrund dieser BAG Entscheidung ist (offenbar), dass die Deutsche Bundesregierung im März 2017 eine Erweiterung des § 26 Abs 1 Satz 2 BDSG auch auf „schwere Pflichtverletzungen" abgelehnt hatte (vgl. BT-Drs 18/11655, S. 30). Die Ausweitung der Anforderungen des § 26 Abs 1 Satz 2 BDSG auch auf „schwere Pflichtverletzungen" war aber bereits seit Jahren höchstgerichtliche BAG Judikatur.[519] Das BAG änderte nun die heranzuziehende Rechtsgrundlage und stützt die Aufklärung „schwerer Pflichtverletzungen" auf § 26 Abs 1 Satz 1 statt auf Satz 2 BDSG. Damit gilt § 26 Abs 1 Satz 1 BDSG nun sowohl für präventive als auch als repressive Maßnahmen[520] und ist in beiden Fällen die heranzuziehende Rechtsgrundlage. Nur wenn es sich bei der repressiven internen (Aufklärungs-)Maßnahme zugleich auch um eine Aufklärung einer im Rahmen des Beschäftigtenverhältnisses begangenen Straftat handelt, ist § 26 Abs 1 Satz 2 BDSG als *lex specialis* Rechtsgrundlage heranzuziehen. Ein tatsächlicher Unterschied in der praktischen Anwendung ist aber – abseits juristischer Förmelei – nicht gegeben. Nach BAG Urteil vom 29. Juni 2017, Az 2 AZR 597/16 – der bisherigen BAG Rechtsprechung

517 *Riesenhuber* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) § 26 BDSG Rn 131; *Oberthür* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel B Rn 432 ff.

518 BT-Drs 18/11325, 96 ff; BT-Drs 16/13657, 20 f.

519 BT-Drs 18/11655, 14; 30 (jeweils zu Nummer 24).

520 *Schröder* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 3. Rn 15 ff; *Schmidt*, Der Nebel lichtet sich: Das BAG systematisiert die Erlaubnistatbestände des Beschäftigtendatenschutzrechts, RDV 2017/6, 284 ff.

unverändert folgend – ist die verdeckte Aufklärung einer (nicht-strafrechtlich relevanten) „schweren Pflichtverletzung" eines Beschäftigten trotzdem nur unter den identischen Voraussetzungen zulässig, wie die Aufdeckung einer Straftat nach § 26 Abs 1 Satz 2 BDSG. Trotz der nun seit Juni 2017 formell unterschiedlichen Rechtsgrundlagen gelten materiellrechtlich weiter die gleichen höchstgerichtlichen Anforderungen des BAG sowohl für die interne heimliche Aufklärung vom im Beschäftigtenverhältnis begangenen Straftaten als auch von schweren Pflichtverletzungen. Insofern sprach das BAG Ende Juni 2017 nur das aus, was die Deutsche Bundesregierung noch Ende März 2017 als Anpassung des BDSG Entwurfs idF. DSAnpUG-EU hinsichtlich textlicher Adaptierung abgelehnt hatte.[521]

Die §§ 201, 202a und 202b StGB müssen bei repressiven Maßnahmen streng beachtet werden.[522] § 206 StGB kommt in europarechtskonformer Anwendung (Art 3, Art 15a ePrivacy-RL 2002/58/EG iVm. Art 95 DSGVO) für Arbeitgeber mA nicht mehr zur Anwendung.[523]

Zweckänderungen

Eine Verschärfung des Datenschutzrechts für Arbeitgeber in Deutschland hinsichtlich des IT-gestützten Arbeitsplatzes bringt nach hA der europäische Grundsatz der Zweckbindung mit gleichzeitigen neuen Möglichkeit der Zweckvereinbarkeit (Art 5 Abs 1 lit b iVm. Art 6 Abs 4 DSGVO). Denn nach diesem Verständnis wird jede Verarbeitung, die der Erhebung der personenbezogenen Daten nachfolgt, als „Weiterverarbeitung" angesehen.[524] Nach hA kenne die DSGVO zu Weiterverarbeitungen also nur zwei Konstellationen:

- Weiterverarbeitung für „inkompatible Zwecke" (Art 6 Abs 4 Hs 1 DSGVO)
- Weiterverarbeitung für „kompatible Zwecke" (Art 6 Abs 4 Hs 2 DSGVO).[525]

Nach Rechtslage bis 24. Mai 2018 war eine Zweckänderung (trotz des an sich viel strengeren Grundsatzes der Zweckbindung mangels Zweckvereinbarkeit nach deutschem Recht[526]) uneingeschränkt möglich, wenn sich die Datenverarbeitung zum neuen Zweck auf eine neue Rechtsgrundlage stützen konnte.[527] Die entscheidendste Möglichkeit für Zweckänderungen

521 BT-Drs 18/11655, 14; 30 (jeweils zu Nummer 24); BAG Urteil v. 29. Juni 2017, Az 2 AZR 597/16, Rn 31 ff; *Schmidt*, RDV 2017/6, 284 ff. *Schmidt,* Datenschutz für „Beschäftigte (2016) 98.

522 *Petri* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel D Rn 60 ff; Kapitel D Rn 74 ff; Kapitel D Rn 115 ff. *Gola*, Datenschutz am Arbeitsplatz[5] (2014) 44 ff.

523 BT-Drs 19/2653, 9. (Antwort BReg Frage 20); *Heun* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) vor § 88 TKG Rn 16 ff; *Heun/Assion* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) Art 95 Rn 10 ff; Rn 19; *Geminn/Richter* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 8 Rn 68; *Geminn/Richter* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 4 Rn 211; Rn 224; *Holländer* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 95 Rn 4.

524 *Forgó/Hänold/Schütze*, The Principle of Purpose Limitation and Big Data in Corrales (Hrsg), New Technology, Big Data and the Law (2017) 29; *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff.

525 *Kastelitz/Hötzendirfer/Tschohl* in Knyrim (Hrsg), DatKomm (Stand 01.10.2018, rdb.at) Art 6 Rn. 59.

526 *Forgó/Krügel*, Die Subjektivierung der Zweckbindung, DuD 2005/12, 732 ff.

527 *Härting*, Zweckbindung und Zweckänderung im Datenschutzrecht, NJW 2015, 3284 (3285); *Helbing*, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 3/2015,

bei Verarbeitungen von nicht-öffentlichen (privaten) Stellen war dabei die rein interessensbasierte Zweckänderung gemäß § 28 Abs 2 Satz 1 Nr 1 BDSG aF.[528] Diese rein interessensbasierte Zweckänderung ist seit 25. Mai 2018 aber durch die DSGVO nach hM in Deutschland nicht mehr in dieser Form möglich. Um eine rechtskonforme Zweckänderung bei personenbezogenen Beschäftigtendaten machen zu können, bedarf es seit 25. Mai 2018 entweder des positiven Kompatibilitätstests gemäß Art 6 Abs 4 Hs 2 DSGVO oder es liegt gemäß Art 6 Abs 4 Hs 1 DSGVO eine qualifizierte Rechtsgrundlage im Unionsrecht bzw. nationalem Recht oder eine informierte freiwillige Einwilligung der betroffenen Beschäftigten vor, die die Zweckänderung legitimiert. „Qualifiziert" ist eine Rechtsvorschrift der Union oder des Mitgliedstaaten iSd. Art 6 Abs 4 Hs 1 DSGVO dann, wenn sie in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DSGVO genannten Ziele darstellt (vgl. Art 8 Abs 2 – Art 11 Abs 2 EMRK).[529] Folgt man dieser (aktuell) hM zur DSGVO, bedeutet das:

Geht der Kompatibilitätstest für den Arbeitgeber gemäß Art 6 Abs 4 Hs 2 DSGVO positiv aus, dürfen die Daten auch für den neuen Zweck verarbeitet werden.[530]

Geht der Kompatibilitätstest hingegen für den Arbeitgeber negativ aus und verfügt der Arbeitgeber auch über keine besonders „qualifizierte Rechtsgrundlage" oder eine informierte freiwillige Einwilligung der betroffenen Beschäftigten iSd. Art 6 Abs 4 Hs 1 DSGVO, kann ein Arbeitgeber bei einem geplanten aber inkompatiblen neuen Zweck – auch bei größter „Erforderlichkeit" iSd. § 26 Abs 1 BDSG bzw. bei einem noch so großen „berechtigtem Interesse" iSd. Art 6 Abs 1 lit f DSGVO auf seiner Seite – nicht (mehr) rechtskonform zweckgebundene personenbezogene Daten zu neuen inkompatiblen Zwecken rein interessensbasiert weiterverarbeiten. Selbst wenn der Arbeitgeber eine neue gültige Rechtsgrundlage fruchtbarmachen kann, ist dies für den Zweckbindungsgrundsatz gemäß Art 5 Abs 1 lit b DSGVO irrelevant, denn für inkompatible Zwecke iSd. Art 6 Abs 4 Hs 2 DSGVO kann seit 25. Mai 2018 nur noch eine „qualifizierte Rechtsgrundlage" iSd. Art 6 Abs 4 Hs 1 DSGVO eine Zweckänderung legitimieren.[531] Das EU-Datenschutzrecht trennt – anders als das bisherigen deutsche Datenschutzrecht BDSG aF – streng zwischen Zweckbindung / Zweckkompatibilität und Rechtmäßigkeit iSv. Rechtsgrundlage. Beides kann nicht (mehr) in einem zusammen betrachtet werden.[532] Diese erhebliche Problematik des Wegfalls der rein (partikulär-)interessensbasierten Zweckänderung für nicht-öffentliche Stellen in Deutschland hatte das Deutsche Bundesministerium des Inneren (BMI) in Berlin von Anbeginn im Rahmen der DSGVO-Verhandlung in Brüssel vor Augen und klar als großes Problem für Deutschland erkannt (ganz anders tlw. die Literatur, die wegen der Zweckkom-

145 (147 f.); *Eickelpasch*, Anpassung des deutschen Datenschutzrechts an die DSGVO, Sonderveröffentlichung zu RDV 06/2017, 7 f.

528 *Gola/Schomerus*, BDSG [aF][12] (2015) § 28 Rn 34 ff.

529 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 6 Rn 51 f.

530 *Schulz* in Gola (Hrsg), DS-GVO[2] (2018) Art 6 Rn 202 ff.

531 *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff; *Helbing*, K&R 3/2015, 147 f*; Eickelpasch*, Sonderveröffentlichung zu RDV 06/2017, 7; *Albrecht/Jotzo,* Das neue Datenschutzrecht der EU (2017) 76 f.

532 *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff.

patibilität der DSGVO sogar von einer „Aufweichung" des „strengen" deutschen Datenschutzes sprach und bzgl. einer Senkung des Datenschutzniveaus hinwies.[533]). Der deutsche BMI Referent *Eickelpasch* hatte hingegen die Anwendungsproblematik iZh. mit der Zweckkompatibilität völlig richtig erkannt und erklärte dazu: *„Artikel 5 Absatz 1, Buchstabe b, erster Halbsatz. Das ist alles nicht neu, aber wir haben es nie so recht umgesetzt im BDSG.* (…) *Im BDSG haben wir einen Ansatz im nicht-öffentliche Bereich, das ist alles interessenbasiert.* (…)*."*[534] Immer wieder wurde daher von deutscher Seite versucht den bisherigen rein interessensbasierten Ansatz für Zweckänderungen entsprechend dem § 28 Abs 2 Satz 1 Nr 1 BDSG aF in der DSGVO zu verankern. *Eickelpasch* erklärte: *„Wir haben ursprünglich im Rat mit der Brechstange Art. 6 Abs. 4 Satz 2 in der Fassung der Allgemeinen Ausrichtung des Rates § 28 Abs. 2 BDSG in seiner zweiten Fallgruppe hineinoperiert, also Weiterverarbeitung auf Basis berechtigter Interessen. Es folgte ein Aufschrei, sowohl im Rechtsdienst der Kommission als auch bei den Mitgliedstaaten."*[535] Der deutsche Vorschlag im Rat für eine rein interessensbasierte Zweckänderung aus der Perspektive des Verantwortlichen im Sinne der bisherigen deutschen Rechtslage (§ 28 Abs 2 Satz 1 Nr 1 BDSG aF) „überlebte" folglich aufgrund des großen Widerstands diverser EU-Mitgliedstaaten den Trilog in Brüssel nicht. *Eickelpasch* führte weiter aus: *„Dann ist, was erwartbar war, Art. 6 Abs. 4 Satz 2 [in der Fassung der Allgemeinen Ausrichtung des Rates] rausgefallen. Und man hat den Art. 6 Abs. 4 im Übrigen noch weiterentwickelt im Trilog und er hat die Gestalt angenommen, die wir jetzt alle kennen."*[536] Trotzdem wurden die intensiven Bemühungen des BMI zum Erhalt des § 28 Abs 2 BDSG aF für rein interessensbasierte Zweckänderungen für nicht-öffentliche Stellen nicht aufgegeben. Im 2. BMI Referentenentwurf vom November 2016 für das DSAnpUG-EU war in § 23 Abs 2 Nr 3 BDSG-2.Referentenentwurf DSAnpUG-EU erneut die nationale Weiterführung des § 28 Abs 2 BDSG aF vorgesehen, die geplante Bestimmung lautete: *„Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nicht-öffentliche Stellen ist über Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 hinaus nur zulässig, wenn* (Nr 3) *sie zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist"*.[537] BMI Referent *Eickelpasch* erklärte zu dieser Bestimmung des 2. BMI Referentenentwurfs vom November 2016: *„Wir bleiben also in der Konzeption des § 28 Abs 2. Hier kommen wir in eine strittige Diskussion. Erstens, dürfen wir das überhaupt? Man kann sagen, nein, man kann sagen, ja. Beide Varianten sind natürlich rechtlich mit guten Gründen darlegbar. Wir meinen, ja. Und wollen wir? Da meinen wir auch, ja. Und zwar deshalb, weil wir nicht so ganz sicher sind, wie weit die Kompatibilität reicht und wir gerne das weiterlaufen lassen wollen, was bislang nach BDSG auch lief."*[538] In der finalen im Deutschen Bundestag dann eingelangten BT-Drs 18/11325 zum DSAnpUG-EU findet sich diese

533 z.B. im Jahr 2016: *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) § 2 Rn 38 ff; aktuelle Auflage: *Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis[2] (2019) § 2 Rn 44 ff.

534 *Eickelpasch*, Sonderveröffentlichung zu RDV 06/2017, 7 f.

535 *Eickelpasch*, Sonderveröffentlichung zu RDV 06/2017, 9.

536 *Eickelpasch*, Sonderveröffentlichung zu RDV 06/2017, 9.

537 *Bundesministeriums des Innern*, Referentenentwurf des Bundesministeriums des Innern Stand: 2. Ressortabstimmung (11.11.2016 16:13), Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU, 24 f.

538 *Eickelpasch*, Sonderveröffentlichung zu RDV 06/2017, 8.

Bestimmung (§ 23 Abs 2 Nr 3 BDSG-2.Referentenentwurf DSAnpUG-EU) nicht mehr im nunmehrigen und aktuell gültigen § 24 BDSG. Dies führt nun dazu, dass es seit 25. Mai 2018 – mangels Möglichkeit der rein interessensbasierten Zweckänderung (§ 28 Abs 2 BDSG aF) – zu der oben beschriebenen faktischen Verschärfung des Zweckbindungsgrundsatzes für Arbeitgeber in Deutschland kommt. Für deutsche Verantwortliche ist dadurch die Möglichkeit der rein interessensbasierten Zweckänderung (§ 28 Abs 2 BDSG aF) völlig weggefallen, was viel gravierender ist, als die Möglichkeit der zweckkompatiblen Weiterverarbeitung.[539] Einzige Rechtsgrundlage zu Zweckänderungen für nicht-öffentliche Stellen – abseits des Kompatibilitätstests gemäß Art 6 Abs 4 Hs 2 DSGVO – ist § 24 Abs 1 BDSG als „qualifizierte Rechtsgrundlage" iSd. Art 6 Abs 4 Hs 1 DSGVO.[540]

Eine andere Ansicht vertritt *Roßnagel*, der – bei technisch identischen Verarbeitungsschritten in der Realität – juristisch zwischen „neuer Datenverarbeitung" (Art 6 Abs 1 DSGVO) und „Weiterverarbeitung" (Art 6 Abs 4 DSGVO) unterscheidet: „*Die Einordnung* (…) *als Weiterverarbeitung ist dann möglich, wenn der Sekundärzweck mit dem Primärzweck vereinbar ist. Ist er dies nicht, kann die gleiche Handlung als (neue) Datenverarbeitung vorgenommen werden, wenn der Verantwortliche sich auf einen eigenen Erlaubnistatbestand (im Beispielfall der berechtigten Interessen) für die als Zweckänderung einzuordnende neue Datenverarbeitung beziehen kann.*"[541] Eine vergleichbare Ansicht zu *Roßnagel* vertreten *Laue/Kremer*.[542] Diese beiden Ansichten entsprechen jedoch nicht dem Verständnis der *Art 29 Datenschutzgruppe* und der Literatur, die als „Weiterverarbeitung" jede Verarbeitung ansieht, die der Erhebung der personenbezogenen Daten nachfolgt:[543] „*Any processing steps following the collection of the personal data are to be seen as further processing of personal data, regardless of whether the processing is for the purpose initially specified or for any additional purpose.*"[544]

Die Praxis wird letztlich zeigen, ob sich diese Ansicht *Roßnagels* zur datenschutzrechtlichen Unterscheidung zwischen „neuer" Datenverarbeitung und „zweckkompatibler Weiterverarbeitung" bei in der Realität jeweils technisch identen Verarbeitungsvorgängen europaweit durchsetzen wird.[545]

Ob auch § 26 Abs 1 BDSG selbst zugleich eine qualifizierte Rechtsvorschrift iSd. Art 6 Abs 4 Hs 1 DSGVO für inkompatible Zweckänderungen im Beschäftigtenverhältnis sein soll, ist mA unklar. Es findet sich kein Hinweis in § 26 BDSG bzw. in den Materialien (BT-Drs 18/11325, S. 96 ff.). Es handelt es sich bei § 26 BDSG iVm. Art 88 DSGVO jedenfalls

539 BT-Drs 18/11325, 28 f; *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff; *Helbing*, K&R 3/2015, 147 f.

540 BT-Drs 18/11325, 96.

541 *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann (Hrsg), Datenschutzrecht (2019) Art 5 Rn 99.

542 *Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis[2] (2019) § 2 Rn 44 ff.

543 *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff; *Forgó/Hänold/Schütze*, The Principle of Purpose Limitation and Big Data in Corrales (Hrsg), New Technology, Big Data and the Law (2017) 29; *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff.

544 *Forgó/Hänold/Schütze*, The Principle of Purpose Limitation and Big Data in Corrales (Hrsg), New Technology, Big Data and the Law (2017) 29.

545 *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann (Hrsg), Datenschutzrecht (2019) Art 5 Rn 96 ff.

um eine Norm zum Schutz der Ziele des Art 23 Abs 1 lit i DSGVO. Die *Datenschutzkonferenz* bezeichnet § 26 BDSG folglich als „*besondere gesetzliche Grundlage*“, für Zweckänderungen stellt die *Datenschutzkonferenz* aber trotzdem auf den Kompatibilitätstest (Art 6 Abs 4 Hs 2 DSGVO) bzw. auf die Rechtsgrundlage für inkompatible Zweckänderungen in § 24 BDSG ab. Gemäß *Datenschutzkonferenz* muss bei neuen Verwendungszwecken von Beschäftigtendaten immer ein innerer Zusammenhang zum Beschäftigtenverhältnis im weitesten Sinne bestehen, ansonsten klare Zweckinkompatibilität (Art 6 Abs 4 Hs 2 DSGVO) vorliege (z. B. Verkauf an Dritte zu Werbezwecken). Die *Datenschutzkonferenz* geht nicht davon aus, dass § 26 BDSG eine Vorschrift iSd. Art 6 Abs 1 Hs 1 DSGVO ist, die inkompatible Zweckänderungen im Beschäftigtenverhältnis legitimieren soll.[546]

Liegt keine Zweckkompatibilität, keine qualifizierte Rechtsgrundlage oder eine informierte freiwillige Einwilligung für inkompatible Zweckänderungen vor, hat der Verantwortliche nach hM (aA *Roßnagel*) datenschutzrechtlich wieder „bei Null“ anzufangen. Das heißt der Verantwortliche darf nach *Buchner/Petri* bzw. *Tinnefeld/Buchner/Petri/Hof* nicht auf vorhandene Datenbestände zurückgreifen, da eine Rechtsgrundlage wie § 28 Abs 2 BDSG aF fehlt.[547]

Zweckänderungen sind zusammengefasst – ohne eine informierte freiwillige Einwilligung der betroffenen Beschäftigten – in folgender Form nach (aktuell) hM möglich:

- Zweckänderungen personenbezogener Daten zur unternehmensinternen Aufklärung und Verfolgung von Straftaten stützen sich direkt auf § 24 Abs 1 Nr 1 BDSG (kein Kompatibilitätstest nach Art 6 Abs 4 Hs 2 DSGVO erforderlich).[548]
- Zweckänderungen zur unternehmensinternen Aufklärung und Verfolgung von Ordnungswidrigkeiten können sich (mangels Straftaten) nicht[549] auf § 24 Abs 1 Nr 1 BDSG berufen und bedürfen in jedem Fall des Kompatibilitätstest gemäß Art 6 Abs 4 Hs 2 DSGVO[550];
- Zweckänderungen zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche stützen sich unmittelbar auf § 24 Abs 1 Nr 2 BDSG (kein Kompatibilitätstest nach Art 6 Abs 4 Hs 2 DSGVO erforderlich).[551]
- Zweckänderungen bei nicht-öffentlichen Stellen zu rein sonstigen privat-wirtschaftlichen Zwecken bedürfen immer des Kompatibilitätstest (Art 6 Abs 4 Hs 2 DSGVO).[552]

Folgt man hingegen der Ansicht *Roßnagels*, wären mit Art 6 Abs 4 DSGVO inkompatible und damit unerlaubte Zweckänderungen aber als „neue“ Datenverarbeitung mit erneuter

546 *Datenschutzkonferenz,* Kurzpapier Nr. 14 Beschäftigtendatenschutz (2018) 3 f; *Gola/Jaspers*, Zweckänderungen bei der Weiterverarbeitung von Beschäftigtendaten, RDV 3/2018, 145 ff (149 ff).

547 *Buchner/Petri* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) Art 6 Rn 185; *Tinnefeld/Buchner/Petri/Hof,* Einführung in das Datenschutzrecht[6] (2018) 240; aA *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann (Hrsg), Datenschutzrecht (2019) Art 5 Rn 96 ff.

548 BT-Drs 18/11325, 96.

549 *Herbst* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) § 24 BDSG Rn 7 ff.

550 *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff.

551 *Herbst* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) § 24 BDSG Rn 13 f.

552 *Herbst* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) § 24 BDSG Rn 7 ff; *Gola/Jaspers*, RDV 3/2018, 145 ff (149 ff); *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff.

vollständiger DSGVO-Konformitätsprüfung bei positiven Ausgang jeweils immer neu legitimierbar, obwohl es sich dabei in der Realität um technisch identische Verarbeitungsschritte handelt.[553]

3.5.4 Österreich – Beschäftigtendatenschutz IT-gestützter Arbeitsplatz

Modell der stufenweisen Kontrollverdichtung

Das österreichische Datenschutzrecht für Private (nicht-öffentliche Stellen) kennt keine eigenen Beschäftigtendatenschutzbestimmungen.[554]

Die §§ 92 ff iVm. § 108 TKG 2003 sind in Österreich auch bei erlaubter Privatnutzung im Beschäftigtenverhältnis nicht anwendbar.[555] Durch die ePrivacy-VO wird sich an der bisherigen Situation der alleinigen Anwendbarkeit der DSGVO (DSG) im Beschäftigtenverhältnis nichts ändern.[556]

In Österreich hat sich in der datenschutzrechtlichen Betrachtung der betrieblichen Datenverarbeitung im Zusammenhang mit dem IT-gestützten Arbeitsplatz das *„Modell der stufenweisen Kontrollverdichtung"* durchgesetzt. Dieses von *Kotschy/Reimer*[557] – nach dem Vorbild der „*Introduction on the use oft the Council of Europe's informaton system*" des Europarats – entwickelte Modell der stufenweisen Kontrollverdichtung sieht eine insofern stufenweise und jeweils verhältnismäßige Zulässigkeit von Kontrollmöglichkeiten des Arbeitgebers gegenüber Beschäftigten hinsichtlich der betrieblichen IKT Nutzung aufgrund unterschiedlicher erforderlicher Zwecke und berechtigter Interessen vor. Das Modell der stufenweisen Kontrollverdichtung setzt eine umfassende transparente Information aller Beschäftigten durch den Arbeitgeber über die tatsächlich im Unternehmen stattfindenden Kontrollen gemäß den 3-Stufen und deren konkreten Zwecke je Stufe vor Beginn der Verarbeitung voraus (Art 5 Abs 1 lit a iVm. Art 14 DSGVO).

Bei rein dienstlicher Nutzung und damit nicht-erlaubter Privatnutzung stützt sich die Verarbeitung im Rahmen der stufenweisen Kontrollverdichtung für die Zwecke der Stufe 1 (Gewährleistung der Systemfunktionalität) und Stufe 2 (Abstellen von signifikanten Abweichungen von der üblichen IT-Nutzung) auf das berechtigte Interesse gemäß Art 6 Abs 1 lit f DSGVO als Rechtsgrundlage vor dem Hintergrund der gesetzlichen Pflicht (Art 32 DSGVO) geeignete technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung zu treffen.[558] Bei erlaubter Privatnutzung werden zusätzlich auch besondere

553 *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann (Hrsg), Datenschutzrecht (2019) Art 5 Rn 96 ff.

554 *Schmidt,* Datenschutz für „Beschäftigte" (2016) 75.

555 OGH 13.06.2002, Ob A 288/01p; *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.1; *Kotschy*, Datenschutz in systematischer Einordnung zum Arbeitsrecht in Brodil (Hrsg), Datenschutz im Arbeitsrecht Mitarbeiterüberwachung versus Qualitätskontrolle. Wiener Oktobergespräche 2009 (2010) 1 ff (11).

556 ErwGr 13 letzter Satz iVm. Art 2 Abs 2 lit c ePrivacy-VO (ausschließlich nur öffentlich-zugängliche Kommunikationsdienste von der ePrivacy-VO erfasst).

557 *Kotschy/Reimer*, Die Überwachung der Internet-Kommunikation am Arbeitsplatz, ZAS 2004, 29.

558 *Art 29 Datenschutzgruppe*, WP 118 (2006) 5 ff; *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff.

Kategorien von personenbezogenen Daten gemäß Art 9 Abs 1 DSGVO (z.B. Aufruf Website politischer Parteien, Kommunikation mit Ärzten, usw.) im Rahmen der stufenweisen Kontrollverdichtung verarbeitet (analysiert, gefiltert). Es bieten sich zwei Lösungen für eine rechtskonforme Verarbeitung, der durch die erlaubte Privatnutzung auf Stufe 1 und Stufe 2 stattfindende Verarbeitung besonderer Kategorien personenbezogener Daten, an:

- Das Unternehmen verbietet im ersten Schritt generell die Privatnutzung und erlaubt in einem zweiten Schritt nur mehr solchen Beschäftigten die Privatnutzung, die der Überwachung ihres Internetverkehrs im entsprechend informierten und transparenten Umfang (Art 5 Abs 1 lit a iVm. Art 14 DSGVO) ausdrücklich zustimmen (Art 9 Abs 2 lit a DSGVO). Die Freiwilligkeit einer solchen Arbeitnehmer-Einwilligung zur Privatnutzung der IT ist aufgrund des damit verbundenen wirtschaftlichen Vorteils für Beschäftigte gegeben.[559] In Unternehmen ohne Betriebsrat stellt diese Arbeitnehmer-Einwilligung sogar die einzige Möglichkeit dar, bei erlaubter Privatnutzung die Verarbeitung der besonderen Kategorien von personenbezogenen Daten im Rahmen der stufenweisen Kontrollverdichtung rechtskonform zu legitimieren.[560] Mit einer solchen ausdrücklichen freiwilligen datenschutzrechtlichen Einwilligung (Art 9 Abs 2 lit a DSGVO) des Beschäftigten kann mA nämlich auch zugleich die obligatorische arbeitsrechtliche Einwilligung des Beschäftigten gemäß § 10 AVRAG in die Kontrollmaßnahme bei Betrieben ohne Betriebsrat rechtssicher eingeholt werden.[561]
- Oder das Unternehmen stützt sich auf die Rechtsgrundlage Art 9 Abs 2 lit b Alt. 2. DSGVO, wo in Form einer Betriebsvereinbarung die „geeigneten Garantien" für die Betroffenen konkretisiert werden können, weil aktuell mA nicht rechtssicher ist, ob die arbeitsrechtliche Erforderlichkeit (z.B. iSd. § 16 ABGB)[562] zugleich die „geeigneten Garantien" iSd. Art 9 Abs 2 lit b Alt. 2. DSGVO schaffen kann[563] (vgl. **Kapitel. 3.5.4**). Bei Kontrollen im Rahmen der erlaubten Privatnutzung ist ohnehin eine Betriebsvereinbarung nach § 96 Abs 1 Z 3 ArbVG (Berühren der Menschenwürde) bzw. – bei Sicherstellung der Anforderungen nach OGH-„Wandlungsthese" – zumindest eine Betriebsvereinbarung nach § 96a Abs 1 Z 1 ArbVG erforderlich.[564] Diese auch nach Art 9 Abs 2 lit b DSGVO mögliche Betriebsvereinbarung müsste inhaltlich die dort genannten

559 BT-Drs 18/11325, 97.

560 *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff; BT-Drs 18/11325, 97.

561 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 10 AVRAG Rn 2 ff; ErläutRV 1590 BlgNR 18. GP 128.

562 *Brodil,* Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 9; *Brodil/Risak,* Arbeitsrecht in Grundzügen[10] (2019) Rn 43a; *Brodil*, ecolex 2018, 486 (488); *Brodil*, Datenschutz und Arbeitsrecht – Was ändert sich durch die Datenschutz-Grundverordnung? DRdA 2018, 463 (468); *Brodil*, Sensible Daten im Arbeitsverhältnis – Nochmals zur Erfassung von § 9 Z 11 DSG 2000, in Kietaibl/Schörghofer/Schrammel (Hrsg), Rechtswissenschaft und Rechtskunde – Liber Amicorum für Robert Rebhahn (2014) 1 ff (5).

563 *Kastelitz/Hötzendirfer/Tschohl* in Knyrim (Hrsg), DatKomm (Stand 01.10.2018, rdb.at) Art 9 Rn. 36.

564 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.168 ff.

Anforderungen („geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“)[565] erfüllen, was das Modell der stufenweisen Kontrollverdichtung[566] mA gewährleistet. Damit werden mA sowohl die Anforderungen an „geeignete Garantien“ in einer Betriebsvereinbarung nach Art 9 Abs 2 lit b DSGVO, als auch die Anforderungem aus der Rechtsprechung des OGH zur „Wandlungsthese“ zu § 96a ArbVG erfüllt.[567] *Goricnik/Grünanger* führen als Beispiel für „Garantien“ iSd. OGH „Wandlungsthese“ an, dass man den Zugriff auf bestimmte personenbezogene Daten zur Kontrolle der Beschäftigten so regeln könnte, dass ein Zugriff für den Arbeitgeber im ersten Schritt nur pseudonymisiert möglich wäre und ein re-identifizierender Zugriff bzw. eine konkret personenbezogene Auswertung nur dann für den Arbeitgeber möglich wird, wenn der Arbeitgeber (bzw. System-Administrator) und der Betriebsrat gemeinsam ein Passwort eingeben („4-Augen-Prinzip“).[568]

Die durch die Stufen 1 und Stufen 2 gewährleistete stufenweise Kontrollverdichtung gegenüber den Beschäftigten darf vom Arbeitgeber nur dann übersprungen werden, wenn ein begründeter Verdacht auf eine strafbare Handlung oder schwere Pflichtverletzung durch den Beschäftigten vorliegt.[569] Die Rechtsgrundlagen für die eingriffsintensive Stufe 3 (Vorliegen eines konkreten Verdachts auf Vertrags- oder Rechtsverletzung) finden sich in Art 6 Abs 1 lit f DSGVO (berechtigte Interessen), § 4 Abs 3 DSG (strafrechtlich relevante Daten) und hinsichtlich besonderer Kategorien personenbezogener Art 9 Abs 2 lit b (mA mit BV) oder lit f DSGVO (Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen). Im Detail:

- *Stufe 1 (Gewährleistung der Systemfunktionalität)*

Auf dieser Stufe 1 erfolgt eine reine maschinelle Überwachung zur Gewährleistung der Systemfunktionalität. Der Arbeitgeber hat ein Recht (Grundrecht auf Eigentum) als Eigentümer der betrieblichen IT-Infrastruktur und Ausstattung, jene Maßnahmen zu setzen, die notwendig sind, um die Funktionsfähigkeit (Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit) der eigenen betrieblichen IT zu gewährleisten. Es erfolgt eine maschinelle Routineprüfung der Kommunikationsvorgänge, es werden also alle erforderlichen Maßnahmen gesetzt, die zur Abwehr von Viren und sonstigen Attacken von Unbefugten auf das IT-System am Stand der Technik erforderlich sind. Das Filtern von elektronischer Kommunikation und das Aufbrechen von (SSL/TLS)-Verschlüsselungen zum Erkennen von Viren und Spam ist durch die gesetzliche Verpflichtung an den Verantwortlichen geboten, geeig-

565 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.97 ff.

566 *Kotschy/Reimer*, ZAS 2004, 29.

567 OGH 13.06.2002, Ob A 288/01p; *Kastelitz/Hötzendirfer/Tschohl* in Knyrim (Hrsg), DatKomm (Stand 01.10.2018, rdb.at) Art 9 Rn. 36; *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff.

568 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.171.

569 *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 6.45 ff; *Kustor,* Unternehmensinterne Untersuchungen (2010) 97 f.

nete technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung zu treffen (Art 5 Abs 1 lit f iVm. Art 32 DSGVO).[570] *Kotschy/Reimer* führen aus: *„Selbstverständlich muss zur Abwehr von Viren der Inhalt der Kommunikation geprüft werden – nur darf dies im Normalfall als gelindestes Mittel nur maschinell erfolgen, wozu auch zahlreiche Virenschutzprogramme entwickelt wurden und eingesetzt werden."*[571] Auf dieser Ebene ist eine Unterscheidung zwischen dienstlicher und privater Kommunikation nicht möglich, da die Bedrohung der Systemfunktionalität sowohl im Rahmen der dienstlichen als auch der privaten Kommunikation gleichermaßen erfolgt. Soweit überhaupt Menschen von den Kommunikationsdaten Kenntnis erlangen, handelt es sich um Systemadministratoren, die im Verständnis des § 119 StGB nicht als „unbefugt" angesehen werden[572]: *„Täter muss ein Unbefugter sein. Fallkonstellationen, in denen etwa Systemadministratoren befugterweise (den Inhalt von) E-Mails analysieren, sind – ohne dass dies audrücklich gesagt werden müsste – von der Strafbarkeit ausgenommen."*[573] Die Verhältnismäßigkeit der Maßnahme ergibt sich aus der klaren Zweckbindung (Gewährleistung der Systemfunktionalität) und die Beschränkung auf befugte Systemadministratoren der IT-Abteilung.[574] *Brodil* stellt aus arbeits- und datenschutzrechtlicher Sicht klar, dass „*ein Zugriff auf dienstliche und private Verkehrs- bzw. Zugangsdaten – somit auf klassische äußere Verbindungsdaten – nach Information* [Art 14 DSGVO] *als zulässig anzusehen [ist]",* weil ein legitimes Kontrollinteresse besteht.[575] Trotz der an die Allgemeinheit adressierten § 93 Abs 3 TKG 2003 iVm. §§ 119, 119a StGB besteht auf Stufe 1 nur ein geringes Strafbarkeitsrisiko, da die Verwendung von Spam- und Virenfiltern aus strafrechtlicher Sicht nicht per se auf die Kenntniserlangung von Nachrichten bzw. Daten am Übertragungsweg abzielt und zudem Systemadministratoren in Unternehmen vom österreichischen Gesetzgeber nicht als unbefugt angesehen werden, eine Einschau zum Zweck der Gewährleistung der Systemfunktionalität in die elektronische Kommunikation zu halten, die an das Unternehmen und die Mitarbeiter adressiert ist.[576]

---

570 *Art 29 Datenschutzgruppe*, WP 118 (2006) 5 ff; *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff; *Kotschy/Reimer*, ZAS 2004, 29.

571 *Kotschy/Reimer*, ZAS 2004, 29; *Kotsch*y, Datenschutz in systematischer Einordnung zum Arbeitsrecht in Brodil (Hrsg), Datenschutz im Arbeitsrecht Mitarbeiterüberwachung versus Qualitätskontrolle. Wiener Oktobergespräche 2009 (2010) 1 ff (11 ff.).

572 *Fabrizy*, StGB[13] (2018) § 119 Rn 4.

573 ErläutRV 1166 BlgNR 20. GP 24.

574 *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 6.45 ff; *Knyrim,* Datenschutzrecht[3] (2015) 265 f; *Kustor,* Unternehmensinterne Untersuchungen (2010) 97 f; *Brodil,* Individualarbeitsrechtliche Fragen der Kontrolle des Arbeitnehmers, in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund neuer Medien (2005) 87 f; *Hattenberger,* Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund neuer Medien (2005) 42 f; *Kotschy/Reimer*, ZAS 2004, 29.

575 *Brodil* in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund neuer Medien (2005) 81.

576 *Lewisch* in Höpfel/Ratz (Hrsg), WK StGB[2] (Stand: Stand 17.10.2017) § 119 Rn 10; *Reindl-Krauskopf* in Höpfel/Ratz (Hrsg), WK StGB[2] (Stand: Stand 17.10.2017) § 119a Rn 11 ff; ErläutRV 1166 BlgNR 20. GP 24.

- *Stufe 2 (Signifikante Abweichung von der üblichen System und IT-Nutzung)*

Wird eine Gefahr für die Systemfunktionalität der betrieblichen IT-Systeme erkannt (Virenbefall, anormaler Download umfangreicher Dateien, etc.), darf die IT-Abteilung zu diesem konkretem Fall eine personenbezogene Auswertung vornehmen, also den konkreten User ausforschen bei dem das maschinell entdeckte Problem auftritt bzw. der dafür verantwortlich sein könnte. Dieser Zweck der Datenverarbeitung ist datenschutzrechtlich kritischer als Stufe 1, denn es führt üblicherweise zur Kenntnisnahme der aufgekommenen Abweichungsdaten durch ein Organ des Arbeitgebers. Es sollte also nur tatsächlich relevanten Abweichungen nachgegangen werden und nicht bereits geringfügige Abweichungen systemseitig bei der IT-Abteilung anschlagen, weil es sonst zu einer unverhältnismäßigen Kontrolle der Arbeitnehmer kommen würde. Wird eine echte abweichende Nutzung durch die IT-Abteilung festgestellt, sollte die IT-Abteilung den jeweiligen Nutzer (Beschäftigter) persönlich informieren und aufklären, dass ein Problem besteht, damit dieser sein Verhalten abstellt bzw. korrigiert. Der konkrete Vorgesetzte des Beschäftigten darf noch nicht personenbezogen darüber informiert werden, sondern lediglich von einer problematischen IT-Nutzung in seiner Abteilung in anonymer Form. Der betroffene Beschäftige selbst kann sich wiederum vertrauensvoll an den Datenschutzbeauftragten – falls vorhanden – gemäß Art 38 Abs 4 DSGVO wenden. Über gelöste und in Gesprächen mit betroffenen Mitarbeitern letztlich erfolgreich aufgeklärte und wirksam abgestellte Anlassfälle durch die IT-Abteilung, sollte eine innerbetriebliche Verschwiegenheitspflicht gegenüber dem Vorgesetzten der jeweiligen Beschäftigten bestehen. Die IT-Abteilung ist auf Stufe 2 vergleichbar einer „Black Box", wo nur die betriebliche IT-Abteilung, der konkret betroffene Beschäftige und ggf. der betriebliche Datenschutzbeauftragte (Art 38 Abs 4 DSGVO) Kenntnis von dem dann erfolgreich gemeinsam geklärten problematischen Vorfall haben dürfen. Die IT-Abteilung ist also auf Stufe 2 der Eskalationsebene im Modell der stufenweisen Kontrollverdichtung zur absoluten innerbetrieblichen Verschwiegenheit verpflichtet, der Datenschutzbeauftragte unterliegt einer gesetzlichen Verschwiegenheitspflicht (Art 38 Abs 5 DSGVO iVm. § 5 DSG 2018).[577] Führen diese gelinderen Maßnahmen aber dennoch nicht zum Erfolg, greift Stufe 3:

- *Stufe 3 (Vorliegen eines konkreten Verdachts auf Vertrags- oder Rechtsverletzung)*

Maßnahmen auf Stufe 3 sind einzuleiten, wenn Stufe 2 zu keinem positiven Ergebnis führt (z.B. Beschäftigter stellt rechtswidrige IT-Nutzung trotz Sensibilisierung durch IT-Abteilung auf Stufe 2 nicht ein). Zudem ist das Überspringen der Stufe 1 und Stufe 2 hinsichtlich der Intensität einer Kontrollmaßnahme durch den Arbeitgeber zusätzlich bei einem konkret begründeten Verdacht auf eine strafbare Handlung oder schwere Pflichtverletzung durch den Beschäftigten aufgrund überwiegend berechtigter Interessen des Arbeitgebers möglich. Dies wäre insbesondere bei Datenverarbeitung in Gewinn- und Schädigungsabsicht (§ 63 DSG), erheblichen Verstößen gegen die Anforderungen der DSGVO (Art 5 ff; Art 83 Abs 4 u. Abs 5 DSGVO), Betriebsspionage (§§ 123 f StGB, §§ 11, 26a ff UWG), NS-Propa-

577 *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 6.45 ff; *Knyrim,* Datenschutzrecht[3] (2015) 265 f; *Kustor,* Unternehmensinterne Untersuchungen (2010) 97 f.

ganda (§§ 3 – 3d Verbotsgesetz), etc. sowie auch bei einem durch das pflichtwidrige Handeln des Beschäftigten unmittelbar drohenden Systemabsturz der Fall.[578] Der Vorgesetzte des Beschäftigten wird auf Stufe 3 (in der Regel) über den bestehenden Verdacht gegen seinen Mitarbeiter informiert und es werden erste Aufklärungsmaßnahmen eingeleitet. Ab diesem Zeitpunkt ist auch der Betriebsrat von diesem Schritt und den dazu ausgewerteten personenbezogenen Daten zu informieren sowie über das Gespräch mit dem Vorgesetzten. Zur internen Aufklärung von im Rahmen des Beschäftigtenverhältnis begangenen Straftaten oder schweren Pflichtverletzungen (Stufe 3) darf gemäß Art 6 Abs 1 lit f DSGVO bzw. § 4 Abs 3 DSG (berechtigte Interessen) bzw. Art 9 Abs 2 lit b (arbeitsrechtliche Erforderlichkeit und geeignete Garantien) bzw. lit f (Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen) DSGVO Einsicht in Verkehrs- und Inhaltsdaten des Beschäftigten vorgenommen werden. Für einen Eingriff muss ein legitimes Kontrollinteresse im sachlichen Zusammenhang mit der arbeitsvertraglich geschuldeten Leistung vorliegen oder der Verdacht auf eine Straftat vorliegen, die während der Arbeitszeit begangen wurde oder – wenn außerhalb der Arbeitszeit begangen – sich gegen den Arbeitgeber richtete. *Kotschy/Reimer* führen aus: *„Soweit zur Aufklärung des Verdachts der Zugriff auf Kommunikationsdaten – Verkehrsdaten wie auch Inhaltsdaten – notwendig ist, kann dem Arbeitgeber das Grundrecht auf Datenschutz nicht prinzipiell eingewendet werden, sondern nur allenfalls hinsichtlich der Einhaltung geeigneter Garantien für den Schutz des Betroffenen in der Durchführung der Kontrollmaßnahme.“*[579]

Auf Stufe 3 ist zu unterscheiden zwischen dem Zugriff auf dienstliche oder private Daten:

- Der Arbeitgeber darf rein dienstliche elektronische Korrespondenz (E-Mail, Chats, etc.) verarbeiten und einsehen, unabhängig ob Verdachtsmomente gegen den Mitarbeiter vorliegen oder nicht. Es besteht ein überwiegend berechtigtes Interesse des Arbeitgebers an der Einsicht in dienstliche Korrespondenz. Dies entspricht dem immer schon anerkannten Einsichtsrecht des Arbeitgebers in die dienstliche Briefkorrespondenz. Hintergrund ist der notwendige Zugriff des Arbeitgebers auf alle dienstlichen Inhaltsdaten z.B. im Zusammenhang mit der Archivierung und Verwaltung der geschäftlichen Korrespondenz (z.B. § 132 BAO, § 212 UGB).[580] Nach *Brodil* sollte sich der Arbeitgeber bei der Einsicht in elektronische dienstliche Korrespondenz jedoch auf Kommunikation im Namen des Arbeitgebers beschränkten. Zusätzlich besteht auch ein berechtigtes Interesse des Zugriffs auf dienstliche Kommunikation zur Aufklärung von arbeitsrechtlichen oder strafrechtlichen Verstößen (Art 6 Abs 1 lit f DSGVO bzw. § 4 Abs 3 DSG).[581] Klar rechtswidrig ist eine anlasslose lückenlose Überwachung des Beschäftigten, auch

578 *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 6.45 ff; *Knyrim,* Datenschutzrecht[3] (2015) 265 f; *Kustor,* Unternehmensinterne Untersuchungen (2010) 97 f; *Oberhofer,* Datenschutz und Arbeitsrecht in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 496 f.

579 *Kotschy/Reimer*, ZAS 2004, 29.

580 *Felten/Mosler,* IKT am Arbeitsplatz: Nutzung und Kontrolle in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 494; *Brodil* in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund neuer Medien (2005) 81 f;

581 *Brodil*, ZAS 2018/33, 203 (205 f.); *Busch/Falb,* Erhebung und Verarbeitung von Arbeitnehmerdaten in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 48 ff; *Brodil* in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund neuer Medien (2005) 81 f; *Brodil*, ZAS 2004, 156 (160 f.).

wenn sich diese arbeitgeberseitige Überwachung nur auf rein dienstliche Daten beschränken würde.[582]

- Der Zugriff auf private Daten des Beschäftigten durch den Arbeitgeber ist aus Sicht des Persönlichkeitsschutzes des Art 8 Abs 1 EMRK grundsätzlich unzulässig und nur in wenigen Ausnahmefällen denkbar.[583] Beim Datenzugriff auf Endgeräten bei erlaubter Privatnutzung der IKT-Infrastruktur hat der Arbeitgeber mit verschiedenen Maßnahmen sicherzustellen, dass grundsätzlich nur in dienstliche Kommunikation eingesehen wird (Heranziehung der Verkehrsdaten zur Feststellung ob private oder dienstliche E-Mail; oder z.B. Einsicht in die Betreffzeile der E-Mail ob privat oder dienstlich; oder den Arbeitnehmer selbst befragen).[584] Trotzdem bleibt es dabei, dass private Daten des Beschäftigten bei Offenkundigkeit des privaten Charakters vom Arbeitgeber nicht eingesehen werden dürfen. Eine Durchbrechung dieses hohen Schutzbereiches für private Daten besteht ausschließlich nur in besonderen Verdachtslagen. Ein Arbeitgeber darf in private Daten eines Beschäftigten rechtskonform Einsicht nehmen, bei begründeten Verdacht von Straftaten oder schweren Vertragsverletzungen (Verrat von Geschäftsgeheimnissen, Mobbing, sexuelle Belästigung, etc.). Der OGH geht davon aus, dass einem Arbeitgeber die Möglichkeit zugestanden werden muss, bei Vorliegen ausreichender Verdachtsmomente für ein vertragswidriges, seinen Interessen zuwiederlaufendes Verhalten des Beschäftigten, durch geeignete Nachforschungen Klarheit zu gewinnen. In solchen Konstellationen ist eine Einschau in offensichtlich private Daten zulässig und von einem berechtigten Interesse des Arbeitgebers gedeckt (Art 6 Abs 1 lit f DSGVO, § 4 Abs 3 Z 2 DSG, Art 9 Abs 2 lit b / lit f DSGVO).[585]

Zusätzlich ist bei einem Zugriff auf Beschäftigtendaten (sowohl dienstlich als auch privat) noch streng zu unterscheiden zwischen Daten, die sich noch am Übertragungsweg befinden, und Daten, die bereits lokal am Endgerät bzw. Laufwerk des Beschäftigten gespeichert sind. Hinsichtlich der noch am Übertragungsweg befindlichen (privaten) Kommunikationsdaten (Telefon, E-Mail, Chats, etc.) greift in jeden Fall der an jedermann adressierte § 93 Abs 3 TKG 2003. Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten durch andere Personen als einen Benutzer[586] ohne Einwilligung aller beteiligten Benutzer ist rechtwidrig (§ 119 StGB, § 119a StGB)[587]. Geschützt werden nur die am Übertragungsweg befindlichen

582 *Knyrim,* Datenschutzrecht[3] (2015) 261 ff (264); *Brodil*, ZAS 2018/33, 203 (205 f.); *Goricnik,* Kontrolle Internet/E-Mail am Arbeitsplatz, Dako 2016/1, 7 ff (8).

583 *Brodil* in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund neuer Medien (2005) 77; 87 f; *Felten/Mosler* in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 494; *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 6.16 ff.

584 *Brodil*, ZAS 2004, 156 (161); *Felten/Mosler* in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 494; *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 BDSG Rn 124.

585 *Brodil* in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund neuer Medien (2005) 81 f; *Brodil*, ZAS 2004, 156 (161 f.); *Rebhahn*, Mitarbeiterkontrolle am Arbeitsplatz (2009) 100 ff; *Busch/Falb,* Erhebung und Verarbeitung von Arbeitnehmerdaten in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 48 ff.

586 „Nutzer" iSd. Art 2 lit a ePrivacy-Richtlinie 2002/58/EG.

587 vgl. § 202b dStGB (Abfangen von Daten) bzw. § 201 Abs 2 Nr 1 dStGB (Abhören von Gesprächen).

Nachrichten und Daten (Übertragungsgeheimnis).[588] Das Filtern von elektronischer Kommunikation und das Aufbrechen von (SSL/TLS)-Verschlüsselung ausschließlich zum Erkennen von Viren und Spam ist – wie bereits auf der 1. Stufe angeführt – als geeignete technische und organisatorische Maßnahme zur Sicherheit der Verarbeitung gemäß Art 5 Abs 1 lit f iVm. Art 32 DSGVO geboten und wird damit idR. nicht strafrechtlich relevant sein.[589] Wird die Kommunikation des Beschäftigten nicht direkt am Übertragungsweg abgefangen, sondern erst nach Beendigung des Kommunikationsvorgangs arbeitgeberseitig direkt auf das dienstliche Endgerät zugegriffen, besteht kein strafrechtliches Risiko bzgl. der §§ 119, 119a StGB. Ein Strafbarkeitsrisiko würde gemäß § 118a StGB im Fall einer Umgehung einer Zugangssicherung oder Verschlüsselung des Computersystems bestehen. Bei betrieblichen Systemen ist der Arbeitgeber aber idR. verfügungsbefugt.[590]

Ganz allgemein soll an dieser Stelle noch der mA relativ geringe strafrechtliche Schutz für elektronische Kommunikation (Nachrichten und Daten) am direkten Übertragungsweg in Österreich angesprochen werden: Bei einem nur irrtümlichen (fahrlässig iSd. § 6 StGB) bzw. nur vorsätzlichem (Eventualvorsatz § 5 Abs 1 Hs 2 StGB) oder sogar bereits wissentlichem (§ 5 Abs 3 StGB) Abfangen von noch direkt am Übertragungsweg befindlichen Nachrichten oder Daten als Form der unbefugten Kenntnisverschaffung, also abseits des grundsätzlich erlaubten Erkennens von Viren und Spam[591], sind trotzdem noch nicht die hohen Anforderungen an den subjektiven Tatbestand der §§ 119, 119a StGB erfüllt, womit noch kein Strafbarkeitsrisiko bestehen kann. Denn die §§ 119, 119a StGB verlangen hinsichtlich aller Tatbestandsmerkmale Absicht iSd. § 5 Abs 2 StGB, womit in Österreich strafrechtlich nur ein äußerst geringer Teil des in § 93 Abs 3 TKG 2003 allgemein ausgesprochenen Abhör- und Abfangverbots von Kommunikation durch Dritte – in Umsetzung von Art 3 Convention on Cybercrime 2001 („Illegal Interception") bzw. Art 6 Cybercrime-Richtlinie 2013/40/EU („Rechtswidriges Abfangen von Daten") und teilweiser Umsetzung der Art 5 iVm. Art 15a ePrivacy-Richtlinie 2002/58/EG[592] (Vertraulichkeit der Kommunikation) – tatsächlich in der Realität strafrechtlich geschützt wird.[593] *Lewisch* möchte den Strafrechtschutz von „Nachrichten" am Übertragungsweg nach § 119 StGB noch weiter reduzieren und schreibt: *„Da § 119 die Vertraulichkeit der Kommunikation schützt, wäre das Anbringen einer „Vorrichtung" bloß zum Aufrufen abgelegter oder gelöschter E-Mails aber insoweit nicht tatbestandlich. An diesem traditionellen Kommunikationsverständnis ist auch pro futuro festzuhalten; bloße „Binnenkommunikation" (also etwa der Informationsaustausch im technischen Sinn mit dem eigenen Account im Wege von „Webmail"-Funktionen oder das Ablegen eigener Entwürfe in einer „Cloud") unterliegt insoweit daher*

588 *Lewisch* in Höpfel/Ratz (Hrsg), WK StGB[2] (Stand: Stand 17.10.2017) § 119 Rn ff.

589 *Art 29 Datenschutzgruppe*, WP 118 (2006) 5 ff; *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff; *Kotschy/Reimer*, ZAS 2004, 29; *Lewisch* in Höpfel/Ratz (Hrsg), WK StGB[2] (Stand: Stand 17.10.2017) § 119 Rn 10; *Reindl-Krauskopf* in Höpfel/Ratz (Hrsg), WK StGB[2] (Stand: Stand 17.10.2017) § 119a Rn 11 ff; ErläutRV 1166 BlgNR 20. GP 24.

590 *Reindl-Krauskopf* in Höpfel/Ratz (Hrsg), WK StGB[2] (Stand: Stand 17.10.2017) § 118a Rn 8 ff.

591 *Art 29 Datenschutzgruppe*, WP 118 (2006) 5 ff.

592 idF. Citizens' Rights Richtlinie 2009/136/EG.

593 *Wessely* in Riesz/Schilchegger (Hrsg), TKG 2003 (2016) § 93 Rn 14; *Steinmaurer* in Stratil (Hrsg), TKG 2003[4] (2013) § 93 Anm. 4; *Zanger/Schöll*, Telekommunikationsgesetz[2] (2004) § 93 Rn 16 f; *Ruhle/Freund/Kronegger/Schwarz*, Das neue österreichische Telekommunikations- und Rundfunkrecht (2005) 471 ff; *Fabrizy*, StGB[13] (2018) § 119 Rn 6; § 119a Rn 3.

nicht dem Kommunikationsgeheimnis."[594] Folgt man *Lewisch*, wäre die Kommunikation zwischen Endgerät und Cloud – trotz der Übertragung von Gedankeninhalten (Übertragung von E-Mail-Entwürfe oder Entwurfstexten in die Cloud, etc.) – nur noch durch § 119a StGB geschützt. Wieso die sensible elektronische Kommunikation im Rahmen der Übertragung von „Nachrichten" in ihrer Definition als Vermittlung von Gedankeninhalten zwischen Cloud und Endgerät insofern nicht (mehr) von § 119 StGB erfasst werden sollen, bleibt mA unklar. In § 119 StGB findet sich keine gesetzliche Anforderung, dass unbedingt zwei oder mehr Menschen über Telekommunikation bzw. über ein Computersystem nicht-öffentlich miteinander kommunizieren müssen, sondern es wird auf den Schutz von menschlichen Gedankeninhalten (Nachrichten) am direkten Übertragungsweg abgestellt, womit die Übermittlung eines E-Mailentwurfs bzw. eines Entwurfstexts in die Cloud als Form der Übertragung von menschlichen Gedankeninhalten am direkten Übertragungsweg mA erfasst und strafrechtlich von § 119 StGB geschützt wäre (Inhaltsdaten).[595]

Strafrechtlich relevante Daten (§ 4 Abs 3 Z 2 DSG, Art 10 DSGVO)

§ 4 Abs 3 Z 2 DSG ist eine spezielle Rechtsgrundlage zur rechtmäßigen Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten, insbesondere auch über den Verdacht der Begehung von Straftaten, durch Private (nicht-öffentliche Stellen). Es handelt sich um eine Ausführungsnorm zu Art 10 DSGVO.[596] Die Norm ist insbesondere auf Stufe 3 im Modell der stufenweisen Kontrollverdichtung von Relevanz.[597] Nach *Feiler/Forgó* sind davon personenbezogene Daten erfasst, die einen konkreten begründeten Verdacht gegen eine bestimmte Person erfassen.[598] Nach anderer Ansicht von *Hanloser* gelte Art 10 DSGVO eigentlich nur für das Sammeln von Daten über Verurteilungen oder sonst wie festgestellte Straftaten insbesondere in Registern und somit nicht schon auf eine vorgelagerte investigative Datenverarbeitung zur Verhinderung oder Aufklärung einer Straftat in Verdachtsfällen.[599] Die Meinung *Hanloser*s steht dem bisherigen § 8 Abs 4 Z 3 DSG 2000 aF entgegen, der gemäß AB 1761 BlgNR 25. GP 5 im neuen § 4 Abs 3 Z 2 DSG fortgeführt werden soll.[600] Diese Diskussion ist aus österreichischer Sicht wichtig, da sie letztlich klärt, ob Art 6 Abs 1 lit f DSGVO oder § 4 Abs 3 Z 2 DSG bei Compliance Untersuchungen als korrekte Rechtsgrundlage heranzuziehen ist. Sind die Daten sowohl strafrechtlich relevant (Art 10 DSGVO, § 4 Abs 3 Z 2 DSG) und enthalten zugleich besondere

---

594 *Lewisch* in Höpfel/Ratz (Hrsg), WK StGB[2] (Stand: Stand 17.10.2017) § 119 Rn 5/1.

595 *Fabrizy*, StGB[13] (2018) § 119 Rn 3; *Tipold* in Leukauf/Steininger (Hrsg), StGB[4] (2017) § 119 Rn 3.

596 AB 1761 BlgNR 25. GP 5; *Feiler/Forgó*, EU-DSGVO (2017) Art 10 Rn 3; *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 4/63 ff.

597 *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 157 f; *Kotschy/Reimer*, ZAS 2004, 29.

598 *Feiler/Forgó*, EU-DSGVO (2017) Art 10 Rn 1.

599 *Hanloser* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 1. Rn 86.

600 ErläutRV 1613 BlgNr 20. GP 6; 41 („*insbesondere auch über den Verdacht der Begehung von Straftaten*"); AB 1761 BlgNR 25. GP 5 („[…] *bisheriger § 8 Abs 4 DSF 2000 zu Regelung der Verarbeitung von strafrechtlich relevanten Daten durch Private in adaptierter Form übernommen*").

Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO), legt nach hA die Regelungssystematik nahe, dass Art 10 DSGVO und seine österreichische Ausführungsbestimmung in § 4 Abs 3 Z 2 DSG vorrangig vor Art 9 Abs 2 DSGVO gelten.[601]

Besondere Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO)

Möchte ein Arbeitgeber besondere Kategorien personenbezogener Daten verarbeiten, unterfällt eine solche Verarbeitung Art 9 DSGVO.[602] Liegen besondere Kategorien personenbezogener Daten vor, die zugleich strafrechtlich relevante Daten sind, geht nach der Spruchpraxis der österreichischen Datenschutzbehörde der Erlaubnistatbestand des § 4 Abs 3 Z 2 DSG iVm. Art 10 DSGVO den Erlaubnistatbeständen des Art 9 Abs 2 DSGVO vor.[603]

Für die Verarbeitung von besonderen Kategorien personenbezogener Daten kommen für Arbeitgeber – abseits der Einwilligung (Art 9 Abs 2 lit a DSGVO) – zwei Rechtsgrundlagen im Beschäftigtenverhältnis (Art 9 Abs 2 lit b und lit f DSGVO) in Frage:

Liegt kein strafrechtlich relevanter Verdacht (§ 4 Abs 3 Z 2 DSG) vor, kann eine Durchsicht (Verarbeitung) von „sensiblen" Beschäftigtendaten aus rein arbeits-, straf- und zivilrechtlichen Gründen durch Art 9 Abs 1 lit f DSGVO legitimiert werden, wenn dies für Zwecke der Verfolgung von Rechtsansprüchen (gegen Mitarbeiter oder andere), oder zur Rechtsverteidigung (Unternehmen selbst in einem Strafverfahren oder Zivilverfahren) erforderlich ist. Weitere berechtigte Interessen des Arbeitgebers lässt der Erlaubnistatbestand Art 9 Abs 2 lit f DSGVO nicht zu.[604]

Eine zweite Möglichkeit für Arbeitgeber bietet Art 9 Abs 2 lit b DSGVO, wenn eine arbeitsrechtliche Erforderlichkeit an der Datenverarbeitung besteht. Die Auslegung der beiden Tatbestandsmerkmale des Art 9 Abs 2 lit b DSGVO ist (in Österreich) umstritten. Die Verarbeitung von „sensiblen" Beschäftigtendaten gestützt auf Art 9 Abs 2 lit b DSGVO bedarf nämlich der Erfüllung zweier Tatbestandsmerkmale: [1.] der arbeitsrechtlichen Erforderlichkeit (im hier relevanten Anwendungsfall „IT-Nutzung" die Interessensabwägung gemäß § 16 ABGB) zusammen mit [2.] einem unionalen oder nationalen Recht mit „geeigneten Garantien" iSd. DSGVO.[605] Im Detail:

---

601 AB 1761 BlgNR 25. GP 5; *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 4/63 ff; DSK 21.01.2009, K121.390/0001-DSK/2009.

602 Art 9 Abs 1 Datenschutz-Grundverordnung (EU) 2016/679.

603 *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 4/63 ff; DSK 21.01.2009, K121.390/0001-DSK/2009; AB 1761 BlgNR 25. GP 5.

604 *Feiler/Horn*, Umsetzung der DSGVO in der Praxis (2017) 157 f; *Feiler,* Datenschutzrechtliche Herausforderungen bei internen Compliance-Untersuchungen in Jahnel (Hrsg), Jahrbuch Datenschutzrecht und E-Government Jahrbuch 2013 (2013) 143 (148 ff.); *Skorjanc* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil VI Annex: Rechtslage Österreich Rn 14.

605 *Schiff* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 9 Rn 39; *Brodil*, Sensible Daten im Arbeitsverhältnis – Nochmals zur Erfassung von § 9 Z 11 DSG 2000, in Kietaibl/Schörghofer/Schrammel (Hrsg), Rechtswissenschaft und Rechtskunde – Liber Amicorum für Robert Rebhahn (2014) 1 ff (4 ff.); *Brodil*, ecolex 2010, 122 (123); *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 4/87 f; *Hattenberger* in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund neuer Medien (2005) 49 ff.

[1.] Die Verarbeitung der „sensiblen" Beschäftigtendaten muss nach dem ersten Tatbestandsmerkmal des Art 9 Abs 2 lit b DSGVO erforderlich sein, um den Rechten und Pflichten des Arbeitgebers auf dem Gebiet des Arbeits- und Dienstrechts (u. Sozialrecht) Rechnung zu tragen. Die Prüfung der „Erforderlichkeit" hat dabei allein nach arbeits- oder dienstrechtlichen Kriterien zu erfolgen, das heißt es handelt sich im ersten Schritt um eine allein arbeitsrechtliche Erforderlichkeitsprüfung. Diese arbeitsrechtliche Erforderlichkeit ist in Österreich – in allen Fällen wo spezielle arbeitsrechtliche Normen (z.B. § 8 Abs 8 AngG, UrlG) fehlen – auf Grundlage der Interessensabwägung gemäß § 16 ABGB (vgl. **Kapitel 4.2.2**) unter Berücksichtigung der Fürsorgepflicht (§ 1157 ABGB, § 18 AngG) anhand der konkreten Interessenslagen zwischen Arbeitgeber und Beschäftigten zu erfassen.[606]

[2.] Die oben festgestellte arbeitsrechtliche Erforderlichkeit (im hier besprochenen Rahmen gemäß § 16 ABGB, vgl. **Kapitel 4.2.2**) muss nach dem zweiten Tatbestandsmerkmal des Art 9 Abs 2 lit b DSGVO nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung (inkl. Betriebsvereinbarungen), mit geeigneten Garantien für die Grundrechte und die Interessen der betroffenen Person, zulässig sein. ErwGr 10 DSGVO führt zu den europarechtlichen Anforderungen an ein solches unionales oder nationales Recht aus:[607] „*Diese Verordnung bietet den Mitgliedstaaten zudem einen Spielraum für die Spezifizierung ihrer Vorschriften, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten (im Folgenden „sensible Daten"). Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.*"[608] Eine differenzierte Ansicht zu ErwGr 10 vertreten *Goricnik/Grünanger*, die zwar kodifizierte „geeignete Garantien" in der Rechtsvorschrift verlangen, aber keinen „echten" datenschutzrechtlichen Erlaubnistatbestand mit kodifizierter Zulässigkeit einer Datenverarbeitung, denn die Zulässigkeit der Datenverarbeitung könne sich auch durch Auslegung der (österreichischen) Norm ergeben.[609] *Goricnik/Grünanger* schreiben bzgl. der „geeigneten Garantien": „*Sowohl eine gesetzliche Grundlage als auch die zuvor erwähnten normativen Rechtsquellen des kollektiven Arbeitsrechts müssen aber – sollen sie als Verarbeitungsgrundlage dienen – angemessene Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte der betroffenen Person vorsehen*.[610] Zu „Garantien" iSd. Art 9 Abs 2 lit b DSGVO gehören nach hM – neben den konkreten Anforderungen in ErwGr 10 DSGVO – auch, dass in diesem unionalen oder mitgliedstaatlichem Recht eine strenge Zweckbindung vorgesehen ist, kurze Löschfristen, angemessene Überprüfbarkeit

606 *Brodil*, Sensible Daten im Arbeitsverhältnis – Nochmals zur Erfassung von § 9 Z 11 DSG 2000, in Kietaibl/Schörghofer/Schrammel (Hrsg), Rechtswissenschaft und Rechtskunde – Liber Amicorum für Robert Rebhahn (2014) 1 ff (4 ff.); *Brodil*, ecolex 2010, 122 (123); *Brodil*, ZAS 2009, 121 (122 ff.); *Brodil*, ZAS 2004, 156 (158 ff.).

607 *Feiler/Forgó*, EU-DSGVO (2017) Art 9 Rn 10.

608 ErwGr 10 Datenschutz-Grundverordung (EU) 2016/679.

609 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn. 2.100; Rn. 2.103; Rn 2.104.

610 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.100.

der Nutzungsregeln, Verschlüsselung, Pseudonymisierung oder, dass darin spezielle Verpflichtungen zur Geheimhaltung festgeschrieben sind.[611] Gemäß Art 6 Abs 4 lit e DSGVO zählen zu „geeigneten Garantien" auch Verschlüsselung und Pseudonymisierung.[612] Nach der deutschen BT-Drs. 18/11325, S. 95 zu § 22 Abs 2 Nr 1 – 10 BDSG können auch weitere spezifische technische und organisatorische Maßnahmen (z.B. „freiwillige" Benennung eines Datenschutzbeaufragten, technische Trennung von sensiblen und sonstigen personenbezogenen Daten, Beschränkung des Zugangs zu diesen personenbezogenen Daten innerhalb der verantwortlichen Stelle, etc.) solche „geeigneten Garantien" iSd. Art 9 Abs 2 lit b DSGVO schaffen (vgl. § 26 Abs 3 Satz 3 BDSG).[613]

Im österreichischen DSG und im hier relevanten § 16 ABGB selbst sind keine „geeigneten Garantien" iSd. DSGVO formuliert.[614] Insofern könnte am ersten Blick eine rechtskonforme individualarbeitsrechtliche Erforderlichkeit einer Verarbeitung von „sensiblen" Beschäftigtendaten gemäß § 16 ABGB (erstes Tatbestandsmerkmal) für sich alleine noch nicht ausreichend sein zur Erfüllung des zweiten Tatbestandsmerkmals der „geeigneten Garantien für die Grundrechte und die Interessen der betroffenen Person" (Art 9 Abs 2 lit b DSGVO). Die Thematik der „geeigenten Garantien" ist insofern noch näher rechtsvergleichend zu untersuchen:

In Deutschland wurde in § 26 Abs 3 BDSG vom Gesetzgeber in Ausführung des Art 9 Abs 2 lit b DSGVO eine allgemeine gesetzliche Erlaubnisnorm für die Verarbeitung besonderer Kategorien von Daten im Beschäftigungsverhältnis verankert. Bei festgestellter rein arbeitsrechtlicher Erforderlichkeit (*„Ausübung von Rechten aus dem Arbeitsrecht"*) hat im zweiten Schritt eine datenschutzrechtliche Interessensabwägung zu erfolgen, ob im Einzelfall die Betroffeneninteressen der Beschäftigten – trotz festgestellter Erforderlichkeit für das Beschäftigtenverhältnis – nicht doch im Einzelfall überwiegen. Nach *Forst* handelt es sich dabei um eine „zweistufige Rechtfertigungsprüfung".[615] Andererseits werden deutschen Arbeitgebern, die ihre Verarbeitung „sensibler" Beschäftigtendaten auf diesen § 26 Abs 3 Satz 1 BDSG als Rechtsgrundlage stützen, gemäß § 26 Abs 3 Satz 3 iVm. § 22 Abs 2 Nr 1 – 10 BDSG ergänzende „geeignete Garantien" durch zusätzliche technische und organisatorische Maßnahmen auferlegt (z.B. „freiwillige" Bestellung eines betrieblichen

611 *Kastelitz/Hötzendirfer/Tschohl* in Knyrim (Hrsg), DatKomm (Stand 01.10.2018, rdb.at) Art 9 Rn. 36; *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997) Art 8 Rn 10; *Jahnel,* Handbuch Datenschutzrecht (2010) Rn 4/89; *Goricnik/Grünanger*, Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.103.

612 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 6 Rn 60; *Schiff* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 9 Rn 39.

613 BT-Drs. 18/11325, 95; *Zöll* in Taeger/Gabel (Hrsg), DSGVO BDSG[3] (2018) § 26 Rn 86; *Rose* in Taeger/Gabel (Hrsg), DSGVO BDSG[3] (2018) § 22 BDSG Rn 44 ff..

614 ErwGr 10 Datenschutz-Grundverordnung (EU) 2016/679; *Frenzel* in Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018) Art 9 Rn 27 f; *Kastelitz/Hötzendirfer/Tschohl* in Knyrim (Hrsg), DatKomm (Stand 01.10.2018, rdb.at) Art 9 Rn. 36; *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997) Art 8 Rn10; *Jahnel,* Handbuch Datenschutzrecht (2010) Rn 4/89; *Rose* in Taeger/Gabel (Hrsg), DSGVO BDSG[3] (2018) § 22 BDSG Rn 44 ff.

615 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 Rn 83; BT-Drs 18/11325, 98.

Datenschutzbeauftragten, etc.).[616] Die Interessensabwägung (§ 26 Abs 3 Satz 1 BDSG) iVm. mit zusätzlich zu treffenden technischen und organisatorischen Maßnahmen (§ 22 Abs 2 iVm. § 26 Abs 3 Satz 3 BDSG) ist seit 25. Mai 2018 im Vergleich zum altem deutschen Recht insofern eine „Erleichterung" für deutsche Arbeitgeber: Bis 24. Mai 2018 stützte sich nur die Verarbeitung von „nicht-sensiblen" und „strafrechtlich-relevanten" Beschäftigtendaten auf die arbeitsrechtliche Erforderlichkeitsprüfung in § 32 Abs 1 Satz 1 bzw. Satz 2 BDSG aF (§ 26 Abs 1 Satz 1 bzw. Satz 2 BDSG nF), die Verarbeitung von „sensiblen" (§ 3 Abs 9 BDSG aF; heute Art 9 Abs 1 DSGVO) Beschäftigtendaten musste sich weiterhin – nach dem ausdrücklichen Willen des deutschen Gesetzgebers (BT-Drs 16/13657, S. 21) und auch mangels „angemessene Garantien" (vgl. Art 8 Abs 2 lit b DSRL 95/46/EG) in § 32 BDSG aF selbst – über die allgemeinen Erlaubnistatbestände für besondere Arten personenbezogener Daten (§ 28 Abs 6 – Abs 8 BDSG aF) ohne eine verfügbare spezifische Interessensabwägung für das Beschäftigungsverhältnis legitimieren.[617] Die seit 25. Mai 2018 geltende Interessensabwägung in Form einer „zweistufigen Rechtfertigungsprüfung"[618] für die Verarbeitung „sensibler" Beschäftigtendaten (§ 26 Abs 3 Satz 1 und Satz 3 iVm. § 22 Abs 2 Nr 1 – 10 BDSG) schafft nun für deutsche Arbeitgeber Abhilfe.[619]

Der österreichische Gesetzgeber hat – anders als der deutsche Gesetzgeber (§ 26 Abs 3 iVm. § 22 Abs 2 BDSG) – seit 25. Mai 2018 im DSG keine vergleichbare allgemeine gesetzliche Bestimmung für eine beschäftigungs-datenschutzrechtliche Interessensabwägung mit dort normierten „geeigneten Garantien" in Ausführung zu Art 9 Abs 2 lit b DSGVO verankert. Mangels Kodifizierung von „geeigenten Garantien" erfüllt § 16 ABGB aus dieser Perspektive alleine diese Anforderungen an das zweite Tatbestandsmerkmal des Art 9 Abs 2 lit b DSGVO offenbar nicht.[620] Art 9 Abs 2 lit b DSGVO mit der Anforderung der „geeigneten Garantien" im zweiten Tatbestandsmerkmal scheint im Hinblick auf das österreichische Arbeitsrecht aber ganz grundsätzlich als problematisch anzusehen zu sein, denn es erfüllen mit hoher Wahrscheinlichkeit zahlreiche etablierte arbeitsrechtliche Vorschriften nicht die Anforderung des zweiten Tatbestandsmerkmals gemäß Art 9 Abs 2 lit b DSGVO. Denn wie *Brodil* kritisch und völlig richtig bereits schon zur fast wortgleichen europäischen Vorgängerbestimmung Art 8 Abs 2 lit b DSRL 95/46/EG aufzeigte, enthält z.B. der Gesetzestext

---

616 BT-Drs 18/11325, 96 f; *Gräber/Nolden* in Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018) § 26 BDSG Rn 41; *Greve* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) Art 9 DSGVO Rn 21; *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 BDSG Rn 82 ff; *Dammann/Simits*, EG-Datenschutzrichtlinie (1997) Art 8 Rn 10.

617 *Düsseldorfer Kreis*, Arbeitsbericht ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer" (2005) 9 ff; *Hanloser* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 1. Rn 63.

618 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018) § 26 Rn 83; BT-Drs 18/11325, 98.

619 BT-Drs 16/13657, 21; BT-Drs. 18/113325, 98; *Wolff* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] [aF] (Stand:01.08.2015) § 28 BDSG 2003 [aF] Rn 240; *Maschmann* in Kühling/Buchner (Hrsg) DS-GVO BDSG[2] (2018) § 26 BDSG Rn 23 ff.

620 ErwGr 10 Datenschutz-Grundverordnung (EU) 2016/679; *Frenzel* in Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018) Art 9 Rn 27 f; *Kastelitz/Hötzendirfer/Tschohl* in Knyrim (Hrsg), DatKomm (Stand 01.10.2018, rdb.at) Art 9 Rn. 36; *Rose* in Taeger/Gabel (Hrsg), DSGVO BDSG[3] (2018) § 22 BDSG Rn 44 ff; *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997) Art 8 Rn10; *Jahnel,* Handbuch Datenschutzrecht (2010) Rn 4/89; *Goricnik/Grünanger*, Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.103.

des § 8 Abs 8 AngG (Anzeige einer Dienstverhinderung durch den Angestellten beim Dienstgeber; Vorlage einer ärztlichen Bestätigung über Ursache und Dauer der Arbeitsunfähigkeit, etc.) bis heute keine entsprechenden „geeigneten Garantien" iSd. europäischen Datenschutzrechts. Insofern wäre streng datenschutzrechtlich betrachtet – zumindest seit unmittelbarer Anwendbarkeit der DSGVO mit 25. Mai 2018 – die Verarbeitung der Information einer Dienstverhinderung wegen Krankheit mangels kodifizierter „geeigneter Garantien" in § 8 Abs 8 AngG nicht allein mit Art 9 Abs 2 lit b DSGVO legitimierbar (wenn Gesundheitsdaten iSd. Art 9 Abs 1 DSGVO Teil der Meldung). Dies führt letzlich aber zu keinem sinnvollen Ergebnis für den praktischen Arbeitsalltag.[621] So weisen bspw. *Goricnik/Grünanger* – wie oben zitiert – im Detail auf diese „geeigneten Garantien" als erforderliche zusätzliche Rechtmäßigkeitsanforderungen hin, in dem dann an selber Stelle jedoch beispielhaft angeführten § 7 Abs 3 ARG[622] (mittlerweile aufgehoben[623]) fehl(t)en im Gesetzestext aber auch genau solche ausformulierten „geeigneten Garantien" iSd. zweiten Tatbestandsmerkmals des Art 9 Abs 2 lit b DSGVO, was jedoch dann von *Goricnik/Grünanger* an selber Stelle nicht näher besprochen wird.[624] *Grünanger* geht jedoch an anderer Stelle auf die Thematik der „geeigneten Garantien" iSd. Art 9 Abs 2 lit b DSGVO im österreichischen Arbeitsrecht ein. Für *Grünanger* sind die Treue- und Fürsorgepflichten (§ 1157 ABGB, § 18 AngG) als „geeignete Garantien" iSd. Art 9 Abs 2 lit b DSGVO anzusehen, denn aus der Fürsorgepflicht ergebe sich eine Pflicht zur Geheimhaltung und eine strenge Zweckbindung und somit „geeignete Garantien".[625] In Deutschland wird diese vorgeschlagene Lösung *Grünangers* mit der Fürsorgepflicht des Arbeitgebers (vgl. § 618 BGB) als „geeignete Garantie" aktuell nicht diskutiert, da die Thematik der „geeigneten Garantien" bereits über die §§ 26 Abs 3 Satz 3 iVm. 22 Abs 2 Nr 1 – 10 BDSG gelöst wird.[626] *Brodil* stellt primär auf das Vorliegen einer streng zu bemessenden arbeitsrechtlichen Erforderlichkeit nach rein österreichischem Arbeitsrecht ab (z.B. § 16 ABGB, § 8 Abs 8 AngG, etc.), wo im Einzelfall dann ein strenger Maßstab anzulegen sei. Damit könne sichergestellt werden, dass durch die strenge arbeitsrechtliche Erforderlichkeitsprüfung (Art 9 Abs 2 lit b DSGVO – erstes Tatbestandsmerkmal) letztlich kein schwächerer Schutz für „sensible" Beschäftigtendaten entstehe, als im Rahmen der Interessensabwägung für „nicht-sensible" Beschäftigtendaten (Art 6 Abs 1 lit f DSGVO).[627] Folgt man der Ansicht des *Deutschen Gesetzgebers*, wäre die Problematik der „geeigneten Garantien" (zweites

621 *Brodil*, Sensible Daten im Arbeitsverhältnis – Nochmals zur Erfassung von § 9 Z 11 DSG 2000, in Kietaibl/Schörghofer/Schrammel (Hrsg), Rechtswissenschaft und Rechtskunde – Liber Amicorum für Robert Rebhahn (2014) 1 ff (7 f.).

622 Verarbeitung von Daten zur Religionszugehörigkeit durch Arbeitgeber iZh. mit dem Karfreitag.

623 Gemäß BGBl. I Nr. 22/2019 seit 22. März 2019 aufgehoben.

624 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.97 ff.

625 *Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 4.94 f.

626 *Rose* in Taeger/Gabel (Hrsg), DSGVO BDSG[3] (2018) § 22 BDSG Rn 44 ff.

627 *Brodil*, Sensible Daten im Arbeitsverhältnis – Nochmals zur Erfassung von § 9 Z 11 DSG 2000, in Kietaibl/Schörghofer/Schrammel (Hrsg), Rechtswissenschaft und Rechtskunde – Liber Amicorum für Robert Rebhahn (2014) 1 ff (5); *Brodil*, Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 9; *Brodil/Risak,* Arbeitsrecht in Grundzügen[10] (2019) Rn 43a; *Brodil*, ecolex 2018, 486 (488); *Brodil*, DRdA 2018, 463 (468).

Tatbestandsmerkmal) ein legistisches Thema. Abseits des Abschlusses von Betriebsvereinbarungen[628] (oder Kollektivverträgen), die im Text konkret solche „geeigneten Garantien" ausformulieren, müsste diese Thematik folglich vom österreichischen Gesetzgeber gelöst werden. Dabei könnte eine Bestimmung zu „geeigneten Garantien" (z.B. freiwillige Bestellung eines Datenschutzbeauftragten, technische Trennung von „sensiblen" und „nicht-sensiblen" Daten, oder in Anlehnung an Art 6 Abs 4 lit e DSGVO eine Verschlüsselungs- bzw. Pseudonymisierungspflicht für besondere Kategorien personenbezogener Beschäftigtendaten beim Arbeitgeber) im DSG eingefügt werden (vgl. Deutschland: § 22 Abs 2 Satz 2 Nr. 1 – 10 BDSG, BT-Drs. 18/11325, S. 95). Alternativ könnten auch „geeigneten Garantien" in den Bestimmungen zur Fürsorgepflicht (§ 1157 ABGB, § 18 AngG) in einem neuen Absatz verankert werden. Stützt ein österreichischer Arbeitgeber dann seine Verarbeitung auf Art 9 Abs 2 lit b DSGVO, könnten solche kodifizierten Maßnahmen die europarechtlichen Anforderungen an „geeignete Garantien" erfüllen (zweites Tatbestandsmerkmal) und damit wäre eine arbeitsrechtlich erforderliche Datenverarbeitung besonderer Kategorien personenbezogener Daten gemäß § 16 ABGB (erstes Tatbestandsmerkmal) stets rechtssicher mit Art 9 Abs 2 lit b DSGVO legitimierbar.[629] Als österreichisches Vorbild für eine legistische Lösung könnten die § 79e Abs 2a iVm. § 79f oder § 79g BDG[630] idF. BGBl. I Nr. 32/2018 als Beschäftigtendatenschutzbestimmung für den öffentlichen Bereich (inkl. Vertragsbedienstete gemäß § 29n VBG[631]) dienen. Diese Bestimmungen legitimieren – aufgrund der erlaubten Privatnutzung im öffentlichen Dienst – die Verarbeitung von besonderen Kategorien personenbezogener Daten bei „unbedingter" Erforderlichkeit und normieren zusätzliche „geeignete Garantien" iSd. Art 9 Abs 2 lit b DSGVO für die österreichischen Beamten und Vertragsbediensteten[632]:

- strikte Zweckbindung von Kontrollen auf:
  - Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit;
  - begründeter Verdacht einer gröblichen Dienstpflichtverletzung.
- Unverzügliche – nach Zweckerreichung – zu dokumentierende Löschung;
- umgehende Information der betroffenen Beamten und Vertragsbediensteten nach Maßgabe der §§ 79f und 79g BDG von der Leitung der Dienststelle;
- die IT-Stelle hat über die Verarbeitung der besonderen Kategorien personenbezogener Protokoll zu führen und die Gründe für die Verarbeitung sowie die erfolgte Information der betroffenen Beamten und Vertragsbediensteten schriftlich zu dokumentieren;
- die Daten des Protokolls sind betroffenen Beamten und Vertragsbediensteten auf Verlangen direkt zur Verfügung zu stellen. Mit „direkt" zur Verfügung zu stellen ist gemeint, dass die Beamten und Vertragsbediensteten die Daten des Protokolls ohne Befassung von Zwischenvorgesetzten einsehen dürfen.

---

628 *Skorjanc* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil VI Annex: Rechtslage Österreich Rn 14.

629 *Kastelitz/Hötzendirfer/Tschohl* in Knyrim (Hrsg), DatKomm (Stand 01.10.2018, rdb.at) Art 9 Rn. 36; *Brodil*, ecolex 2010, 122 (123).

630 Beamten-Dienstrechtsgesetz 1979 (BDG) BGBl. Nr. 333/1979.

631 § 29n Vertragsbedienstetengesetz 1948 (BGBl. I Nr. 77/2009).

632 *Goricnik* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 6.82.

- die betroffenen Beamten und Vertragsbediensteten haben das Recht, direkt gegenüber der Leitung der Dienststelle eine zu dokumentierende Stellungnahme abzugeben.[633]

Folgt man der Meinung *Brodils* – bzw. mit anderer Begründung *Grünangers* – wäre jedoch durch eine rein strenge Erforderlichkeitsprüfung (§ 16 ABGB), bzw. bei einer besonderen Berücksichtigung der Fürsorgepflicht (§ 1157 ABGB, § 18 AngG) iZh. mit der Verarbeitung „sensibler Daten" im Betrieb, das Kriterium der „geeigneten Garantien" bereits schon erfüllt, es bedürfe dann keiner legistischen Lösung.[634]

Aufgrund dieser Rechtsunsicherheit können derzeit (Stand 2019) mA österreichische Arbeitgeber die Rechtsgrundlage Art 9 Abs 2 lit b DSGVO absolut (europa-)rechtssicher nur über eine Betriebsvereinbarung (§ 29 ArbVG) oder über einen Kollektivertrag (§ 2 ArbVG) nutzen, wenn in einer solchen Betriebsvereinbarung bzw. Kollektivvertrag auch konkret „geeigenete Garantien" ausformuliert und umgesetzt werden.[635] Meiner Ansicht bedarf es daher zur Rechtssicherheit für Österreich – abseits von Betriebs- und Kollektivvereinbarungen – auch für den privaten Bereich der gesetzlichen Formulierung von „geeigneten Garantien" direkt im DSG oder in den § 1157 ABGB, § 18 AngG vergleichbar zu § 79e Abs 2a iVm. § 79f und § 79g BDG bzw. den deutschen § 26 Abs 3 iVm. § 22 Abs 2 BDSG.

Zweckänderungen

Allgemein nicht berücksichtigt wurde vom österreichischen Gesetzgeber die Thematik „Zweckkompatibilität" und „Zweckänderungen", obwohl sich bereits die ErläutRV zum DSG 2000 aus dem Jahr 1999 hinsichtlich innerbetrieblicher Zweckkompatibilität umfassend damit beschäftigt hatte: „*Wenn in [§ 6 Abs 1 Z 2 DSG 2000] statuiert wird, daß eine Weiterverwendung von Daten nur zulässig sein soll, wenn dies mit dem ursprünglichen Ermittlungszweck "nicht unvereinbar" ist, so sei dazu angemerkt, daß diejenigen innerbetrieblichen Datenverwendungen, die der Aufrechterhaltung und Optimierung der Organisation (wie zB Rechnungswesen und Controlling) oder der Analyse und Planung dienen, jedenfalls nicht als eigener Verwendungszweck zu sehen sind, der mit dem Zweck der ursprünglichen Datenermittlung (zB im Rahmen des Abschlusses eines Handelsgeschäftes) "unvereinbar" ist.*"[636] Das Problem ist in Österreich nun, dass für private (nicht-öffentliche) Stellen keine „qualifizierte" nationale Rechtsvorschrift iSd. Art 6 Abs 4 Hs 1 DSGVO existiert, die eine Weiterverarbeitung zu inkompatiblen Zwecken für den privatwirtschaftlichen Bereich (z.B. zivilrechtliche Rechtsverfolgung, Aufklärung von Strafverstößen, etc.) legitimieren würde. Nicht einmal in § 4 Abs 3 DSG, wo es um Straftaten geht, wurde vom österreichischen Gesetzgeber die Möglichkeit einer zweckinkompatiblen Weiterverarbeitungsmöglichkeit für private nicht-öffentliche Stellen zum Zweck der unternehmensinternen Strafaufklärung vorgesehen. Eine solche Bestimmung würde Zweckänderungen ohne

---

633 §§ 79e – 79g BDG (BGBl. I Nr. 77/2009 idF. BGBl. I Nr. 32/2018); ErläutRV 65 BlgNr 26. GP 12 f.

634 *Brodil*, Sensible Daten im Arbeitsverhältnis – Nochmals zur Erfassung von § 9 Z 11 DSG 2000, in Kietaibl/Schörghofer/Schrammel (Hrsg), Rechtswissenschaft und Rechtskunde – Liber Amicorum für Robert Rebhahn (2014) 1 ff (5); *Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 4.94 f.

635 so auch: *Skorjanc* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil VI Annex: Rechtslage Österreich Rn 14.

636 ErläutRV 1613 BlgNR 20 GP 39 (Datenschutzgesetz 2000 – DSG).

Kompatibilitätstests in Art 6 Abs 4 Hs 2 DSGVO z.B. im Rahmen von internen Compliance Untersuchungen oder (US-)Terrorlisten-Screening möglich machen, wo regelmäßig eine zweckändernde Verarbeitung von an sich zweckgebundenen Beschäftigtendaten erforderlich wird und dann ggf. an der mangelnden Zweckkompatibilität – trotz Vorliegens eines erheblichen berechtigten Interesses (Art 6 Abs 1 lit f DSGVO; § 4 Abs 3 DSG) – letztlich scheitern kann.[637] Gesetzgeberisch wäre es möglich und auch unionsrechtskonform gewesen § 4 Abs 3 DSG selbst oder eine andere Norm im DSG als qualifizierte Rechtsvorschrift iSd. Art 6 Abs 4 Hs 1 DSGVO im Fall von zweckinkompatiblen Weiterverarbeitungen zu gestalten (vgl. dazu Deutschland: § 24 Abs 1 BDSG idF. DSAnpUG-EU).[638] Mangels einer solchen qualifizierten Rechtsgrundlage iSd. Art 6 Abs 1 Hs 1 DSGVO im österreichischen DSG als Legitimierung solcher inkompatibler Zweckänderungen für nicht-öffentliche (private) Stellen, ergibt sich für österreichische Arbeitgeber – abseits der informierten freiwilligen Einwilligung der betroffenen Beschäftigten (Art 6 Abs 4 Hs 1 DSGVO) – immer die Erforderlichkeit eines Zweckkompatibilitätstest (Art 6 Abs 4 Hs 2 DSGVO) bei geplanten Zweckänderungen von zweckgebundenen Beschäftigtendaten, wenn der (aktuell) hM zu Zweckänderungen gefolgt wird:

- Zweckänderungen personenbezogener Daten zur unternehmensinternen Aufklärung von im Beschäftigtenverhältnis (Internal Investigations) begangenen Straftaten bedürfen des Kompatibilitätstest des Art 6 Abs 4 Hs 2 DSGVO;
- Zweckänderungen zur unternehmensinternen Aufklärung und Verfolgung von Verwaltungsstrafen bedürfen des Kompatibilitätstest des Art 6 Abs 4 Hs 2 DSGVO;
- Zweckänderungen zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche bedürfen des Kompatibilitätstest des Art 6 Abs 4 Hs 2 DSGVO;
- Sonstige beabsichtigte Zweckänderungen bei nicht-öffentlichen Stellen (insb. zu privatwirtschaftlichen Zwecken) z.B. auf Basis berechtigter Interessen bedürfen immer des Kompatibilitätstest gemäß Art 6 Abs 4 Hs 2 DSGVO.[639]

Auch in Österreich fiel – genau wie in Deutschland – durch die DSGVO die bisherige praktische Möglichkeit der rein interessensbasierten Zweckänderung weg (vgl. § 8 Abs 1 iVm. § 7 Abs 2 iVm. § 4 Z 12 Hs 2 DSG 2000 aF). Eine zweckändernde Verwendung von personenbezogenen Daten für ein anderes Aufgabengebiet des Verantwortlichen wurde in Österreich bis 24. Mai 2018 den Regelungen der Datenübermittlung unterworfen (§ 4 Z 12 DSG 2000) und konnte folglich rein interessensbasiert („überwiegend berechtigtes Interesse“ gemäß § 8 Abs 1 Z 4 iVm. § 7 Abs 2 DSG 2000) stattfinden.[640] Seit 25. Mai 2018 sind rein interessensbasierte Zweckänderungen nicht mehr möglich, sondern es ist in jedem Fall einer Weiterverarbeitung der Kompatibilitätstest nach Art 6 Abs 4 Hs 2 DSGVO erforderlich oder eine informierte freiwillige Einwilligung der betroffenen Beschäftigten gemäß

637 *Herbst* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) § 24 BDSG Rn 7 ff; *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff.
638 *Kühling/Martini et al*., Die DSGVO und das nationale Recht (2016) 38 ff.
639 *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff.
640 *Knyrim,* Datenschutzrecht[3] (2015) 98.

Art 6 Abs 4 Hs 1 DSGVO.[641] *Kotschy* spricht bei diesem Punkt von einer klaren Verschärfung des Datenschutzrechts für Österreich.[642]

Liegt keine Zweckkompatibilität, keine qualifizierte Rechtsgrundlage oder eine informierte freiwillige Einwilligung für inkompatible Zweckänderungen vor, hat der Verantwortliche nach hM wieder „bei Null" anzufangen. Das heißt der Verantwortliche dürfte folglich nicht auf die vorhandenen Datenbestände zurückgreifen, denn eine Bestimmung wie § 4 Z 12 Hs 2 iVm. § 7 Abs 2 DSG 2000 aF kennt die DSGVO nicht.[643]

Nur wenn man der Ansicht *Roßnagels* folgt (siehe **Kapitel 3.5.3**), wäre jede mit Art 6 Abs 4 inkompatible bzw. unerlaubte Zweckänderung jeweils als „neue" Datenverarbeitung mit vollständige neuer DSGVO-Konformitätsprüfung – bei in der Realität technisch identischen Verarbeitungsvorgängen – jedenfalls datenschutzrechtlich neu legitimierbar.[644]

Bildverarbeitung

Das DSG enthält in den §§ 12 f. DSG auch Rechtsgrundlagen und konkretisierende Sonderregelungen für Bildverarbeitungen. Die Legitimation zum Erlass dieser Spezialregelungen wird auf ErwGr 10 iVm. Art 6 Abs 1 lit c bzw. lit e iVm. Art 6 Abs 2 u. Abs 3 und Art 23 DSGVO gestützt.[645] Der Anwendungsbereich ist die *„Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum"* (§ 12 Abs 1 DSG). In den Materialien wird ausgeführt, dass die §§ 12 f. DSG darauf abzielen, grundsätzlich alle Bildaufnahmen durch Verantwortliche des privaten Bereichs (nicht-öffentliche Stellen) den Bestimmungen unterliegen zu lassen (wie bspw. auch Fotografien durch beruflich tätige Fotografen). Mit erfasst sind auch die mit einer Bildverarbeitung verbundenen Tonaufnahmen. Es stellt sich die Frage, ob bspw. bei betrieblichen Videokonferenzen wie bei Skype for Business, etc. Art 6 Abs 1 lit f DSGVO oder die §§ 12 f DSG zur Anwendung gelangen. Der Einsatz von Videokonferenzen dient offensichtlich nicht der Kontrolle der Beschäftigten (§ 12 Abs 4 Z 2 DSG). Wäre Art 6 Abs 1 lit f DSGVO (berechtigtes Interesse) nicht die vorrangige Erlaubnisnorm, würde sich im Beschäftigtenbereich für Videokonferenzen nur eine Erlaubnis aus § 12 Abs 2 Z 2 DSG (Einwilligung) sowie § 12 Abs 2 Z 4 DSG (überwiegend berechtigte Interessen) ergeben. [646]

Zu beurteilen ist nun die Vereinbarkeit mit der DSGVO: Mangels rechtlicher Verpflichtung zur Durchführung einer Videokonferenz, noch einer damit verbundenen Wahrnehmung einer Aufgabe im öffentlichen Interesse, werden zumindest die besonderen Rechtsgrundlagen in § 12 Abs 2 – Abs 5 DSG umfassend vom Anwendungsvorrang des Art 6 Abs 1 lit f DSGVO verdrängt.[647] Die § 12 Abs 1 sowie § 13 DSG hingegen können als eine spezielle

641 *Art 29 Datenschutzgruppe*, WP 203 (2013) 21 ff; *Bergauer*, Zur Rechtmäßigkeit der (Weiter)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 6/2018, 231 (232 ff.).

642 *Kotschy*, Zweckbindungsprinzip und zulässige Weiterverarbeitung – Debattenbeitrag zur Datenschutz-Grundverordnung (2016) 11.

643 *Buchner/Petri* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) Art 6 Rn 185; *Tinnefeld/Buchner/Petri/Hof,* Einführung in das Datenschutzrecht[6] (2018) 240.

644 *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann (Hrsg), Datenschutzrecht (2019) Art 5 Rn 96 ff.

645 AB 1761 BlgNR 25. GP 8.

646 AB 1761 BlgNR 25. GP 8.

647 Art 2 Abs 1 DSGVO; EuGH Rs. 6/64, Slg. 1964, S. 1251, 1269 – Costa/ENEL.

nationale Konkretisierung der Art 5 Abs 1 lit b (legitime Zwecke) u. lit e (Speicherbegrenzung), Art 5 Abs 1 lit f iVm. Art 25 und Art 32 (besondere Datensicherheitsmaßnahmen) sowie Art 14, Art 15, (Kennzeichnung und Auskunft) angesehen werden. Nach *Roßnagel* darf nationales Datenschutzrecht die rein abstrakten Vorgaben der DSGVO – unabhängig davon ob eine Öffnungsklausel besteht oder nicht – konkretisieren bzw. präzisieren und damit für Normunterworfene Handlungs- und Bewertungsmaßstäbe schaffen, was der DSGVO selbst fehlt. Dies gilt aber nur solange die nationalen Normen sich innerhalb der Vorgaben und Ziele der DSGVO bewegen, also nicht im Widerspruch zu Entscheidungen der DSGVO stehen. Die § 12 Abs 1 sowie § 13 DSG konkretisieren mA die allgemeinen Regelungen der DSGVO hinsichtlich Bildverarbeitungen. Eine Videokonferenz würde sich als Rechtsgrundlage direkt auf Art 6 Abs 1 lit a, lit b bzw. lit f DSGVO stützen, die § 12 Abs 1 sowie § 13 DSG bleiben als reine Konkretisierungen der DSGVO parallel anwendbar und sind von österreichischen Arbeitgeber zu beachten, da sie der DSGVO nicht widersprechen.[648]

3.6 Konzerninterne Datentransfers

3.6.1 Datenschutzrechtliche Rollen im Konzern

Verantwortlicher (Art 4 Nr 7 DSGVO

Der Hauptadressat der datenschutzrechtlichen Pflichten aus der Datenschutz-Grundverordnung (EU) 2016/679 ist der „Verantwortliche" („Controller") als *„natürliche oder juristische Person, (...) die allein (...) über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet."* Kennzeichnend für die Rolle des allein Verantwortlichen ist, dass er/sie:

- über den Zweck bzw. die Zwecke der Verarbeitung personenbezogener Daten (Zweck der Verarbeitung) entscheidet,
- allein über die wesentlichen Aspekte der Mittel entscheidet, um das Ziel der Verarbeitung zu erreichen. Wesentliche Aspekte der Mittel sind dabei:
  - welche personenbezogenen Daten werden verarbeitet und mit welchem Inhalt,
  - die Aufbewahrungsdauer der personenbezogenen Daten,
  - wer Zugriff auf die personenbezogenen Daten hat (Rollen und Rechtekonzept),
  - an wen eine Übermittlung der Daten stattfinden soll und welche Rechtsgrundlage als Legitimation in Frage kommen soll.[649]

---

648 *Roßnagel* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 2 Rn 15 ff; § 5 Rn 9; *Roßnagel* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 1 Rn 13; § 9 Rn 9; *Barlag* in Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016) § 3 Rn 210 ff; AB 1761 BlgNR 25. GP 8.

649 *Art 29 Datenschutzgruppe,* WP 169 (2010) 10 ff.

Ein Arbeitgeber ist Verantwortlicher für die Daten seiner Beschäftigten und unterliegt damit vollumfänglich der DSGVO und den nationalen Datenschutzanpassungsgesetzen, die für ihn/sie anwendbar sind.[650]

Gemeinsam Verantwortliche (Art 4 Nr 7 DSGVO)

Neben dem allein Verantwortlichen existiert auch die Rolle des „gemeinsam Verantwortlichen" („Joint Controller"). Es geht hier darum, dass die oben genannten Punkte (Zwecke und/oder wesentliche Aspekte der Mittel) nicht von einer Stelle allein entschieden werden, sondern von zwei oder mehr Stellen gemeinsam, den dann gemeinsam Verantwortlichen (*„natürliche oder juristische Person (…), die gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet"*). Liegt gemeinsame Verantwortlichkeit (Joint Controllership) vor, ist eine Art 26 DSGVO Vereinbarung abzuschließen. Die gemeinsame Entscheidung über Zwecke und Mittel der Verarbeitung kann dabei unterschiedlich vorliegen, d.h. die Beteiligung der Parteien an den gemeinsamen Entscheidungen kann verschiedene Formen aufweisen und muss nicht gleichmäßig verteilt sein. Beispiele für gemeinsame Verantwortlichkeit sind Soziale Netzwerke, Social Plugins oder verschiedene Formen von Plattformen, wo von mehreren Verantwortlichen gemeinsam über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entschieden wird.

In einem Konzern wäre ein Beispiel für gemeinsame Verarbeitung (Joint Controllership) ein konzerninternes Corporate Social Network, wo Mitarbeiter verschiedener Konzerngesellschaften Inhalte hochladen und zugreifen können oder gemeinsame konzernübergreifende Plattformen oder Websites für Mitarbeiter und Kunden.[651]

Auftragsverarbeiter (Art 4 Nr 8 DSGVO)

Ein Auftragsverarbeiter ist *„eine natürliche oder juristische Person* (…)*, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet."* Die Existenz eines Auftragsverarbeiters hängt einmal von der Entscheidung eines Verantwortlichen (Art 4 Nr 7 DSGVO) ab, ob dieser personenbezogene Daten innerhalb seines eigenen Unternehmens durch seine eigenen Mitarbeiter verarbeiten lässt, oder die Verarbeitung personenbezogener Daten ganz oder teilweise an *„eine rechtlich selbstständige Person, die in seinem Auftrag handelt"* (externe natürliche oder juristische Person) delegieren will. Ein Auftragsverarbeiter (Art 4 Nr 8 DSGVO) ergibt sich insofern aus zwei maßgeblichen Kriterien:

- rechtliche Eigenständigkeit (natürliche oder juristische Person);
- die Verarbeitung personenbezogene Daten erfolgt im Auftrag des Verantwortlichen.

„Im Auftrag eines anderen zu handeln" bedeutet iSd. Europäischen Datenschutzrechts, dass man in dessen Interesse handelt iSv. Aufgabenübertragung („Delegation"). Im Kontext des Europäischen Datenschutzrechts ist es die Aufgabe eines Auftragsverarbeiters, die von dem für die Verarbeitung Verantwortlichen erteilten Weisungen zumindest hinsichtlich des

650 *Art 29 Datenschutzgruppe*, WP 249 (2017) 6 ff; *Art 29 Datenschutzgruppe*, WP 55 (2002) 3 ff; *Art 29 Datenschutzgruppe*, WP 48 (2001) 1 ff; *Art 29 Datenschutzgruppe* WP 42 (2001) 2 f.

651 Art 29 Datenschutzgruppe, WP 169 (2010) 21 ff; EuGH Urteil v. 29.07.2019, C-40/17 Rn 64 ff; EuGH Urteil v. 10.07.2018, C-25/17 Rn 63 ff; EuGH Urteil v. 05.06.2018, C-210/16 Rn 30; Rn 36 ff.

Zwecks der Verarbeitung und der wesentlichen Elemente der Mittel zu befolgen. Der Auftragsverarbeiter hat jedoch einen gewissen Ermessensspielraum in der Wahl der technischen und organisatorischen Mittel, damit er die Interessen des Verantwortlichen am besten wahrnehmen kann (Bsp. Hosting, Cloud Computing, Call Center, etc.).[652] Liegt ein solches Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter vor (Art 4 Nr 8 DSGVO), ist eine Vereinbarung nach Art 28 DSGVO abzuschließen. Wird der zulässige Rahmen der Auftragsverarbeitung gemäß den Vorgaben in Art 28 DSGVO verlassen, z.B. in dem sich der Auftragsverarbeiter nicht an die Weisungen des Verantwortlichen hält, wird der Auftragsverarbeiter selbst zum Verantwortlichen und rückt gemäß Art 28 Abs 10 DSGVO vollständig in die datenschutzrechtliche Verantwortung als Verantwortlicher (Art 4 Nr 7 DSGVO) mit den damit verbundenen Risiken.[653]

In Konzernen bestehen zwischen den einzelnen Konzerngesellschaften in der Regel diverse Auftragsverarbeitungsverhältnisse z.B. mit Beschäftigtendaten (u.a. Auslagerung der Lohn- und Gehaltsabrechnung, Errechnung der Löhne und Gehälter entsprechend der Tarifverträge, Erstellung der erforderlichen Steuererklärungen und die Auszahlung der Löhne und Gehälter, etc).[654]

Dritter (Art 4 Nr 10 DSGVO)

Die Datenschutz-Grundverordnung (EU) 2016/679 versteht unter dem Begriff „Dritter" einen Akteur, der über keine spezifische Legitimierung oder Befugnis – wie sie beispielsweise mit der Rolle als Verantwortlicher, Auftragsverarbeiter oder Mitarbeiter dieser Stellen verbunden ist – für die Verarbeitung personenbezogener Daten verfügt. Der Begriff wird hier ähnlich verwendet wie im Zivilrecht, wo ein Dritter ein Akteur ist, der weder Vertragspartei noch Teil einer Organisation ist.[655] Ordnet sich jemand als Arbeitnehmer einem Verantwortlichen (Art 4 Nr 7 DSGVO) oder einem Auftragsverarbeiter (Art 4 Nr 8 DSGVO) zu, setzt die Zuordnung im datenschutzrechtlichen Sinne zu diesen Stellen voraus, dass der Arbeitnehmer unter dessen unmittelbarer Verantwortung auch befugt ist, die in Rede stehenden Daten zu verarbeiten. Ist die Datenverarbeitung nicht von seiner arbeitsrechtlichen Kompetenz erfasst, ist auch ein Arbeitnehmer des Verantwortlichen oder eines Auftragsverarbeiters ein „Dritter" iSd Norm. Wenn der Arbeitnehmer die Daten unbefugt zu eigenen Zwecken verarbeitet, wird der Arbeitnehmer selbst zum Verantwortlichen iSd. Art 4 Nr 7 DSGVO.[656] Somit dient der Begriff des „Dritten" der Zuweisung von datenschutzrechtlicher Verantwortung, aus der sich entsprechende Rechtspflichten und ggf. eine entsprechende Haftung ergeben können. Kommt man zum Ergebnis, dass ein Dritter – rechtmäßig oder rechtswidrig – personenbezogene Daten empfangen hat, ist der Dritte als ein Verantwortlicher anzusehen und unterliegt sämtlichen Pflichten der DSGVO.[657]

Konzerngesellschaften sind rein datenschutzrechtlich zueinander „Dritte". Die konzerninterne Übermittlung von personenbezogenen Daten innerhalb einer Unternehmensgruppe

652 *Art 29 Datenschutzgruppe*, WP 169 (2010) 30 ff.
653 *Hartung* in Kühling/Buchner (Hrsg), DS-GVO BDSG^2 (2018) Art 4 Rn 9.
654 *Düsseldorfer Kreis*, Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer" (2005) 2 ff.
655 *Art 29 Datenschutzgruppe*, WP 169 (2010) 37 f.
656 *Ernst* in Paal/Pauly (Hrsg), DS-GVO BDSG^2 (2018) Art 4 Rn 59 f.
657 *Hartung* in Kühling/Buchner (Hrsg), DS-GVO BDSG^2 (2018) Art 4 Rn 5.

wird aber vom Europäischen Gesetzgeber bspw. zu Zwecken der Verhinderung von Betrug (ErwGr 47), zu internen Verwaltungszwecken von Kunden- und Beschäftigtendaten (ErwGr 48) und zu Zwecken der IT-Sicherheit (ErwGr 49), etc. ausdrücklich als berechtigte Interessen der jeweils betroffenen Verantwortlichen innerhalb der Unternehmensgruppe anerkannt und – bei Einhaltung aller anderen Datenschutzanforderungen – damit grundsätzlich als legitim angesehen.

Empfänger (Art 4 Nr 9 DSGVO)

Empfänger ist jede Person oder Stelle, der personenbezogene Daten offengelegt (übermittelt) werden (Art 4 Nr 2 DSGVO). Auch der „Dritte" (Art 4 Nr 10 DSGVO) und der Auftragsverarbeiter (Art 4 Nr 8 DSGVO) fallen unter den Begriff „Empfänger". Nicht geklärt ist, ob die Definition des „Empfängers" in jedem Fall eine rechtliche Eigenständigkeit verlangt, oder ob z.B. der Betriebsrat in einem Unternehmen auch als Empfänger iSd. Art 4 Nr 9 DSGVO gilt. Der Begriff des Empfängers ist wichtig im Rahmen der Informationspflichten (Art. 12 ff DSGVO), der Auskunftsrechte (Art 15 DSGVO), Mitteilungspflichten (Art 19 DSGVO) und beim Verzeichnis der Verarbeitungstätigkeiten (Art 30 DSGVO).[658]

Somit sind in einem Konzern sowohl Konzerngesellschaften, die Daten übermittelt bekommen (z.B. die Übermittlung von Compliance-Hinweisen zwischen Konzerngesellschaften gemäß Art 6 Abs 1 lit f DSGVO)[659], als auch Konzerngesellschaften denen Daten im Rahmen einer Auftragsverarbeitung (Art 4 Nr 8 iVm. Art 28 DSGVO) überlassen werden (iSv. offen gelegt werden iSd. Art 4 Nr 2 DSGVO) jeweils „Empfänger" gemäß des Art 4 Nr 9 DSGVO.[660]

3.6.2 Allgemeine Voraussetzungen von Datentransfers im Konzern

Für die Übermittlung von personenbezogenen Daten im Konzern gilt wie auch an externe Stellen die sogenannte 2-Stufen-Prüfung. Werden die personenbezogenen Daten nur innerhalb des EU und EWR Raums übermittelt, entfällt die Prüfung der Stufe 2.

Stufe 1: Die Verarbeitungstätigkeit muss alle DSGVO Anforderungen für eine Verarbeitung innerhalb des EU/EWR-Raums erfüllen, insbesondere muss eine gültige Rechtgrundlage (Art 6 Abs 1, Art 9 Abs 2 DSGVO) vorliegen und die Datenschutzgrundsätze (Art 5 Abs 1 DSGVO) insbesondere Treu und Glauben und Transparenz müssen strikt beachtet werden.

Stufe 2: Ist gemäß 1. Stufe eine Verarbeitung DSGVO-konform und sollen die Daten auch an einen unsicheren Drittstaat außerhalb der EU übermittelt werden, müssen die spezifischen Anforderungen der Art 44 ff DSGVO an die Übermittlung in Drittländer beachtet

658 *Ernst* in Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018) Art 4 Rn 57 f.

659 *Datenschutzkonferenz*, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines – Firmeninterne Warnsysteme und Beschäftigtendatenschutz (2018) 4 ff.

660 *Düsseldorfer Kreis*, Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer" (2005) 2 ff.

werden. Dies gilt auch, wenn die empfangende Konzernstelle im Drittland die Daten nochmals weiterübermitteln will (ErwGr 101 iVm. Art 44 Satz 1 Hs 2 DSGVO).[661]

3.6.3 Auftragsverarbeitung

Eine Auftragsverarbeitung ist dadurch gekennzeichnet, dass der Auftraggeber (Verantwortlicher iSd. Art 4 Nr 7 DSGVO) eine andere Gesellschaft (Auftragsverarbeiter) beauftragt, bestimmte personenbezogene Daten weisungsgebunden zu verarbeiten. Die Rechtmäßigkeit der Datenverarbeitung wird über die Einhaltung der in Art 28 DSGVO definierten Anforderungen sichergestellt (1. Stufe). Der Auftragnehmer handelt wie eine virtuelle Abteilung des Auftraggebers und darf nur nach Weisungen des Auftraggebers Daten verarbeiten und nicht selbst über Zwecke und Mittel der Verarbeitung entscheiden.

Es ist gemäß Art 28 DSGVO ein Vertrag zur Auftragsverarbeitung abzuschließen. Ein AVV-Vertrag hat folgende Regelungsinhalte zu beinhalten:

- Gegenstand und Dauer der weisungsgebundenen Verarbeitung und Definition von Art und Zweck der Verarbeitung;[662]
- Definition von Art der personenbezogenen Daten der Kategorien betroffener Personen die im Rahmen der Auftragsverarbeitung verarbeitet werden;[663]
- Regelung der Rechte und Pflichten des Auftragsverarbeiters, insbesondere Verarbeitung der personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen;[664]
- Bekanntgabe und Hinweispflicht durch den Auftragsverarbeiter hinsichtlich des auf ihn anwendbaren Rechts eines EU-Mitgliedstaates oder Unionsrecht, welches den Auftragsverarbeiter verpflichtet – ohne Rücksprache mit dem Verantwortlichen – Daten des Verantwortlichen offen zu legen (z.B. StPO, etc.);[665]
- Ausdrückliches Verbot (bei externen Dienstleistern z.B. mit Konventionalstrafe) an den Auftragsverarbeiter hinsichtlich nach dem Unionsrecht unzulässigen Übermittlungen (es muss grundsätzlich gemäß Art 48 DSGVO ein MLAT Abkommen[666] mit der EU oder einem EU-Mitgliedstaat vorliegen) und Verbot von unabgestimmten Offenlegungen von Daten des Verantwortlichen an Stellen in Nicht-EU-Drittstaaten – z.B. unabgestimmte Offenlegung von Daten an Nicht-EU Drittstaaten Sicherheitsbehörden.[667]
- Dokumentationspflicht für Weisungen;[668]

---

661 *Datenschutzkonferenz*, Kurzpapier Nr. 4 – Datenübermittlung in Drittländer (2017) 1 ff; *Düsseldorfer Kreis*, Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen (2013) 1; *Europäische Datenschutzausschuss*, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 (2018) 3 f; *Art 29 Datenschutzgruppe*, WP 158 (2009) 9 ff.

662 Art 28 Abs 3 Satz 1 DSGVO.

663 Art 28 Abs 3 Satz 1 DSGVO.

664 Art 28 Abs 3 Satz 2 lit a DSGVO.

665 Art 28 Abs 3 Satz 2 lit a Hs 2 DSGVO.

666 MLAT: Mutual Legal Assistance Treaty.

667 Art 48 DSGVO; *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz (2014) Teil 7 Rn 19; (diese Anforderung an ein MLAT Abkommen wird von *Spies* in v.d. Busche/Voigt (Hrsg), Konzerndatenschutz 2. Auflage 2019 Teil 7 Rn 13 ff offenbar nicht mehr behandelt, wie noch in der 1. Auflage 2014).

668 Art 28 Abs 3 Satz 2 lit a DSGVO.

- Hinweispflicht des Auftragsverarbeiters bei potentiell rechtswidrigen Weisungen durch den Auftragsverarbeiter;[669]
- nur weisungsabhängige Drittlandsübermittlung;[670]
- Einhaltung aller Maßnahmen gem. Art. 29, 30, 32 – 36 DSGVO und Unterstützungspflicht des Auftraggebers bei der Einhaltung der DSGVO;[671]
- Nachweispflicht gegenüber dem Auftraggeber im Hinblick auf die Einhaltung der DSGVO-Anforderungen als Auftragsverarbeiter;[672]
- Verpflichtung der zur Verarbeitung betraute Personen auf Vertraulichkeit, sofern diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheit unterliegen;[673]
- Kein Einsatz weiterer Auftragsverarbeiter ohne Genehmigung des Verantwortlichen;[674]
- Unterstützung des Verantwortlichen mit technischen und organisatorischen Maßnahmen bei der Einhaltung der Anforderungen zur Sicherheit personenbezogener Daten und bei der Datenschutz-Folgenabschätzung;[675]
- Löschung oder Rückgabe sämtlicher personenbezogener Daten nach Vertragsende (Wahlrecht durch Verantwortlichen);[676]
- Bereitstellung aller Informationen für den Nachweis der Einhaltung sämtlicher DSGVO-Pflichten (Accountability).[677]

Soll im Rahmen einer Auftragsverarbeitung eine Datenweitergabe im Konzern an eine Konzerngesellschaft in einem unsicheren Drittstaat erfolgen, sind die allgemeinen Anforderungen der Art 44 ff DSGVO an Internationale Datentransfers zusätzlich zu erfüllen (2. Stufe).[678] Bei Auftragsverarbeitungen schaffen die EU-Standardvertragsklausen Entscheidung 2010/87/EU (Controller to Processor) ein angemessenes Schutzniveau auf der 2. Stufe.[679]

3.6.4 Datenschutzrechtliche Übermittlung

Personenbezogene Daten dürfen auf Basis einer gültigen Rechtsgrundlage an einen anderen Verantwortlichen übermittelt werden. Im Regelfall stützt sich die Datenübermittlung im Konzern auf ein berechtigtes Interesse iSd. Art 6 Abs 1 lit f DSGVO bzw. in Deutschland, wenn es die Tätigkeit erfordert, auch im Rahmen der Erforderlichkeit zur Durchführung des Beschäftigtenverhältnisses gemäß § 26 Abs 1 BDSG. Folgende berechtigte Interessen an

669 Art 28 Abs 3 Satz 3 DSGVO.
670 Art 28 Abs 3 Satz 2 lit a DSGVO.
671 Art 28 Abs 3 lit c und lit f DSGVO.
672 Art 28 Abs 3 Satz 2 lit h DSGVO.
673 Art 28 Abs 3 Satz 2 lit b DSGVO iVm. Art 29 DSGVO iVm. Art 32 Abs 4 DSGVO.
674 Art 28 Abs 3 Satz 2 lit d Art 28 Abs 2 und Abs 4 DSGVO.
675 Art 28 Abs 3 Satz 2 lit e und lit f DSGVO.
676 Art 28 Abs 3 Satz 2 lit g DSGVO.
677 Art 28 Abs 3 Satz 2 lit h DSGVO.
678 Hessischer Landtag, Drucksache 16/7646, 19 ff.
679 Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates 2010/87/EG, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 (zuletzt abgerufen am 20.06.2019).

der Übermittlung von personenbezogenen Daten werden unmittelbar in der DSGVO anerkannt:

- (ErwGr 47): Verarbeitung personenbezogener Daten zu Zwecken der Verhinderung von Betrug;
- (ErwGr 48): Verarbeitung personenbezogener Daten innerhalb einer Unternehmensgruppe zu internen Verwaltungszwecken von Kunden- und Beschäftigtendaten;
- (ErwGr 49): Verarbeitung personenbezogener Daten zu Zwecken der Verbesserung der Netz- und IT-Sicherheit.

Darüberhinaus existieren noch viele denkmögliche berechtigte Interessen im Konzern. Bei einer datenschutzrechtlichen Übermittlung ohne gemeinsame Verarbeitung, bleiben die einzelnen Stellen im Konzern jeweils getrennt verantwortlich (Art 4 Nr 7 DSGVO). Die Datenhoheit liegt bei jeder einzelnen Konzerngesellschaft. Die Gesellschaft, welche übermittelt, trägt die Verantwortlichkeit für die Rechtskonformität dieser Übermittlung (Offenlegung). Erhält eine Konzerngesellschaft personenbezogene Daten und hat sie keine Rechtsgrundlage, die erhaltenen personenbezogenen Daten selbst zu verarbeiten, sind diese daher *ex lege* sofort wieder zu löschen (Art 17 Abs 1 lit a, lit b, lit d DSGVO).

In Deutschland wurde ab 2004 ein Modell entwickelt, wie man konzerninterne Datentransfers (ohne gemeinsame Verantwortlichkeit) datenschutzrechtskonform gestalten kann. Dazu wären innerhalb eines Konzerns sogenannte (nicht gesetzlich geforderte) Datenschutzvereinbarungen abzuschließen, welche die Effektivität des Datenschutzes im Konzern gewährleisten sollen (Company-to-Company-Agreement).[680] Ein berechtigtes Interesse (Art 6 Abs 1 lit f DSGVO) an der Übermittlung zwischen Konzerngesellschaften liegt nach Ansicht der *ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer"* vor, wenn folgende Voraussetzungen vorliegen:

- Die Übermittlung darf nicht dazu führen, dass andere Konzernunternehmen die Daten in einer Weise nutzen, die dem Arbeitgeber selbst verwehrt wäre.
- Die Übermittlung darf nur mit klarer Festlegung der Zweckbindung erfolgen und nur, wenn und soweit die personenbezogenen Daten für die von anderen Konzernunternehmen jeweils übernommene Funktion erforderlich sind. Die Datenverarbeitung beim Zielunternehmen sollte nicht über die zweckgebundene Datenverarbeitung des übermittelnden Unternehmens hinausgehen.
- Haftung des Daten empfangenden Unternehmens für Verstöße gegen den Vertrag (Company-to-Company-Agreement) inklusive Kontrollrechte bzgl. der Daten.
- Besondere Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO) sollten soweit als möglich nicht verarbeitet werden.
- Klare Überprüfungsfristen für die Speicherung der personenbezogenen Daten.
- Der Konzern muss besondere Maßnahmen ergreifen, um den Interessen der Betroffenen Rechnung zu tragen. Dazu gehört:
  - ein konzernweites Datenschutzkonzept,
  - dass das Arbeitgeber-Unternehmen – zusätzlich – umfassend datenschutzrechtlicher Ansprechpartner für seinen Arbeitnehmer bleibt, z.B. betreffend Schadenersatz, Auskunft etc.,

680 *Lachenmann,* Datenübermittlung im Konzern (2016) 312 ff.

– dass die entsprechenden Regelungen intern (im Konzern) und extern (gegenüber den Betroffenen) tatsächlich und effektiv verbindlich sind.[681]

Soll eine Datenübermittlung im Konzern in einem unsicheren Drittstaat erfolgen, sind die speziellen Anforderungen der Art 44 ff DSGVO an Internationale Datentransfers zu erfüllen (2. Stufe).[682] Möglichkeiten bieten dabei der Abschluss der EU-Standardverträge für Controller to Controller Verhältnisse (Entscheidung 2001/497/EG[683] bzw. Entscheidung 2004/915/EG)[684] oder ein Berufen auf einen Ausnahmetatbestand in Art 49 Abs 1 DSGVO.

3.6.5 Gemeinsame Verantwortlichkeit

Nach aktueller Rechtsprechung des EuGH liegt eine gemeinsame Verantwortlichkeit vor, wenn eine natürliche oder jurstische Person aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel der Verarbeitung mitwirkt. Dabei wird keine gleichwertige Verantwortlichkeit aller beteiligten Akteure vorausgesetzt, die Akteure können jeweils in verschiedenen Phasen der Verarbeitung und in unterschiedlichem Ausmaß einbezogen sein. Der Grad der Verantwortlichkeit eines jeden ist unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen.[685] Für vor- oder nachgelagerte Verarbeitungsphasen, wo ein Akteur weder die Zwecke noch die Mittel (mit-)festlegt, besteht keine datenschutzrechtliche (Mit-)Verantwortlichkeit. Es ist insofern die konkrete Verantwortlichkeit anhand der jeweiligen Phase einer Datenverarbeitung zu prüfen.[686]

Hinsichtlich der von den beteiligten Akteuren festzulegenden gemeinsamen „Zwecke" wird vom EuGH dabei nicht auf eine eindeutige (identische) Zweckidentität abgestellt, sondern es reicht das Vorliegen einer Einheit der von den beteiligten Akteueren verfolgten Zwecke (z.B. die beteiligten Akteuere verfolgen gemeinsam zusammenwirkend jeweils eigene kommerzielle oder werbliche Zwecke zu ihren Vorteilen im wirtschaftlichen Interesse).[687]

Hinsichtlich der gemeinsamen „Mittel" ist abzustellen, ob die beteiligten Akteure über die eingesetzten Mittel gemeinsam entscheiden, dies ist z.B. bei der Einbindung eines Social

---

681 *Düsseldorfer Kreis*, Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer" (2005) 2 ff; *Hessischer Landtag*, Drucksache 16/4752, 28 ff; *Hessischer Landtag*, Drucksache 16/7646, 19 ff; *Hartung* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) Art 26 Rn 24.

682 *Hessischer Landtag*, Drucksache 16/7646, 19 ff; *Lachenmann,* Datenübermittlung im Konzern (2016) 315 f.

683 Entscheidung der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (2001/497/EG), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32001D0497 (zuletzt abgerufen am 20.06.2019).

684 Entscheidung der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2004/915/EG), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32004D0915 (zuletzt abgerufen am 20.06.2019).

685 EuGH Urteil v. 29.07.2019, C-40/17 Rn 68 ff; EuGH Urteil v. 10.07.2018, C-25/17 Rn 66 ff; EuGH Urteil v. 05.06.2018, C-210/16 Rn 30 ff.

686 EuGH Urteil v. 29.07.2019, C-40/17 Rn 74.

687 EuGH GA v. 19.12.2018, C-40/17 Rn 104; EuGH Urteil v. 29.07.2019, C-40/17 Rn 80 ff.

Plugins auf der Website der Fall. Der Websitebetreiber als Verantwortlicher für die Website entscheidet sich ein Plugin, welches von einem anderen Akteur zur Verfügung gestellt wird, auf seiner Website einzubinden. Dieses Plugin erhebt Daten und sendet diese Daten (auch) an den Bereitsteller des Plugins. Damit entscheiden für die Phasen der Erhebung auf der Website durch das Plugin und der nachfolgenden Übermittlung an den Bereitsteller des Plugins beide gemeinsam über die Mittel der Verarbeitung in den Verarbeitungsphasen „Erhebung" und „Übermittlung" und sind dafür dann gemeinsam verantwortlich.[688] Für die spätere Weiterverarbeitung nach der erfolgten Übermittlung an den Betreiber des Plugins, besteht für den Website-Betreiber keine datenschutzrechtliche Verantwortlichkeit mehr.[689]

Nach EuGH ist es bezüglich der Rechtsgrundlagen (Art 5 Abs 1 lit a DSGVO) – am Beispiel der „berechtigten Interessen" (Art 6 Abs 1 lit f DSGVO) – „*erforderlich, dass jeder dieser Verantwortlichen mit diesen Verarbeitungsvorgängen ein berechtigtes Interesse im Sinne von [Art 6 Abs 1 lit f DSGVO]*[690] *wahrnimmt, damit diese Vorgänge für jeden Einzelnen von ihnen gerechtfertigt sind.*"[691] Insofern muss für jeden Akteur das berechtigte Interesse jeweils gleichzeitig vorliegen. *Piltz* vertrat vor dem EuGH Urteil (C-40/17) vom Juli 2019 mit Verweis auf Art 4 Nr 10 DSGVO („Verantwortlicher" ist kein „Dritter") noch die divergierende Meinung, welcher der EuGH nicht folgte, dass bei gemeinsamer Verantwortlichkeit iSd. Art 26 DSGVO keine rechtfertigungsbedürftige Datenübermittlung vorliege, sondern eine privilegierte Datenweitergabe wie bei der Auftragsverarbeitung.[692]

Gemeinsam Verantwortliche haben eine Vereinbarung gemäß Art 26 Abs 1 Satz 2 DSGVO abzuschließen. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln und das Wesentliche der Vereinbarung ist auch den betroffenen Personen zur Verfügung zu stellen. Aufsichtsbehörden als auch die betroffenen Personen müssen wissen, wer für welche (Phase einer) Verarbeitung verantwortlich ist.[693] In dieser Vereinbarung ist in transparenter Form festzulegen, wer von den gemeinsam Verantwortlichen welche Verpflichtung gemäß der DSGVO erfüllt (insb. Sicherstellung der Betroffenenrechte gem. Art. 12 ff DSGVO). Es hat „*eine klare Zuteilung der Verantwortlichkeiten*" (ErwGr 79) zu erfolgen.[694]

Eine betroffene Person kann ihre durch die DSGVO gewährleisteten Rechte jedoch auch weiterhin gegenüber jedem einzelnen der gemeinsam Verantwortlichen im Konzern geltend machen. Diese Klarstellung in Art 26 Abs 3 DSGVO betrifft aber nicht die nach der Geltendmachung des Betroffenen erfolgende Erfüllung der den jeweiligen Betroffenenrechten zu Grunde liegenden gesetzlichen Verpflichtungen. Welcher der gemeinsamen Verantwort-

688 EuGH Urteil v. 29.07.2019, C-40/17 Rn 77 ff; EuGH GA v. 19.12.2018, C-40/17 Rn 130.
689 EuGH Urteil v. 29.07.2019, C-40/17 Rn 76; EuGH GA v. 19.12.2018, C-40/17 Rn 108.
690 Im Originaltext: Art. 7 Buchst. f der Richtlinie 95/46
691 EuGH Urteil v. 29.07.2019, C-40/17 Rn 96.
692 *Piltz* in Gola (Hrsg), DS-GVO^2 (2018) Art 26 Rn 8.
693 *Hartung* in Kühling/Buchner (Hrsg), DS-GVO BDSG^2 (2018) Art 26 Rn 22; *Piltz* in Gola (Hrsg), DS-GVO^2 (2018) Art 26 Rn 2.
694 *Piltz* in Gola (Hrsg), DS-GVO^2 (2018) Art 26 Rn 9 ff.

lichen etwa Auskunft erteilt, Daten löscht oder sperrt oder Daten an einen anderen Verantwortlichen übertragen muss, kann sich aus der Vereinbarung gemäß Art 26 Abs 1 Satz 2 DSGVO zwischen den gemeinsam Verantwortlichen ergeben.[695]

Für eine Art 26 DSGVO-Vereinbarung ergibt sich folgender Regelungsgegenstand[696]:

- in Anlehnung Art 28 Abs 3 Satz 1 DSGVO eine Beschreibung der Datenverarbeitung (Gegenstand und Dauer, Art und Zweck, Art der personenbezogenen Daten sowie Kategorien betroffener Personen);
- die verschiedenen Phasen der Verarbeitungen, Funktionen und Beziehungen der gemeinsam Verantwortlichen zueinander;
- eine generelle Beschreibung der Verteilung der datenschutzrechtlichen Verantwortlichkeiten inkl. einer Regelungen über den Haftungsausgleich im Innenverhältnis wegen der gesamtschuldnerischen (Außen-)Haftung (Art 82 DSGVO).
- eine Festlegung der jeweiligen Rechtmäßigkeitsvoraussetzungen, insbesondere dann, wenn eine übergreifende Zusammenarbeit bei der Umsetzung erforderlich ist (wer verfasst welche Einwilligungserklärungen? Wer legt berechtigte Interessen fest? Wer kümmert sich um Widersprüche der Betroffenen nach Art 21 Abs 1 DSGVO?);
- Vereinbarung über den Umgang mit Betroffenenrechten:
  - wer erteilt wie die Informationen nach Art 13, Art 14 DSGVO;
  - fakultativ – Benennung eines gemeinsamen Ansprechpartners für Anfragen und Ausübung der Betroffenenrechte;
  - Vereinbarung über die interne praktische Umsetzung und technische Verwirklichung der Betroffenenrechte (wie bewerkstelligt man ein Löschungsbegehren bei allen Verantwortlichen? Wie setzt man das Recht auf Datenübertragbarkeit um?);
  - Vereinbarungen über die Vornahme von technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO (wer ist wofür verantwortlich, welche Schnittstellen gibt es?);
  - notwendige Zusammenarbeit und gegenseitige Unterstützung im Rahmen der Datenschutz-Folgenabschätzung nach Art 35, Art 36 DSGVO;
  - Zusammenarbeit bei der Feststellung, Behandlung und Meldung von Datenschutzverletzungen nach Art 33, Art 34 DSGVO (gegenseitige Information, eventuell Bestimmung eines federführenden Verantwortlichen);
  - Nennung von gegenseitigen Ansprechpartnern für den Datenschutz und Vereinbarung von Notfall- und Eskalationsmechanismen (z.B. im Falle von Datenschutzverletzungen oder Behördenanfragen);
  - gegenseitige Pflichten zur Information soweit erforderlich (z.B. für die Erstellung von Verarbeitungsverzeichnissen);
  - bei internationalen Übermittlungen Festlegung der eingesetzten Mechanismen und Verantwortlichkeiten;
  - Bestimmung über den Umgang mit Änderungen, die Auswirkungen auf den Datenschutz und die anderen Verantwortlichen haben können (Change Management).[697]

Die Rechtmäßigkeit der gemeinsamen Verarbeitung ergibt sich aus den Art 5 ff DSGVO (1. Stufe). Hinsichtlich internationaler Datentransfers müssen zusätzlich die Anforderungen

695 *Piltz* in Gola (Hrsg), DS-GVO^2 (2018) Art 26 Rn 25 ff.
696 *Hartung* in Kühling/Buchner (Hrsg), DS-GVO BDSG^2 (2018) Art 26 Rn 25.
697 *Hartung* in Kühling/Buchner (Hrsg), DS-GVO BDSG^2 (2018) Art 26 Rn 25.

aus den Art 44 ff DSGVO sichergestellt werden (2. Stufe). Möglichkeiten bieten dabei der Abschluss der EU-Standardverträgen für Controller to Controller Verhältnisse (Entscheidung 2001/497/EG[698] bzw. Entscheidung 2004/915/EG)[699] oder ein Berufen auf einen Ausnahmetatbestand in Art 49 Abs 1 DSGVO.

698 Entscheidung der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (2001/497/EG); abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32001D0497 (zuletzt abgerufen am 20.06.2019).

699 Entscheidung der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2004/915/EG), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32004D0915 (zuletzt abgerufen am 20.06.2019).

4 Arbeitsrechtliche Anforderungen IT-gestützter Arbeitsplatz

4.1 Deutschland

4.1.1 Überblick

Zur finalen allgemeinen arbeitsrechts- und datenschutzrechtlichen Zulässigkeit eines IT-Systems bzw. einer Maßnahme bedarf es der Zulässigkeit in allen drei Themenbereichen:

- Allgemeinen Persönlichkeitsrecht (Art 2 Abs 1 iVm. Art 1 Abs 1 GG iVm. § 823 Abs 1 BGB) und den Arbeitsschutzvorschriften als Teil der arbeitsrechtlichen Fürsorgepflicht des Arbeitgebers gemäß § 618 BGB (siehe **Kapitel 4.1.2** und **Kapitel 4.1.4**);
- Kollektives Arbeitsrecht gemäß § 75 Abs 2 iVm. § 87 Abs 1 Nr 6 BetrVG (siehe **Kapitel 4.1.3**);
- DSGVO und BDSG Konformität von Verarbeitungen (siehe oben **Kapitel 3**).

4.1.2 Allgemeines Persönlichkeitsrecht (Art 2 Abs 1 iVm. Art 1 Abs 1 GG, § 823 BGB)

In Deutschland wird der Schutz des Allgemeinen Persönlichkeitsrechts jedermann nach Art 2 Abs 1 iVm. Art 1 Abs 1 GG garantiert (vgl. **Kapitel 2.2.3**). Auch juristischen Personen sind im Rahmen der Gewährleistung ihrer wirtschaftlichen Betätigung davon erfasst.[700] Das Allgemeine Persönlichkeitsrecht aus Art 2 Abs 1 GG iVm Art 1 Abs 1 gilt im Zivilrecht im Wege der mittelbaren Drittwirkung, wobei im Zivilrecht die Grenzen und die Reichweite des Allgemeinen Persönlichkeitsrecht als sonstiges Recht iSd. § 823 Abs 1 BGB autonom bestimmt werden unter Berücksichtigung dieser mittelbaren Drittwirkung.[701]

Im Arbeitsverhältnis limitiert das Allgemeine Persönlichkeitsrecht die Reichweite der Direktions- und Kontrollrechte des Arbeitgebers und knüpft sie an den Verhältnismäßigkeitsgrundsatz und das Gebot des billigen Ermessens. Der Arbeitgeber hat ein Interesse an der „Aufrechterhaltung der betrieblichen Ordnung“ und, dass sich die Arbeitnehmer während ihrer Arbeitszeit „nur betrieblichen Beschäftigungen“ (arbeitsvertragliche Pflichten) widmen und betriebliche Mittel nicht für eigene Zwecke entfremden oder gar strafrechtswidrig entwenden. Es handelt sich also um einen Grundkonflikt zwischen Compliance und Persönlichkeitsschutz. Seine Interessenswahrnehmung kann der Arbeitgeber mit entsprechenden Mitarbeiterkontrollen erreichen.[702] Gleichzeitig hat auch der Arbeitgeber selbst das Persönlichkeitsrecht seiner Arbeitnehmer streng zu achten und muss dazu die Arbeitnehmer vor Beeinträchtigungen ihrer Persönlichkeitsrechte schützen (Fürsorgepflicht gemäß § 618

700 zuletzt: BVerfG Beschluss v. 27.06.2018, Az. 2 BvR 1405/17 Rn. 61.

701 *Geiger* in Weth/Herberger/Wächter (Hrsg), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014) Teil A. II. Rn 5 ff; Rn 23 ff.

702 *Geiger* in Weth/Herberger/Wächter (Hrsg), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014) Teil A. II. Rn 40 ff; *Oberwetter*, Arbeitnehmerrechte bei Lidl, Aldi & Co, NZA 2008, 609; *Raffler/Hellich*, NZA 1997, 862; BAG Urteil v. 04.04.1990 – 5 AZR 299/89; BVerfG Urteil v. 19.12.1991, Az. 1 BvR 382/85.

C. Jaksch, *Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes*,
AutoUni – Schriftenreihe 143, https://doi.org/10.1007/978-3-658-29450-2_4

BGB).[703] Die Grundrechtskollisionen zwischen Arbeitgeber und Beschäftigte stellen sich wie folgt dar: Auf der Seite des Arbeitgebers stehen als Grundrechtspositionen das Recht auf Berufsfreiheit (Art 12 GG und Art 15 EU-GRC), das Recht auf Eigentum (Art 14 GG sowie Art 1 des 1. Zusatzprotokoll EMRK und Art 17 EU-GRC) und das Recht auf unternehmerische Freiheit (Art 16 EU-GRC). Auf der Seite der Beschäftigten stehen das Allgemeine Persönlichkeitsrecht in seinen unterschiedlichen Ausprägungen u.a. als Recht auf informationelle Selbstbestimmung und Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art 2 Abs 1 iVm. Art 1 Abs 1 GG), sowie das Brief- Post- und Fernmeldegeheimnis (Art 10 GG), das Recht auf Privatleben und Vertraulichkeit der Korrespondenz bzw. Kommunikation (Art 8 EMRK bzw. Art 7 EU-GRC), das Recht auf Datenschutz (Art 8 EU-GRC), das Recht auf Unterrichtung und Anhörung der Arbeitnehmerinnen und Arbeitnehmer im Unternehmen (Art 27 EU-GRC) und das Recht auf gerechte und angemessene Arbeitsbedingungen (Art 31 EU-GRC).[704] Es hat im Einzelfall eine Abwägung dieser Interessen (als divergierende Grundrechtspositionen) stattzufinden, bei der die Belange der Beschäftigten umso mehr Gewicht gewinnen, je intensiver eine bestimmte Sphäre des Persönlichkeitsrechts der Beschäftigten betroffen ist:

- *Sozialsphäre*: Diese Sphäre betrifft Beziehungen zur Umwelt, öffentliches, wirtschaftliches und berufliches Wirken. Die Sozialsphäre ist typischerweise Beschränkungen ausgesetzt und ist Gegenstand des Direktionsrechts des Arbeitgebers unter Berücksichtigung des Maßregelungsverbots und des Gebots des billigen Ermessens;
- *Persönlichkeitssphäre:* Diese Sphäre betrifft die Weltanschauung, persönliche und familiäre Beziehungen, Vermögensverhältnisse, Hobbies. Es darf nur ausnahmsweise eingegriffen werden mit besonderer Rechtfertigung (Überwachung am Arbeitsplatz).
- *Intimsphäre:* Eingriffe in die Intimsphäre (Gesundheit, Partnerschaft, Sexualität, etc.) sind regelmäßig nicht zu rechtfertigen (z.B. Recht auf Lüge eines Bewerbers).[705]

Durch die immer nur im Einzelfall mögliche und notwendige Abwägung dieser Interessen (grundrechtliche Positionen des Arbeitgebers gegen insb. Persönlichkeitsrechte des Arbeitnehmers) besteht erhebliche Rechtsunsicherheit bei der richtigen Beurteilung.[706]

Aufgrund des Umstandes, dass in Deutschland § 26 BDSG im Beschäftigtenverhältnis gemäß § 26 Abs 7 BDSG auch auf Sachverhalte anzuwenden ist, wenn personenbezogene Daten von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen (vgl. anders Art 2 Abs 1 DSGVO), ist die datenschutzrechtliche Prüfung nach § 26 BDSG in fast jeder Sachverhaltskonstellation am Arbeitsplatz relativ gleichlaufend mit der Prüfung nach der Vereinbarkeit mit den Persönlichkeitsrechten (z.B. bei Spindkontrolle ohne automatisierte Datenverarbeitung bzw. nicht-au-

703 *Zöllner/Loritz/Hergenröder*, Arbeitsrecht[7] (2015) 2. Teil § 19 Rn 6 ff; *Weidenkaff* in Palandt (Hrsg), Bürgerliches Gesetzbuch[78] (2019) § 618 Rn 3 ff; *Dütz/Thüsing*, Arbeitsrecht[23] (2018) § 7 Rn 304a.

704 *Däubler*, Gläserne Belegschaften[8] (2019) § 3 Rn 110 ff; *Raffler/Hellich*, NZA 1997, 862.

705 *Geiger* in Weth/Herberger/Wächter (Hrsg), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014) Teil A. II. Rn 36 ff; *Sprau* in Palandt (Hrsg), Bürgerliches Gesetzbuch[78] (2019) § 823 Rn 83 ff.

706 *Geiger* in *Weth/Herberger/Wächter (Hrsg)*, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014) 26 f.

tomatisierte Datenverarbeitung in einem Dateisystem). Im unbestimmten Merkmal der „Erforderlichkeit“ in der Generalklausel des § 26 Abs 1 Satz 1 BDSG findet sich nach *Dütz/Thüsing* die Einbruchstelle für die mittelbare Drittwirkung der Grundrechte. Durch diese Generalklausel wird es möglich, bei der Abwägung der divergierenden Interessen im Rahmen der datenschutzrechtlichen Prüfung, sich weitgehend an den verfassungsrechtlichen (bzw. zivilrechtlichen) Entscheidungen zum Persönlichkeitsrecht zu orientieren.[707]

Damit ist mA ein enormer Gleichlauf zwischen Datenschutzrecht und dem verfassungs- und zivilrechtlichem Persönlichkeitsrechten direkt über die Generalklausel der „Erforderlichkeit“ in § 26 Abs 1 Satz 1 BDSG möglich, sodass die Prüfung der Vereinbarkeit und Verhältnismäßigkeit von Maßnahmen (DSGVO/BDSG und §§ 242, 823, 1004 BGB, etc.) relativ rechtssicher über die Rechtsgrundlage § 26 BDSG laufen kann.

4.1.3 Mitwirkung und Mitbestimmung des Betriebsrats nach BetrVG

§ 75 Abs 2 Satz 1 BetrVG bildet den Anknüpfungspunktfür den Beschäftigtendatenschutz im BetrVG[708] und lautet: „*Arbeitgeber und Betriebsrat haben die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern*.“[709]

§ 80 Abs 1 Nr 1 BetrVG trägt dem Betriebsrat dazu eine konkrete und umfassende Überwachungspflicht auf, darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze (z.B. DSGVO, BDSG), Tarifverträge und Betriebsvereinbarungen, etc. im Unternehmen/Betrieb eingehalten und durchgeführt werden. § 80 Abs 2 Satz 1 BetrVG gibt dem Betriebsrat dazu korrespondierend starke Informationsrechte zur effektiven Durchführung seiner Aufgaben. § 80 Abs 2 Satz 2 BetrVG konkretisiert diese Informationsrechte, dass dem Betriebsrat auf sein Verlangen jederzeit Unterlagen zur Verfügung zu stellen sind, soweit dies zur Durchführung seiner Tätigkeit erforderlich ist. Nach § 80 Abs 2 Satz 4 hat der Arbeitgeber zudem dem Betriebsrat auch sachkundige Arbeitnehmer als Auskunftspersonen zur Verfügung zu stellen (IT-Beauftragter, Datenschutzbeauftragter). Diese Überwachungspflicht des Betriebsrats gemäß § 80 Abs 1 BetrVG tritt beim Thema Datenschutz direkt neben die korrespondierende Überwachungspflicht des betrieblichen Datenschutzbeauftragten nach Art 39 Abs 1 lit b DSGVO („Prinzip der doppelten Kontrolle“). Dazu gehört auch, dass der Betriebsrat die Tätigkeit des betrieblichen Datenschutzbeauftragten selbst zu prüfen hat, dass dieser seine Tätigkeit gemäß Art 38 DSGVO ordnungsgemäß und tatsächlich weisungsfrei ausüben kann. Die Überwachungspflicht des Betriebsrats nach § 80 Abs 1 BetrVG allein begründet noch kein eigenständiges Mitbestimmungsrecht. Die Überwachungspflicht des Betriebsrats nach § 80 Abs 1 Nr 1 BetrVG ist bei der Thematik Datenschutz insofern sehr ähnlich zur Aufgabe des betrieblichen Datenschutzbeauftragten (Art 39 Abs 1 lit b DSGVO iVm. Art 38 Abs 3 Satz 3 DSGVO), nämlich mögliche Rechtsverstöße zu identifizieren, den Arbeitgeber auf die entdeckten möglichen (Datenschutz-)Rechtsverstöße hinzuweisen und zur Korrektur zu bewegen. Auch der Datenschutzbeauftragte hat keine eigenen Handlungsbefugnisse selbst Datenschutzverstöße kraft eigener Autorität im Unternehmen abzustellen. Dem Datenschutzbeauftragten trifft jedoch

707 *Dütz/Thüsing*, Arbeitsrecht[23] (2018) § 1 Rn 13; § 2 Rn 54; § 7 Rn 304 f; Rn 307 f.

708 *Selk* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 3. Rn 32 ff.

709 § 75 Abs 2 BetrVG idF. BGBl. 2006 I. 1897.

zusätzlich zur Überwachungspflicht auch eine Beratungspflicht des Verantwortlichen (Art 39 Abs 1 lit a und lit c DSGVO), also konkrete Lösungen vorzuschlagen.[710] Entdeckt der Betriebsrat einen Datenschutzverstoß, muss er aufgrund des Grundsatzes der vertraulichen Zusammenarbeit (§ 2 Abs 1 BetrVG) zunächst auf innerbetrieblicher Ebene auf die Herstellung eines datenschutzrechtskonformen Zustandes hinwirken, bevor er die datenschutzrechtliche Aufsichtsbehörde kontaktiert.[711]

Gemäß § 87 Abs 1 Nr 1 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei Regelungen der Ordnung des Betriebs und damit hinsichtlich verbindlicher Verhaltensregeln. Zu unterscheiden ist dabei zwischen den mitbestimmungsfreien Maßnahmen des Arbeitgebers, die sich ausschließlich auf die arbeitsvertraglichen Leistungpflichten der Arbeitnehmer (Arbeitsverhalten) beziehen (z.B. generelle Untersagung der Privatnutzung der IT; Einsatz von Privatdetektiven, etc.) und den mitbestimmungspflichtigen Maßnahmen iSd. § 87 Abs 1 Nr 1 BetrVG, die das Ordnungsverhalten der Arbeitnehmer betreffen (Regelungen zur Benutzung betrieblicher Einrichtungen wie bspw. Benutzung des Telefons, Nutzung des Internets bzw. E-Mailssystems, etc.).[712]

Gemäß § 87 Abs 1 Nr 6 BetrVG hat der Betriebsrat – zur Konkretisierung des § 75 Abs 2 Satz 1 BetrVG[713] – ein zwingendes Mitbestimmungsrecht bei der Einführung und Anwendungen von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen. Das Mitbestimmungsrecht des § 87 Abs 1 Nr 6 BetrVG geht als speziellere Regelung dem Mitbestimmungsrecht des § 87 Abs 1 Nr 1 BetrVG vor. Voraussetzung für die Anwendung des § 87 Abs 1 Nr 6 BetrVG ist, dass eine „Überwachung" durch „technische Einrichtungen" erfolgt. Daher greift § 87 Abs 1 Nr 6 BetrVG nicht, wenn die Überwachung ohne technische Einrichtungen erfolgt (Testkunden, Privatdetektive, Vorgesetzte, etc.) oder nur über organisatorische Maßnahmen (Tätigkeits- und Arbeitsberichte, Arbeitsbücher, etc.). Sobald aber bspw. Privatdetektive technische Einrichtungen einsetzen, kommt § 87 Abs 1 Nr 6 BetrVG wieder zur Anwendung. Eine „Überwachung" iSd. § 87 Abs 1 Nr 6 BetrVG liegt vor, wenn durch den Einsatz von technischen Einrichtungen Informationen über das Verhalten oder die Leistung der Arbeitnehmer erhoben und aufgezeichnet werden. Unerheblich ist, ob der Arbeitgeber diese technischen Einrichtungen tatsächlich zur Kontrolle oder Überwachung einsetzt oder die technische Einrichtung zu einem anderen Zweck verwendet. Auf eine Überwachungsabsicht auf Seiten des Arbeitgebers hinsichtlich der technischen Einrichtung kommt es nicht an. Eine technische Einrichtung liegt vor, wenn es sich um ein optisches, akustisches, mechanisches oder elektronisches Gerät handelt, das objektiv geeignet ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (die erhobenen Daten können in irgendeiner Weise für die Beurteilung der Arbeitnehmer von Bedeutung sein). Beispiele für technische Einrichtungen, die das zwingende Mitbestimmungsrecht (§ 87 Abs 1 Nr 6 BetrVG) auslösen:

---

710 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017), C. III. Rn 10 ff; *Art 29 Datenschutzgruppe*, WP 243 rev.01, Leitlinien in Bezug auf Datenschutzbeauftragte (2017) 20.

711 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017), C. III. Rn 8.

712 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017), C. I. Rn 47 ff.

713 *Ricard/Maschmann* in Ricardi (Hrsg), Betriebsverfassungsgesetz[16] (2018) § 87 Rn 492; *Werner* in Rolfs/Giesen/Kreikebohm/Udsching (Hrsg), BeckOK Arbeitsrecht[51 Edition] (Stand 01.03.2019) § 87 BertVG Rn 89.

- Biometrische Kontrollsysteme,
- Telefonvermittlungsanlagen,
- Technische Geräte zum Einsatz von E-Mails oder Nutzung des Internets,
- Tonbandaufnahmen,
- Personalinformationssysteme (SAP),
- Mobile Kommunikationsgeräte (Smartphones, etc.),
- Privatdetektiv, der im Rahmen seiner Tätigkeit technische Einrichtungen einsetzt.

Nach *Ricardi/Maschmann* wird nach Judikatur des BAG praktisch jede Form der automatischen Erhebung, Speicherung oder sonstige Verarbeitung von Daten von § 87 Abs 1 Nr 6 BetrVG erfasst, sobald sich daraus Rückschlüsse auf das Verhalten oder Leistung der Beschäftigten ergeben. Folglich besteht nur dann kein Mitbestimmungsrecht, wenn die vom Arbeitgeber erhobenen Arbeitnehmerdaten keinen Rückschluss auf das Verhalten oder die Leistung von Beschäftigten zulassen. Die Aussagen über Verhalten und Leistung müssen dabei einzelnen Beschäftigten zugeordnet werden können. Die Erfassung der Leistung oder des Verhaltens der Gesamtbelegschaft, ohne Zuordnungsmöglichkeit an einzelne Beschäftigte, reicht nach BAG Rechtsprechung nicht aus.[714]

Kommt zwischen Betriebsrat und Arbeitgeber keine Einigung zustande, entscheidet über den Inhalt und den Abschluss der Betriebsvereinbarung die Einigungsstelle (§ 87 Abs 2 Satz 1 iVm. § 76 BetrVG).[715]

4.1.4 Anhang ArbStättV Punkt 6.5. Abs 5 Anforderungen und Maßnahmen für Arbeitsstätten (EG-Bildschirmrichtlinie 90/270/EWG)

Die EG-Bildschirmrichtlinie 90/270/EWG regelt Mindestvorschriften in Bezug auf die Sicherheit und den Gesundheitsschutz bei der Arbeit an Bildschirmgeräten. Im Anhang Nr 3 lit. b Hs 2 EG-Bildschirmrichtlinie 90/270/EWG (Mensch-Maschine-Schnittstelle) wird zudem der Schutz der Persönlichkeit normiert: *„[O]hne Wissen des Arbeitnehmers darf keinerlei Vorrichtung zur quantitativen oder qualitativen Kontrolle verwendet werden.“*[716]

In Deutschland war Anhang Nr 3 lit. b Hs 2 EG Bildschirmrichtlinie 90/270/EWG bis Dezember 2016 im Anhang Anforderung Nr. 22 Bildschirmarbeitsverordnung (BGBl. 1996 I. 1841, 1843) umgesetzt, die Bestimmungen wurden im Dezember 2016 (BGBl. 2016 I. 2681, 2691) in den Anhang Punkt 6.5. der Arbeitsstättenverordnung (ArbStättV) verschoben. Anhang Punkt 6.5. Abs 5 ArbStättV lautet: *„Eine Kontrolle der Arbeit hinsichtlich der qualitativen oder quantitativen Ergebnisse darf ohne Wissen der Beschäftigten nicht durchgeführt werden.“* Demgemäß bedürfen Arbeitgeberkontrollen an Bildschirmarbeitsplätzen aus rein arbeitsrechtlicher Sicht hinsichtlich qualitativer oder quantitativer Ergebnisse immer der vorhergehenden Information der Beschäftigten.[717]

---

714 *Ricard/Maschmann* in Ricardi (Hrsg), Betriebsverfassungsgesetz[16] (2018) § 87 Rn 488; 508; 511.

715 *Selk* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 3. Rn 128 ff.

716 Nr 3 lit b Anhang EG Bildschirmrichtlinie 90/270/EWG.

717 Anhang Arbeitsstättenverordnung (ArbStättV) Punkt 6.5. Abs. 5.

Die grundsätzlich öffentlich-rechtlichen Pflichten des Arbeitgebers z.B. aus dem Arbeitsschutz (z.B. ArbStättV) werden privatrechtlich gleichzeitig als Konkretisierung der Fürsorgepflicht (§ 618 Abs 1 BGB) angesehen und können als unabdingbare (§ 619 BGB) privatrechtliche Pflichten in die arbeitsrechtliche Beziehung als Bestandteil des Arbeitsvertrages hineintransformiert werden. Der Arbeitnehmer kann die Erfüllung dieser ihm gegenüber bestehenden klagbaren Nebenpflichten des Arbeitgebers (z.B. Herstellung der gesetzlich vorgeschriebenen Arbeitsschutzeinrichtungen) gerichtlich geltend machen und kann unter Umständen bei bestehender Vergütungspflicht des Arbeitgebers seine Arbeitsleistung zurückbehalten, da dem Arbeitnehmer das Erbringen der Arbeitsleistung unter Bedingungen, die eine Missachtung arbeitsschutzrechtlicher Normen darstellen, in der Regel unzumutbar ist.[718]

Ob dies auch bei einem dauerhaften Verstoß gegen Anhang Punkt 6.5. Abs 5 ArbStättV ebenso in der Form zutrifft, ist mA weder in der Literatur noch in der Rechtsprechung final geklärt worden.

4.2 Österreich

4.2.1 Überblick

- Individualarbeitsrechtliche Vereinbarkeit gemäß § 16 ABGB, § 1157 ABGB, § 18 AngG (siehe **Kapitel 4.2.2**);
- Kollektives Arbeitsrecht gemäß § 91 Abs 2 iVm. § 96 Abs 1 Z 3, § 96a Abs 1 Z 1 ArbVG sowie § 10 AVRAG (siehe **Kapitel 4.2.3** und **Kapitel 4.2.4**);
- DSGVO und DSG Konformität von Verarbeitungen (siehe oben **Kapitel 3**).

4.2.2 Individualarbeitsrechtlicher Persönlichkeitsschutz (§ 16 ABGB)

Grundsätzlich ist die Kontrollunterworfenheit Bestandteil der persönlichen Abhängigkeit des Arbeitnehmers vom Arbeitgeber im Arbeitsverhältnis. Der Arbeitgeber ist einerseits aus dem Persönlichkeitsrecht des Arbeitnehmers (§ 16 ABGB) und andererseits aus der aus dem Arbeitsverhältnis resultierenden Fürsorgepflicht (§ 1157 ABGB, § 18 AngG) verpflichtet, die Privatsphäre des Arbeitnehmers zu wahren und zu schützen.[719] Angeboren im Sinne des § 16 ABGB ist jedem Menschen u.a. das Recht auf Wahrung der Geheimsphäre. Es schützt gegen das Eindringen in die Privatsphäre. Schutzgegenstand ist die Privatheit der Person. Totalüberwachung des Arbeitnehmers durch automatisierte Systeme ist Persönlichkeitsverletzung iSd. § 16 ABGB, weniger schwere Eingriffe *„berühren die Menschenwürde“* (vgl. § 96 Abs 1 Z 3 ArbVG).[720] Das Recht auf informationelle Selbstbestimmung wird in Österreich unter Verweis auf die deutsche Rechtsprechung als Persönlichkeitsrecht

718 *Weidenkaff* in Palandt (Hrsg), Bürgerliches Gesetzbuch[78] (2019) § 618 Rn 6 ff; *Zöllner/Loritz/Hergenröder*, Arbeitsrecht[7] (2015) 2. Teil § 32 Rn 5 ff; § 31 Rn 85 ff.

719 *Rebhahn,* Mitarbeiterkontrolle am Arbeitsplatz (2009) 15 f; 20 ff; *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.6 ff; *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 96 Rn 19 ff.

720 *Aicher* in *Rummel/Lukas* (Hrsg), ABGB[4] (Stand 1.7.2015, rdb.at) § 16 Rn 42 ff.

iSd § 16 ABGB anerkannt.[721] Der von § 16 ABGB anerkannte Persönlichkeitsschutz ist kein absolutes Recht wie bspw. Leben und Freiheit. Beim Recht auf Leben und Freiheit indiziert deren Kernbereichsverletzung bereits die Rechtswidrigkeit des Verhaltens, bei Eingriffen in das Persönlichkeitsrecht kann das Rechtswidrigkeitsurteil erst nach einer umfassenden Interessensabwägung gefunden werden.[722] § 16 ABGB dient hier als Transformationsstelle für primär an den Staat gerichtete Grund- und Menschenrechte in das Privatrecht. Auf diese Weise sind die Grundrechtspositionen mittelbar auch zwischen Privaten anzuwenden. Nur das Grundrecht auf Datenschutz gemäß § 1 DSG [2000] gilt aufgrund seiner unmittelbaren Drittwirkung auch zwischen Privaten, die aus § 1 DSG [2000] fließenden Wertungen werden bei der Auslegung im Rahmen des § 16 ABGB ebenso berücksichtigt. Die durch § 16 ABGB eingeräumten Persönlichkeitsrechte werden vom OGH als absolute Rechte anerkannt, sie genießen damit Schutz gegen Eingriffe Dritter. Jedes Verhalten eines Dritten, welches diese Rechte gefährdet, ist rechtswidrig. Die Festlegung des konkreten Schutzbereichs erfolgt über eine Interessensabwägung der divergierenden Rechtspositionen. Von den im Rahmen der Anwendung des § 16 ABGB zu beachtenden Grundrechtspositionen sind das auf Seiten des Beschäftigten: das Grundrecht auf Datenschutz (§ 1 DSG [2000] und Art 8 EU-GRC), das Recht auf Achtung des Privatlebens und der Korrespondenz und Kommunikation (Art 8 EMRK und Art 7 EU-GRC), das Brief- und Fernmeldegeheimnis (Art 10 und Art 10a StGG 1867), das Recht auf Unterrichtung und Anhörung der Arbeitnehmerinnen und Arbeitnehmer im Unternehmen (Art 27 EU-GRC), Recht auf gerechte und angemessene Arbeitsbedingungen (Art 31 EU-GRC).[723] Auf Seiten des Arbeitgebers sind folgende Grundrechtspositionen zu beachten und mit denen des Beschäftigten in Einklang zu bringen: Recht auf Eigentum (Art 5 StGG 1867 und Art 1 des 1. Zusatzprotokoll EMRK und Art 17 EU-GRC), Freiheit der Erwerbstätigkeit (Art 6 StGG 1867), Recht auf Berufsfreiheit (Art 15 EU-GRC), Recht auf unternehmerische Freiheit (Art 16 EU-GRC). Abzuwägen sind dann im Einzelfall über § 16 ABGB die jeweils berührten Persönlichkeitsinteressen und die Informations- und Kontrollinteressen des Arbeitgebers.[724]

Für Eingriffe in die durch § 16 ABGB gewährleisteten Persönlichkeitsrechte gilt:

- Eine Maßnahme muss einem sachlichen und legitimen Ziel (z.B. keine undifferenzierte Totalüberwachung) dienen, das heißt sie muss sachlich gerechtfertigt sein.
- Unter mehreren möglichen Möglichkeiten zur Zweckerreichung ist das schonendste Mittel zu wählen (Verhältnismäßigkeitsgrundsatz). Stellt die Maßnahme nicht das schonendste Mittel dar, ist sie rechtswidrig (keine Interessensabwägung mehr erforderlich). Unwirtschaftliche Maßnahmen müssen dabei nicht ergriffen werden. Dieses Ergebnis ergibt sich zugleich aus der Fürsorgepflicht (§ 1157 ABGB, § 18 AngG) des Arbeitgebers; zur Zweckerreichung ist das schonendste Mittel zur Achtung der Persönlichkeitsrechte der Beschäftigten auszuwählen.

721 *Egger* in *Schwimann/Neumayr* (Hrsg), ABGB-TaKomm[4] (2017) § 16 Rn 15; *Aicher* in *Rummel/Lukas* (Hrsg), ABGB[4] (Stand 1.7.2015, rdb.at) § 16 Rn 40 letzter Satz.

722 *Aicher* in *Rummel/Lukas* (Hrsg), ABGB[4] (Stand 1.7.2015, rdb.at) § 16 Rn 18.

723 *Rebhahn,* Mitarbeiterkontrolle am Arbeitsplatz (2009) 15.

724 *Aicher* in *Rummel/Lukas* (Hrsg), ABGB[4] (Stand 1.7.2015, rdb.at) § 16 Rn 42 ff; *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.6 ff.

- Liegt eine sachliche, legitime und verhältnismäßige Maßnahme vor, hat im letzten Schritt eine Interessensabwägung zwischen den legitimen Informations- und Kontrollinteressen des Arbeitgebers einerseits und dem angeborenen Persönlichkeitsschutz des Arbeitnehmers auf der anderen Seite zu erfolgen.[725]

Es bestehen letztlich erhebliche Schwierigkeiten die Grenzen rechtskonformer Arbeitgebermaßnahmen auszuloten. Eine Lösung kann immer nur im Einzelfall gefunden werden, denn die berechtigten Informations- und Kontrollinteressen des Arbeitgebers stehen immer in einem Spannungsverhältnis mit den Persönlichkeitsrechten der Arbeitnehmer.[726]

Die Prüfung nach der Vereinbarkeit mit dem Persönlichkeitsrecht gemäß § 16 ABGB bzw. der Fürsorgepflicht des Arbeitgebers nach § 1157 ABGB, § 18 AngG behält trotz DSGVO und DSG weiter seine volle Berechtigung. Anders als in Deutschland (vgl. § 26 Abs 7 BDSG) ist in Österreich das Datenschutzrecht nur anwendbar „*für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen*“ (Art 2 Abs 1 DSGVO). Erfolgt eine Maßnahme eines Arbeitgebers ohne automatisierte Verarbeitung von personenbezogenen Daten bzw. nichtautomatisierte Verarbeitung in einem Dateisystem, ist das Datenschutzrecht in Österreich nicht anwendbar (z.B. Spindkontrolle ohne jede Datenverarbeitung). Die Prüfung der Rechtmäßigkeit der Maßnahme erfolgt dann allein nach den § 16 ABGB bzw. § 1157 ABGB, § 18 AngG. Sind die DSGVO und das DSG anwendbar (Art 2 Abs 1 DSGVO), entfällt mA trotzdem nicht die Prüfung nach § 16 ABGB bzw. § 1157 ABGB, § 18 AngG, denn österreichisches Persönlichkeitsrecht und EU-Datenschutzrecht gelten mA parallel. Der OGH geht (in Entscheidungen zum Brief- und Bildnisschutz gemäß §§ 77, 78 UrhG iZh. mit der DSGVO[727]) auch weiter von einem Nebeneinander der Bestimmungen zu persönlichkeitsrechtlichen und datenschutzrechtlichen Aspekten aus und kommt zum klaren Ergebnis, „*dass der Gesetzgeber nicht von einer Derogation nationaler persönlichkeitsrechtlicher Schutzbestimmungen durch die DSGVO ausgeht*.“[728]

4.2.3 Betriebliche Mitwirkung und Mitbestimmung des Betriebsrats nach ArbVG

Das ArbVG stattet den Betriebsrat mit Informations-, Überwachungs-, Interventions- und Beratungsrechten sowie Mitbestimmungsrechten (§§ 89 ff ArbVG) aus. § 89 Abs 1 ArbVG gibt dem Betriebsrat das Recht, die Einhaltung der die Arbeitnehmer des Betriebes betreffenden Rechtsvorschriften zu überwachen. Dabei stehen dem Betriebsrat diverse Befugnisse gegenüber dem Betriebsinhaber (Arbeitgeber) zur Verfügung, die in den § 89 ff ArbVG konkretisiert werden.[729] In § 91 Abs 2 ArbVG wird klar normiert, dass der

725 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.6 ff; *Brodil*, ZAS 2009, 121 (122 ff.); *Brodil* in *Resch* (Hrsg), Die Kontrolle des Arbeitnehmers (2005) 74; G*oricnik*, wbl 2012, 301; *Rebhahn,* Mitarbeiterkontrolle am Arbeitsplatz (2009) 15 f; 20 ff.

726 *Brodil* in *Resch* (Hrsg), Die Kontrolle des Arbeitnehmers (2005) 72 ff.

727 OGH 29.08.2019, 6 Ob 152/19z; OGH 20.12.2018, 6 Ob 131/18k.

728 OGH 29.08.2019, 6 Ob 152/19z.

729 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 89 ArbVG Rn 12.

Betriebsinhaber dem Betriebsrat Mitteilung zu machen hat, welche Arten von personenbezogenen Arbeitnehmerdaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht. Dem Betriebsrat ist auf Verlangen die Überprüfung der Grundlagen für die Verarbeitung und Übermittlung zu ermöglichen. Dadurch wird es dem Betriebsrat effektiv möglich, die Rechtmäßigkeit der Beschäftigtendatenverarbeitung zu kontrollieren.[730] Die Überwachungspflicht des Betriebsrats nach § 91 Abs 2 ArbVG korrespondiert zum gleichzeitig mit BGBl. Nr. 394/1986 eingeführten Mitbestimmungsrecht nach § 96a Abs 1 Z 1 ArbVG hinsichtlich betrieblicher Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen.[731] Ist im Betrieb auch ein Datenschutzbeauftragter bestellt, haben dieser und der Betriebsrat die Aufgabe – aus ihrer jeweils unterschiedlichen Position – (vgl. Art 39 Abs 1 lit b DSGVO sowie §§ 89 Abs 1, 91 Abs 2 ArbVG) Datenschutzverstöße zu identifizieren, den Arbeitgeber auf die entdeckten mögliche (Datenschutz-)Rechtsverstöße hinzuweisen und zur Korrektur zu bewegen („Prinzip der doppelten Kontrolle“[732]).[733]

Gemäß § 96 Abs 1 Z 3 ArbVG wird eine notwendige fakultative Betriebsvereinbarung verlangt für die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren. „Notwendige“ Betriebsvereinbarung bedeutet, dass ohne Zustimmung des Betriebsrats der Betriebsinhaber die Maßnahme gar nicht treffen darf und „fakultative“ Betriebsvereinbarung bedeutet, dass die fehlende Zustimmung des Betriebsrats nicht durch die Schlichtungsstelle (§§ 144 ff ArbVG) ersetzt werden kann (= betriebliche Mitbestimmung ohne Rechtskontrolle und Zwangsschlichtung).[734] Unter „Kontrollmaßnahmen“ iSd. § 96 Abs 1 Z 3 ArbVG wird die systematische Überwachung von Eigenschaften, Handlungen oder das allgemeinen Verhalten durch Arbeitnehmer durch den Betriebsinhaber verstanden. Bei der Kontrollmaßnahme muss es sich um eine betriebsbezogene Kollektiv-Kontrolle und nicht bloß um eine individuelle Kontrolle handeln. Der Gesetzgeber führt im AB zu dieser Bestimmung erläuternd aus: *„Zustimmungspflichtig gemäß [§ 96] Abs. 1 Z. 3 sind nur auf Dauer angelegte Kontrollmaßnahmen. Ad-hoc-Kontrollen im Einzelfall (etwa bei Diebstahlsverdacht usw.) bedürfen, sofern sie überhaupt zulässig sind, nicht der Zustimmung des Betriebsrates.“*[735] Ist ein technisches System objektiv geeignet die Beschäftigten zu kontrollieren, auch wenn die Kontrollabsicht des Arbeitgebers fehlt, ist § 96 Abs 1 Z 3

730 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 91 ArbVG Rn 11 ff; *Drs* in Strasser/Jabornegg/Resch, ArbVG (Stand 1.9.2015, rdb.at) § 91 Rn 34 ff; *Knyrim,* Datenschutzrecht[3] (2015) 241 ff.

731 *Naderhirn* in Strasser/Jabornegg/Resch, ArbVG (Stand 1.12.2012, rdb.at) § 96a Rn 1; IA 205/A 16. GP 4 f; 21; AB 1062 BlgNR 16. GP 2.

732 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017), C. III. Rn 10 ff.

733 *Drs* in Strasser/Jabornegg/Resch (Hrsg), ArbVG (Stand 1.9.2015, rdb.at) § 91 Rn 37; *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 91 ArbVG Rn 12; *Knyrim,* Datenschutzrecht[3] (2015) 241 ff; *Art 29 Datenschutzgruppe*, WP 243 rev.01, Leitlinien in Bezug auf Datenschutzbeauftragte (2017) 20.

734 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 96 ArbVG Rn 6 ff; *Jabornegg in* Strasser/Jabornegg/Resch (Hrsg), ArbVG (Stand 1.12.2012, rdb.at) § 96 Rn 8 ff.

735 AB 993 BlgNR 14. GP 3.

ArbVG trotzdem umfassend einschlägig, wenn zusätzlich die Menschenwürde dadurch berührt wird. Erfasst sind bspw. Videokameras, Telefonregistrieranlagen, Lokalisierungsfunktionen von Mobiltelefonen durch Ortungssysteme wie GPS, Einblick in Bildschirminhalte sowie in die Aufzeichnung von Zugriffs- und Bewegungsdaten auf Computern, die Benutzung von Internet im Betrieb (Internet u. E-Mail), sowie mittels biometrischer Daten arbeitende Zutritt- und Zugriffskontrollsysteme, etc.[736] Bisher hatte sich der OGH mit einer Telefonregistrieranlage und einem Zeiterfassungssystem, welches auf biometrischem Fingerscanning beruhte, konkret zu befassen und in beiden Fällen eindeutig ein „Berühren der Menschenwürde" festgestellt.[737] Die „Menschenwürde" wird nach Ansicht des OGH von einer Kontrollmaßnahme oder einem Kontrollsystem des Arbeitgebers dann „berührt", wenn **[1.]** dadurch die vom Arbeitnehmer in den Betrieb miteingebrachte Privatsphäre kontrolliert wird (z.B. Kontrollen bei erlaubter IKT-Privatnutzung) oder **[2.]** wenn durch die hohe Kontrollintensität der Arbeitsleistung und des arbeitsbezogenen Verhaltens des Arbeitnehmers eine Berührung der Menschenwürde bewirkt wird. Dies ist der Fall bei Kontrollen mit übersteigerter Intensität, wo jenes Maß überschritten wird, das für Arbeitsverhältnisse dieser Art typisch und geboten ist. Es kommt also entweder auf die Intensität der Kontrolle an oder ob die miteingebrachte Privatsphäre (mit-)kontrolliert wird. Ausschlaggebend sind die Art der Kontrolle (durch Menschen oder durch Technik), die zeitliche Dauer (Stichproben oder permanente Kontrolle), der Umfang der Kontrolle (Verknüpfung verschiedener Daten) und die dabei erfassten Datenarten (Sensibilität). Der österreichische Gesetzgeber will mit der Anknüpfung an die „Menschenwürde" in § 96 Abs 1 Z 3 ArbVG erreichen, dass die freie Entfaltung der Persönlichkeit des Arbeitnehmers keinen übermäßigen Eingriffen ausgesetzt wird. Allein in der Erfassung der Arbeitszeit, an der dem Arbeitgeber ein durch den Arbeitsvertrag vorgegebenes Interesse zuzubilligen ist, kann nach OGH noch keine Beeinträchtigung der in den Betrieb eingebrachten Persönlichkeit des Arbeitnehmers erblickt werden. Die bloße Anwesenheitskontrolle ist daher bspw. nicht nach § 96 Abs 1 Z 3 ArbVG BR-zustimmungspflichtig, weil durch eine Zeitstempeleinrichtung oder Magnetkarte zur Arbeitszeitkontrolle (solange sie nicht ein arbeitnehmerbezogenes Bewegungsprofil während des ganzen Arbeitstages ermöglicht) die Menschenwürde noch nicht einmal berührt wird.[738] Eine Kontrollmaßnahme kann aber ohne Berührung der Menschenwürde aufgrund eines anderen Tatbestands im ArbVG trotzdem mitbestimmungspflichtig sein (z.B. § 96a Abs 1 Z 1 ArbVG – *siehe unten*).[739] Erfolgt die Arbeitszeitkontrolle über ein Zeiterfassungssystem, das auf biometrischem Fingerscanning beruht, trägt nach OGH bereits die Abnahme von Fingerabdrücken der Arbeitnehmer für sich gesehen eine so hohe Kontrollintensität in sich, womit es zu einer Berührung der Menschwürde und damit zur Anwendung des § 96 Abs 1 Z 3 ArbVG kommt. Denn durch den Einsatz der biometrischen Daten kommt es dem Arbeitgeber gerade darauf an, einen unmittelbaren Personenbezug herzustellen um gezielt Aufzeichnungen der Zutritte der einzelnen Arbeitnehmer vorzunehmen.[740]

736 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 96 ArbVG Rn 19 ff.
737 OGH 20.12.2006, 9 ObA 109/06d; OGH 13.06.2002, Ob A 288/01p.
738 OGH 20.12.2006, 9 ObA 109/06d.
739 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 96a ArbVG Rn 11 ff.
740 OGH 20.12.2006, 9 ObA 109/06d.

Gemäß § 96a Abs 1 Z 1 ArbVG wird eine notwendige erzwingbare Betriebsvereinbarung verlangt, für die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen. „Notwendige" Betriebsvereinbarung bedeutet, dass ohne Zustimmung des Betriebsrats die Maßnahmen nicht getroffen werden dürfen. „Erzwingbare" Betriebsvereinbarung bedeutet, dass der Betriebsinhaber aber – anders als bei § 96 Abs 1 Z 3 ArbVG – die Möglichkeit hat, die nicht erteilte Zustimmung des Betriebsrats durch die Schlichtungsstelle (§§ 144 ff ArbVG) zu ersetzen und insofern die Betriebsvereinbarung zu erzwingen (§ 96a Abs 2 ArbVG).[741] Unter die nichtmitbestimmungspflichtige „Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen" fallen Generalien wie Name und Adresse sowie die formelle berufliche Qualifikation (nicht die Leistungsfähigkeit). Eine über die Verarbeitung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehende personenbezogene Datenverarbeitung bleibt zudem mitbestimmungsfrei, wenn die Verarbeitung durch eine Verpflichtung aus einem Gesetz (z.B. Sozialrecht), einer Kollektivvereinbarung bzw. Betriebsvereinbarung erfolgt.[742]

Problematik und Lösung: Durch § 96 Abs 1 Z 3 ArbVG (notwendige fakultative Betriebsvereinbarung) hat der Betriebsrat in Österreich die Möglichkeit die Einführung von (neuen) technischen Systemen, die objektiv zur Kontrolle der Arbeitnehmer geeignet sind und dabei die Menschenwürde berühren (z.B. Internet, E-Mail, Enterprise Social Media; weil dabei jeweils – unabhängig von einer Kontrollabsicht eines Arbeitgebers – ein umfassendes in der Regel die Menschenwürde berührendes objektives Kontrollpotential enthalten ist), mit der Nichterteilung seiner Zustimmung, deren Einführung im Betrieb umfassend zu blockieren (Vetorecht). Dies veranlasste den OGH dazu, einerseits dieses Recht des Betriebsrats hinsichtlich solcher technischer Systeme umfassend zu bestätigen, aber andererseits zugleich einen Bogen zu § 96a Abs 1 Z 1 ArbVG (notwendige erzwingbare Betriebsvereinbarung) zu spannen. Der OGH führte im Fall der Telefonregistrieranlage aus*: „Die Einführung eines elektronischen Telefonkontrollsystems, das die Nummern der angerufenen Teilnehmer systematisch und vollständig den jeweiligen Nebenstellen zugeordnet erfasst, berührt daher selbst dann die Menschenwürde im Sinn des § 96 Abs 1 Z 3 ArbVG, wenn durch Betätigen einer Taste am Telefonapparat hinsichtlich der dann besonders gekennzeichneten Gespräche die Endziffern der Rufnummer im System unterdrückt werden. Allerdings würde es der dargestellten Interessenabwägung nicht gerecht, wollte man es mit diesem Rechtssatz dem Betriebsrat in die Hand geben, die Einführung derartiger Telefonsysteme generell zu verhindern und so dem Dienstgeber jede Möglichkeit zu nehmen, die missbräuchliche Verwendung seiner Telefonanlage zu bekämpfen. Es entspricht einer ausgewogenen Berücksichtigung der beiderseitigen Interessen und den Besonderheiten des technischen Mediums, für jede automationsunterstützt arbeitende Telefonregistrieranlage den Abschluss einer Betriebsvereinbarung zu verlangen, in welcher etwa einerseits verpflichtend der Umfang der Nutzung der Anlage ebenso festgelegt wird, wie eine Infor-*

741 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 96a ArbVG Rn 5 ff; *Naderhirn* in Strasser/Jabornegg/Resch (Hrsg), ArbVG (Stand 1.12.2012, rdb.at) § 96a Rn 3.

742 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 96a ArbVG Rn 11 ff.

mationspflicht des Dienstgebers über allfällige Änderungen und andererseits Schutzmaßnahmen zu Gunsten des Dienstnehmers vor willkürlicher übermäßiger Kontrolle vereinbart werden."[743] Der OGH sprach als konkrete Anforderungen für Arbeitgeber zur Anwendung des § 96a Abs 1 Z 1 iVm. Abs 2 ArbVG anstatt des § 96 Abs 1 Z 3 ArbVG aus:

- verbindliche Festlegung des konkreten Umfangs der Nutzung (Kontrollmaßnahme),
- Informationspflicht des Arbeitgebers über Änderungen der Kontrollmaßnahme,
- Schutzmaßnahmen zu Gunsten der Beschäftigten vor willkürlicher übermäßiger Kontrolle durch:
  - Einschau und Kontrolle nur im Verdachtsfall (auffällige Kostenbelastung, etc.);
  - Einbeziehung des Betriebsrats bei Einschau;
  - im Falle des Weiterbestehens der Verdachtsmomente, diese nach Information des Betriebsrates mit dem Beschäftigten erörtern;
  - ergibt sich daraus aber keine Klärung und Entkräftung der Vorwürfe, dürfen erst weitere Aufklärungsmaßnahmen eingeleitet werden.[744]

Bietet ein Arbeitgeber eine Betriebsvereinbarung mit solchen inhaltlichen „Garantien" iSd. der OGH Rechtsprechung an, kann der Arbeitgeber bei Nichtzustimmung des Betriebsrats die Schlichtungsstelle gemäß § 96a Abs 2 ArbVG anrufen, weil durch die Maßnahmen die grundsätzlich bestehende Eingriffsintensität soweit herabgesetzt wird („Wandlungsthese"), dass die Menschenwürde davon nicht mehr berührt wird. § 96a Abs 1 Z 1 bzw. Abs 2 ArbVG ist insofern in diesen Fällen subsidiär zu § 96 Abs 1 Z 3 ArbVG anwendbar, weil die Datenverarbeitung (z.B. Telefonanlage, Internet, etc.) weiter über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen einerseits weit hinausgeht und diese Datenverarbeitung nicht gesetzlich oder durch einen Kollektivvertrag, etc. vorgeschrieben ist.[745] Mit Hilfe der „Wandlungsthese" erfolgte eine Annäherung an die deutsche Rechtslage, wo eine nicht nach § 87 Abs 1 Nr 6 BetrVG erteilte BR-Zustimmung zu technischen Überwachungseinrichtungen, gemäß § 87 Abs 2 BetrVG immer durch den Spruch der Einigungsstelle (§ 76 BetrVG) ersetzt werden kann.[746]

§ 97 Abs 1 Z 6 ArbVG enthält eine Regelung zur betrieblichen Mitbestimmung bei Maßnahmen zur zweckentsprechenden Benutzung von Betriebseinrichtungen und Betriebsmitteln. Es handelt sich dabei um eine erzwingbare Betriebsvereinbarung, weil die betreffenden Maßnahmen dürfen auch ohne Zustimmung des Betriebsrates eingeführt werden. Der Abschluss einer dbzgl. Betriebsvereinbarung wird als zulässig erklärt und im Falle einer Nichteinigung über eine Betriebsvereinbarung können sowohl der Betriebsinhaber als auch

743 OGH 13.06.2002, Ob A 288/01p.

744 OGH 13.06.2002, Ob A 288/01p; *Feiler/Horn*, Umsetzung der DSGVO in der Praxis (2017) 157 f; *Risak*, Betriebliche Mitbestimmung bei der Mitarbeiterkontrolle in Brodil (Hrsg), Datenschutz im Arbeitsrecht Mitarbeiterüberwachung versus Qualitätskontrolle. Wiener Oktobergespräche 2009 (2010) 35 ff (49 f.).

745 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 96a ArbVG Rn 11 ff; *Risak*, Betriebliche Mitbestimmung bei der Mitarbeiterkontrolle in Brodil (Hrsg), Datenschutz im Arbeitsrecht Mitarbeiterüberwachung versus Qualitätskontrolle. Wiener Oktobergespräche 2009 (2010) 35 ff (49 f.); *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.168 ff.

746 *Selk* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil V. Kapitel 3. Rn 128 ff.

der Betriebsrat die Schlichtungsstelle anrufen um die Betriebsvereinbarung zu erzwingen. Darunter fallen bspw. Regelungen zu Telefonanlagen sowie der Nutzung des betrieblichen Internetzugangs, etc.[747]

4.2.4 § 10 AVRAG (EG-Bildschirmrichtlinie 90/270/EWG)

Die österreichische Umsetzung des Anhang Nr 3 lit. b Hs 2 EG-Bildschirmrichtlinie 90/270/EWG (*„[O]hne Wissen des Arbeitnehmers darf keinerlei Vorrichtung zur quantitativen oder qualitativen Kontrolle verwendet werden.“*[748]) erfolgte durch BGBl. Nr. 450/1994 in § 10 AVRAG in der Form, dass der Beschäftige nicht nur zu informieren ist, sondern auch selbst dazu zustimmen muss. § 10 AVRAG orientiert sich an § 96 Abs 1 Z 3 ArbVG hinsichtlich die Menschenwürde berührenden Kontrollmaßnahmen und technischen Einrichtungen von Seiten des Arbeitgebers. Sie gilt immer dann, wenn in einem Betrieb Kontrollmaßnahmen bzw. dbzgl. technischen Einrichtungen mit objektivem Kontrollpotential vom Arbeitgeber eingesetzt werden und kein Betriebsrat für den betroffenen Betrieb existiert bzw. eingerichtet wurde. § 10 AVRAG ermöglicht somit nicht die Substituierung der nach § 96 Abs 1 Z 3 ArbVG erforderlichen Betriebsvereinbarung bei einem eingerichtetem Betriebsrat. Die Einführung von Kontrollmaßnahmen oder technischer Einrichtungen, welche die Menschenwürde berühren, bei Betrieben ohne Betriebsrat ist ohne die Zustimmung der betroffenen Arbeitnehmer gemäß § 10 Abs 1 AVRAG absolut unzulässig. Eine erteilte Zustimmung kann vom Beschäftigten jederzeit widerrufen werden, außer es wurde gemäß § 10 Abs 2 AVRAG schriftlich festgelegt, wie lange die Zustimmung zur Kontrollmaßnahme konkret erteilt wird (Befristung), dann gilt die Zustimmung entsprechend der vereinbarten Frist als erteilt.[749]

Zugleich wurde in der ErläutRV definiert, was der österreichische Gesetzgeber am Bildschirmarbeitsplatz unter eine „die Menschenwürde berührende Kontrollmaßnahme“ versteht: *„Jede verdeckte Kontrollmaßnahme, insbesondere solche zur qualitativen oder quantitativen Kontrolle der Arbeitsleistung an Bildschirmgeräten, ist als Maßnahme anzusehen, die die Menschenwürde berührt und die der Zustimmung entweder durch Abschluß einer Betriebsvereinbarung oder des einzelnen Arbeitnehmers bedarf.“*[750]§ 10 AVRAG kommt – wie § 96 Abs 1 Z 3 ArbVG – nur zur Anwendung bei planmäßigen Kontrollen mit generalisierendem Muster und nicht bei rein singulären ad-hoc Kontrollen in Einzelfällen (z.B. Betrugsverdacht gegen einen einzelnen Beschäftigten, etc.).[751]

Wird § 10 AVRAG verletzt, hat in Betrieben ohne Betriebsrat jeder Arbeitnehmer das Recht auf einen Unterlassungs- und Beseitigungsanspruch und ggf. das Recht auf Schadenersatz gemäß §§ 16 iVm. 1328a ABGB u.a. wegen rechtswidriger und schuldhafter Verletzung

747 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm^3 (Stand 1.1.2018, rdb.at) § 97 ArbVG Rn 5 ff; *Burger-Ehrnhofer;Drs;Eichinger;Födermayr;Jabornegg; Mayr;Reiner* in Jabornegg/Resch (Hrsg), ArbVG (Stand 1.3.2016, rdb.at) § 97 Rn 210 ff (Rn 212).

748 Nr 3 lit b Anhang EG Bildschirmrichtlinie 90/270/EWG.

749 ErläutRV 1590 BlgNR 28. GP 128; *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm^3 (Stand 1.1.2018, rdb.at) § 10 AVRAG Rn 1 ff.

750 ErläutRV 1590 BlgNR 28. GP 128.

751 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm^3 (Stand 1.1.2018, rdb.at) § 10 AVRAG Rn 11 ff.

der Privatsphäre.[752] Nach *Rebhahn* sollte ein Beschäftigter das Recht haben, bei Fehlen der erforderlichen Zustimmung die Arbeit zu verweigern.[753]

Bei erlaubter Privatnutzung der IT und der damit verbundenen Verarbeitung von besonderen Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO) im Rahmen der stufenweisen Kontrollverdichtung[754] der IT bietet sich eine sinnvolle Möglichkeit, die erforderliche ausdrückliche informierte Einwilligung nach Art 9 Abs 2 lit a DSGVO und zugleich die Zustimmung nach § 10 AVRAG einzuholen (siehe bereits **Kapitel 3.5.4**):

- Es wird allgemein die Privatnutzung im Unternehmen verboten.
- Es wird nur mehr Beschäftigten die Privatnutzung anschließend wieder erlaubt, die der Überwachung des Internetverkehrs in Art und Weise der stufenweisen Kontrollverdichtung ausdrücklich ihre informierte und freiwillige[755] Einwilligung erteilen (Art 9 Abs 2 lit a DSGVO) und zudem der Kontrollmaßnahme nach § 10 AVRAG zustimmen. So ist in Betrieben ohne Betriebsrat mit erlaubter Privatnutzung der IT das Modell der stufenweisen Kontrollverdichtung rechtskonform umsetzbar.[756]

Nach *Brodil* wird aber § 10 AVRAG seit 25. Mai 2018 von der DSGVO umfassend verdrängt, da die Zustimmung nach § 10 ARVRAG nunmehr überflüssig sei (Anwendungsvorrang DSGVO) und auch § 10 Abs 2 AVRAG mit der Möglichkeit der befristeten unwiderruflichen Zustimmung den strengen Anforderung der DSGVO mit der jederzeitigen Widerrufbarkeit von Einwilligungen widerspreche.[757]

Es sprechen mA gute Gründe im Sinne *Brodils* aber auch andere Gründe dagegen:

Dafür, dass § 10 AVRAG nicht mehr anwendbar ist, spricht, dass § 10 AVRAG den freien Datenverkehr behindert, da eine DSGVO-konforme Verarbeitung wegen § 10 AVRAG trotzdem einzustellen wäre. Sie müsste demzufolge hinter den Anwendungsvorrang der DSGVO zurücktreten.[758] § 10 AVRAG ist zudem eine überschießende Umsetzung des Unionsrechts („gold plating"), da die europäische Norm nur die Information („*ohne Wissen*") der Beschäftigten verlangt aber keine Zustimmung wie § 10 AVRAG. Die Thematik der Informationspflichten wurde zudem 5 Jahre nach Verabschiedung der EG-Bildschirmrichtlinie 90/270/EWG durch Art 11 EG-Datenschutzrichtlinie 95/46/EG und seit 25. Mai 2018 noch umfassender durch Art 14 DSGVO geregelt. Somit wäre ggf. bereits auf europäischer Ebene die spezielle Informationspflicht nach EG-Bildschirmrichtlinie 90/270/EWG durch die viel detaillierteren Regelungen gemäß Art 14 DSGVO verdrängt.[759]

---

752 *Goricnik/Grünanger* in *Grünanger/Goricnik* (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.279 ff.

753 *Rebhahn,* Mitarbeiterkontrolle am Arbeitsplatz (2009) 23 f.

754 *Kotschy/Reimer*, ZAS 2004, 29.

755 BT-Drs 18/11325, 97. (Freiwilligkeit der Einwilligung in IT-Privatnutzung – wirtschaftlicher Vorteil).

756 *Feiler/Horn,* Umsetzung der DSGVO in der Praxis (2018) 131 ff.

757 *Brodil,* Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 11.

758 EuGH, Rs. 6/64, Slg. 1964, S. 1251, 1269 – Costa/ENEL; Art 2 Abs 1 Datenschutz-Grundverordnung (EU) 2016/679.

759 Anhang Nr 3 lit. b Hs 2 EG-Bildschirmrichtlinie 90/270/EWG; ErläutRV 1590 BlgNR 28. GP 128.

Auf der anderen Seite handelt es sich bei § 10 AVRAG um keine datenschutzrechtliche Norm iSd. Art 16 AEUV, sondern um eine rein arbeitsrechtliche Norm mit einer anderen unionsrechtlichen Grundlage (Art 153 Abs 1 lit b oder lit f, Art 154 AEUV; EG-Bildschirmrichtlinie 90/270/EWG). Eine absolut DSGVO-konforme Verarbeitung kann weiterhin wegen anderer entgegenstehender rechtlicher Anforderungen – z.B. Arbeitsrecht – nicht durchführbar und damit nicht erlaubt sein.[760] § 10 AVRAG ist insofern eine rein arbeitsrechtliche Norm für Betriebe ohne Betriebsrat und keine datenschutzrechtliche Norm. Auch die österreichische Datenschutzbehörde trennte bisher bereits klar zwischen Zustimmungen nach § 4 Z 14 DSG 2000 aF und Zustimmungen nach § 10 AVRAG, was ebenso für eine zukünftig weitere parallele Anwendbarkeit von Art 4 Nr 11 DSGVO und § 10 AVRAG sprechen könnte.[761]

Aufgrund der engen Verzahnung zwischen § 10 AVRAG und § 96 Abs 1 Z 3 ArbVG bleibt mA § 10 AVRAG als rein arbeitsrechtliche Norm[762] anwendbar (Art 153 Abs 1 lit b u. lit f, Art 154 AEUV; EG-Bildschirmrichtlinie 90/270/EWG) und wird trotz „gold plating" des damaligen österreichischen Gesetzgebers in BGBl. Nr. 450/1994 (statt einer Informationspflicht wird eine Zustimmung in § 10 AVRAG verlangt) von der DSGVO nicht verdrängt, denn eine betriebliche vollständig DSGVO-konforme Datenverarbeitung kann weiterhin aus arbeitsrechtlichen Gründen unzulässig sein.[763]

760 *Art 29 Datenschutzgruppe*, WP 203 (2013) 12; 19 ff; *Feiler/Forgó,* EU-DSGVO (2017) Art 5 Rn 6.

761 DSK Bescheid v. 13.05.2014 DSB-D600.328-001/0001-DSB/2014; DSK Bescheid v. 26.06.2013 K506.250-005/0002-DVR/2013; DSK Bescheid v. 30.04.2013 K600.322-005/0003-DVR/2013.

762 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm^3 (Stand 1.1.2018, rdb.at) § 10 AVRAG Rn 5.

763 *Art 29 Datenschutzgruppe*, WP 203 (2013) 12; 19 ff; *Feiler/Forgó,* EU-DSGVO (2017) Art 5 Rn 6.

5 Neue Technologien für den IT-gestützten Arbeitsplatz

5.1 Vom Laptop und Smartphone zum Digitalen Assistenten

Bereits Anfang der 2000er Jahre wurden in den USA (militärische) informationstechnische Entwicklungen im Zusammenhang mit dem Themenbereich Cognitive Computing und Digitalen Assistenten eingeleitet, die heute unter tlw. Rückgriff auf diese militärischen Entwicklungen zur Etablierung von Digitalen Assistenten sowohl im Konsumentenbereich als auch im Arbeitsbereich führen.[764] Im Jahr 2000 trat die DARPA (Defense Advanced Research Projects Agency) an das Standford Research Institute (SRI) mit der Idee heran, die Art und Weise wie Computer Menschen unterstützen durch kognitive Systeme zu verbessern. Es handelt sich dabei um IT-Systeme, die aus Erfahrungen lernen, Schlüsse ziehen und so eine virtuelle effektive persönliche Assistenz ermöglichen können. Aus diesen Überlegungen resultierte schließlich das sogenannte PAL-Projekt (**P**ersonalized **A**ssistant that **L**earns).[765] Das von der DARPA in Auftrage gegebene PAL-Projekt hatte eine Projektdauer von 5 Jahren (2003 – 2008). Es waren in dieser Zeit über 20 US-Universitäten[766] eingebunden und ca. 300 – 500 Forscher auf dem Gebiet der künstlichen Intelligenz arbeiteten an der Grundlagenforschung zu kognitiven virtuellen persönlichen Assistenzsystemen. Einer der Lead Researchers, *David Isreal*, erklärte dazu: *"by any measure, the largest AI*[767] *program in history."*[768] Das PAL-Projekt (u.a. Digitaler Assistent mit Sprachsteuerung) wird in einem DARPA-Werbevideo von Mitte der 2000er Jahre wie folgt beschrieben: *„The mission: Radically improve computer support to Commanders and Staff. Enable cognitive systems that learn from experience, learn by instruction, learn to organize information, learn from interaction between people, learn to retrieve information – Personalized – Cognitive Assistance – Machine Learning On The Job – Adapts To Changing Conditions – Better,*

764 *Mazzucato*, Das Kapital des Staates – Eine andere Geschichte von Innovation und Wachstum (2014) 136 ff; *DARPA*, Personal Assistant That Learns (PAL), abrufbar unter: https://www.darpa.mil/about-us/timeline/personalized-assistant-that-learns (zuletzt abgerufen am 20.06.2019); *Kubiv* in macwelt.de (06.11.2012), Siri: 40 Jahre Forschung für intelligenten Sprachassistenten, abrufbar unter: https://www.macwelt.de/news/Siri-als-intelligenter-Sprachassistent-40-Jahre-Forschung-7022972.html (zuletzt abgerufen am 20.06.2019).

765 *Ackerman* in wired.com (10.05.2011), The iPhone 4S' Talking Assistant Is a Military Veteran, abrufbar unter: https://www.wired.com/2011/10/siri-darpa-iphone/ (zuletzt abgerufen am 20.06.2019); *Safire* in nytimes.com (05.06.2003), Dear Darpa Diary, abrufbar unter: http://www.nytimes.com/2003/06/05/opinion/dear-darpa-diary.html (zuletzt abgerufen am 20.06.2019); PAL: personalized assistant that learns, abrufbar unter: http://www.web3.lu/pal-personalized-assistant-that-learns/ (zuletzt abgerufen am 20.06.2019).

766 Homepage des CALO-Projekts: http://www.ai.sri.com/project/CALO (zuletzt abgerufen am 20.06.2019).

767 AI – Artificial Intelligence.

768 *Bosker* in huffingtonpost.com (24.01.2013), SIRI RISING: The Inside Story Of Siri's Origins — And Why She Could Overshadow The iPhone, abrufbar unter: http://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone_n_2499165.html (zuletzt abgerufen am 20.06.2019).

C. Jaksch, *Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes*,
AutoUni – Schriftenreihe 143, https://doi.org/10.1007/978-3-658-29450-2_5

Faster Decisions – Fewer People"[769] Eine Teilkomponente des PAL-Projekts hatte den Namen CALO (**C**ognitive **A**ssistent that **L**earns and **O**rganizes). Das Wort selbst stammt aus dem Lateinischen („calonist") und bedeutet „Diener" (des Soldaten). DARPA hatte im Rahmen dieser Teilprojektkomponente das Standford Research Institute (SRI) beauftragt, einen virtuellen persönlichen Assistenten für die im Büro IT-gestützt arbeitenden US-Militärangehörigen zu entwickeln. Die CALO-Projektkomponente erwies sich nach Analyse von *Bosker* in der Huffington Post (Huffpost) aus heutiger Perspektive als wissenschaftlicher Triumph, denn es konnten zum ersten Mal verschiedene Disziplinen der künstlichen Intelligenz (KI) zusammengeführt werden.[770] Die Fähigkeiten des militärischen CALO-Assistenten werden (Stand 2013) wie folgt beschrieben: *„CALO was capable of performing an impressive variety of tasks that once seemed exclusive to human assistants. Say your colleague canceled shortly before a meeting. CALO, knowledgeable about each person's role on a project, could discern whether to cancel the meeting, and if needed, reschedule, issue new invitations and pin down a conference room. If the meeting went ahead as planned, CALO could assemble (and rank) all the documents and emails you'd need to be up to speed on the topic at hand. The assistant would listen in on the meeting, and, afterward, deliver a typed transcript of who said what and outline any specific tasks laid out during the conversation. CALO was also able to help put together presentations, organize files into folders, sort incoming messages and automate expense reports, among a host of other tasks."*[771] Das Ziel der Projektkomponente CALO war es für Angehörige der US Armee ihre zeitraubenden Alltagsaktivitäten (bspw. das Ansetzen von Meetings, das Priorisieren und Lesen bzw. analysieren von E-Mails, etc.) weitgehend über einen autonom agierenden virtuellen Assistenten zu optimieren.[772] Gemäß einem Bericht auf der Website *www.army.mil* wurden Teile des PAL-Projekts u.a. in das *US Army Command Post of the Future System* integriert und ab dem Jahr 2010 operativ im Irak eingesetzt.[773] In einer

769 DARPA Werbevideo zum PAL Project 2003 – 2008: https://www.youtube.com/watch?v=BF-KNFlOocQ (zuletzt abgerufen am 20.06.2019).

770 *Bosker* in huffingtonpost.com (24.01.2013), SIRI RISING: The Inside Story Of Siri's Origins — And Why She Could Overshadow The iPhone, abrufbar unter: http://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone_n_2499165.html (zuletzt abgerufen am 20.06.2019); PAL: personalized assistant that learns, abrufbar unter: http://www.web3.lu/pal-personalized-assistant-that-learns/ (zuletzt abgerufen am 20.06.2019); *Kubiv* in macwelt.de (06.11.2012), Siri: 40 Jahre Forschung für intelligenten Sprachassistenten, abrufbar unter: https://www.macwelt.de/news/Siri-als-intelligenter-Sprachassistent-40-Jahre-Forschung-7022972.html (zuletzt abgerufen am 20.06.2019); *Roush* in xconomy.com (14.06.2010), The Story of Siri, from Birth at SRI to Acquisition by Apple—Virtual Personal Assistants Go Mobile, abrufbar unter: http://www.xconomy.com/san-francisco/2010/06/14/the-story-of-siri-from-birth-at-sri-to-acquisition-by-apple-virtual-personal-assistants-go-mobile/ (zuletzt abgerufen am 20.06.2019).

771 *Bosker* in huffingtonpost.com (24.01.2013), SIRI RISING: The Inside Story Of Siri's Origins — And Why She Could Overshadow The iPhone, abrufbar unter: http://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone_n_2499165.html (zuletzt abgerufen am 20.06.2019).

772 *Stevens* in engadget.com (30.07.2009), DARPA's CALO project, the militaristic Clippy, set to invade iPhones this year, abrufbar unter: https://www.engadget.com/2009/07/30/darpas-calo-project-the-militaristic-clippy-set-to-invade-iph/ (zuletzt abgerufen am 20.06.2019).

773 *Ililau,* army.mil (18.09.2010),'Big Red One' debuts new communication system, abrufbar unter: https://www.army.mil/article/45376/ (zuletzt abgerufen am 20.06.2019).

Präsentation zum PAL-Project auf der Homepage des *Standford Reseach Insitute* SRI selbst, wird erläutert: "*PAL technologies have been deployed within the U.S. Army's Command Post of the Future (CPOF), and the U.S. Air Force Research Laboratory's (AFRL) Web Enabled Temporal Analysis System (WebTAS). In addition, PAL technologies are being evaluated in United States Strategic Command's (USSTRATCOM) Strategic Knowledge Integration Web (SKIWeb) and Integrated Strategic Planning and Analysis Network Global Adaptive Planning Collaborative Information Environment (ISPAN GAP CIE), and the U.S. Navy Marine Corps Intranet (NMCI).*"[774] Die von SRI entwickelten militärischen Anwendungen aus der CALO-Projektkomponente haben seit Ende 2000er Jahre auch zahlreiche zivile „Spin outs".[775] Das berühmteste CALO „Spin out" des Standford Research Institute ist dabei Apples SIRI (Speech Interpretation and Recognition Interface). Als im Jahr 2007 das erste iPhone von Steve Jobs vorgestellt wurde, erkannten Mitarbeiter des Standford Research Institute (SRI) auch die kommerzielle Chance auf einen profitablen Erfolg, nämlich aus der bisherigen rein militärischen CALO-Projektkomponente eine zivile Smartphone Anwendung zu machen. Die in der CALO- Projektkomponente u.a. entwickelte Technologie eines virtuellen Sprachassistenten wurde in diesem Fall über das „Start-up" Unternehmen SIRI Inc. für den zivilen Bereich kommerzialisiert. Der virtuelle Assistent SIRI sollte vom Fokus – im Unterschied zum militärischen CALO-Projekt – mehr den Blickwinkel der Konsumenten haben, also den Nutzern dabei helfen Produkt und Reviews zu finden bzw. selbst vorzuschlagen und Reservierungen autonom für die Nutzer vorzunehmen. Im April 2010 wurde das „Start Up" SIRI Inc. von der Apple Inc. mit allen Rechten an den Produkten um ca. 200 – 250 Millionen US Dollar gekauft. Zu dieser Zeit war das zivile SIRI bereits mit 42 verschiedenen Web Services – u.a. Yelp, StubHub, Rotten Tomatoes und Wolfram Alpha – verbunden und konnte mit einer einzigen Antwort die relevantesten und wichtigsten Details von den diversen Ressourcen beauskunften bzw. vorschlagen. Apple reduzierte die verbundenen Webservices und damit die eigentlichen bereits existierenden umfangreichen Fähigkeiten des ursprünglichen SIRI Assistenten stark, gleichzeitig wurden SIRI neben der englischen Sprache auch andere Sprachen beigebracht. Mit dem persönlichen virtuellen Assistenten SIRI wurde letztlich ein neues Kapitel der Interaktion von Mensch und Maschine im kommerziellen Bereich aufgeschlagen.[776] SIRI

774 *sri.com,* Presentation PAL Technologies for the Military, abrufbar unter: https://www.sri.com/sites/default/files/brochures/sri_palmilitary.pdf (zuletzt abgerufen am 20.06.2019).

775 *Mazzucato*, Das Kapital des Staates – Eine andere Geschichte von Innovation und Wachstum (2014) 136 ff; PAL: personalized assistant that learns, abrufbar unter: http://www.web3.lu/pal-personalized-assistant-that-learns/ (zuletzt abgerufen am 20.06.2019).

776 *Mazzucato*, Das Kapital des Staates – Eine andere Geschichte von Innovation und Wachstum (2014) 136 ff; *Trillo* in giga.de (23.01.2013), Siri: Ein Militär-Projekt, das fast bei Android gelandet wäre, abrufbar unter: https://www.giga.de/apps/siri/news/siri-ein-militar-projekt-das-fast-bei-android-gelandet-ware/ (zuletzt abgerufen am 20.06.2019); *Lardinois* in readwrite.com (13.10.2008), Semantic Stealth Startup Siri Raises $8.5 Million, abrufbar unter: http://readwrite.com/2008/10/13/semantic_stealth_startup_siric/ (zuletzt abgerufen am 20.06.2019); *Wortham* in NewYorkTimes (29.04.2010), Apple Buys a Start-Up for Its Voice Technology, abrufbar unter: http://www.nytimes.com/2010/04/29/technology/29apple.html (zuletzt abgerufen am 20.06.2019); *Bosker* in huffingtonpost.com (24.01.2013), SIRI RISING: The Inside Story Of Siri's Origins — And Why She Could Overshadow The iPhone, abrufbar unter: http://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone_n_2499165.html (zuletzt abgerufen am 20.06.2019); *Schonfeld* in techcrunch.com (28.04.2010), Silicon Valley Buzz: Apple Paid

übermittelt dabei die am Endgerät erhobenen die Sprachdaten und Sprachbefehle an einen Apple-Server, der diese in der Apple-Cloud verarbeitet und über längere Zeit speichert und anschließend die Ergebnisse wieder an das Endgerät (iPhone, iPad, Apple Smart-TVs und Wearables) zurücksendet. SIRI benötigt dazu zwingend eine Internetverbindung.[777]

Digitale Assistenten stellen das bisherige Verhältnis des Menschen zu seiner IT auf den Kopf. Bei einem normalen Computer bzw. auch Smartphone ist es der Benutzer, der steuert und entscheidet, und das Gerät, welches ausführt. Ein digitaler Assistent verknüpft selbsttätig Informationen, die ihr Anwender aktiv bereitstellt, mit Kontextwissen, das der digitale Assistent selbst erhebt, sowie mit „Weltwissen" und Big-Data-Auswertungen aus ganz anderen Quellen. Aufgrund dieser Informationsbasis treffen digitale Assistenten Entscheidungen für den Benutzer, agieren für ihn und lenken ihn ein Stück weit. Assistenten „leben" dabei zu einem Großteil in der Cloud ihrer Betreiber. Für den Benutzer sind sie oft wie Blackboxen, in die sie nicht „hineinsehen" können. Der Benutzer kann regelmäßig nicht nachvollziehen wie ein Suchergebnis oder eine autonome Entscheidung eines digitalen Assistenten zustande gekommen ist und auf Grund welcher Daten. Ein digitaler Assistent führt dazu, dass noch einmal viel mehr Informationen über ihre Benutzer zusammengetragen werden.[778]

Im Jahr 2021 wird es gemäß der Studie *Ovum* wahrscheinlich bereits mehr installierte Digitale Assistenten geben als menschliche Weltbevölkerung.[779]

More Than $200 Million For Siri To Get Into Mobile Search, abrufbar unter: https://techcrunch.com/2010/04/28/apple-siri-200-million/ (zuletzt abgerufen am 20.06.2019); *Roush* in xconomy.com (14.06.2010), The Story of Siri, from Birth at SRI to Acquisition by Apple—Virtual Personal Assistants Go Mobile, abrufbar unter: http://www.xconomy.com/san-francisco/2010/06/14/the-story-of-siri-from-birth-at-sri-to-acquisition-by-apple-virtual-personal-assistants-go-mobile/ (zuletzt abgerufen am 20.06.2019).

777 *golem.de*, SIRI, https://www.golem.de/specials/siri/ (zuletzt abgerufen am 20.06.2019).

778 *Bager* in c't – Magazin für Computertechnik, Gelenkte Menschen, 16/2015, abrufbar unter: https://www.heise.de/ct/ausgabe/2015-16-Digitale-Assistenten-und-ihre-Anwender-Wer-steuert-wen-2734536.html (zuletzt abgerufen am 20.06.2019).

779 *Studie Ovum*, Virtual digital assistants to overtake world population by 2021, abrufbar unter: https://ovum.informa.com/resources/product-content/virtual-digital-assistants-to-overtake-world-population-by-2021 (zuletzt abgerufen am 20.06.2019).

5.2 Der IT-gestützte Arbeitsplatz mit Digitalen Assistenten

5.2.1 Digitaler Assistent

Für den IT-gestützten Arbeitsplatz ist abzugrenzen zwischen Digitalen Assistenten und reinen Enterprise-Software-(Chat-)Bots, s. Abb. 3.

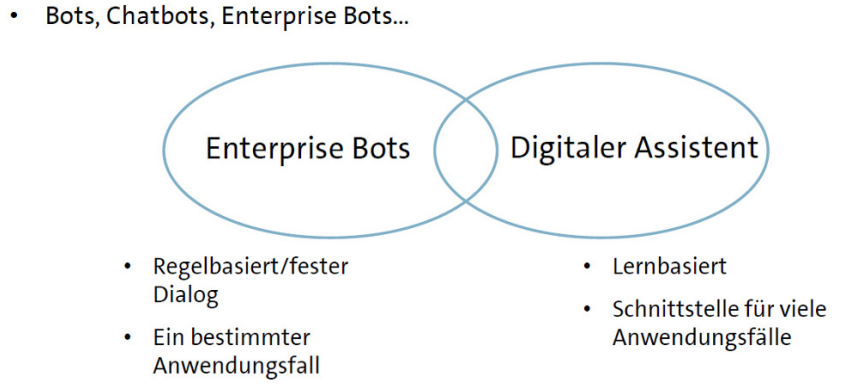


Abbildung 3: *Meier/Klein*, Die Zukunft der Büroarbeit bei Volkswagen – Der digitale Assistent, Vortrag Volkswagen AG (2017).

Die Anwendungsfälle von (insofern echten) Digitalen Assistenten in einem Unternehmen sind zahllos:

- Informationssuche und proaktive Informationsbereitstellung;
- automatisierte Terminplanung,
- Dienstreisebuchungen,
- Kommunikation mit Personen,
- Enterprise Helpdesk EHD Funktionalitäten
- Sprach- und Textschnittstelle,
- Mehrsprachenunterstützung,
- etc.

Ein Digitaler Assistent erledigt Standardaufgaben automatisiert und unterstützt bei komplexer Wissensarbeit in Form von proaktiver Informationsaufbereitung und der Abgabe von Empfehlungen. Dabei lernt der Digitale Assistent von den Entscheidungen des Mitarbeiters, seinem Verhalten und aus seiner Kommunikation. Einen digitalen Assistenten kann man definieren als ein Werkzeug, dass dem Nutzer in natürlicher Sprache die Interaktion mit verschiedenen Systemen und Prozessen erlaubt sowie aus den Gewohnheiten des Nutzers lernt und ihn durch Vorschläge unterstützt.“[780]

780 *Meier/Klein,* Die Zukunft der Büroarbeit bei Volkswagen – Der digitale Assistent, Vortrag Volkswagen AG (2017).

Das US Unternehmen IBM Inc. erklärte im Herbst 2016, dass der von IBM entwickelte Supercomputer IBM Watson auch zum intelligenten persönlichen digitalen Assistenten für den Arbeitsplatz der Zukunft taugt (Cognitive Computing). Unter Cognitive Computing versteht man eine neue Ausrichtung von Rechnern in Richtung menschlichen Denkens. Die Wege der Entscheidungsfindung erfolgen über Hypothesen und der Berücksichtigung von zusätzlichen Informationen aufgrund von gemachten Erfahrungen oder externen Steuerimpulsen. Der Vorteil eines solchen Systems ist es, dass es gegenüber dem Menschen „am Internet angebunden" ist und beliebig belesen sein kann und in Fachgebieten tagesaktuell jegliche Literatur kennen kann. Menschen haben dagegen wissensgestützt keine Chance. Insofern benötigt ein solches System auch Wissen über das Unternehmen, nämlich die Daten aus und über das Unternehmen. Das Unternehmen muss es folglich schaffen, dieses bisher in den Köpfen der Menschen vorliegende Wissen für die Zukunft elektronisch aufzubereiten. Dies kann in Form von Enterprise Social Networks oder Enterprise Wikis (Social Business) erfolgen. Insofern ist ein Cognitive Computing nicht von heute auf morgen in einem Unternehmen einzuführen, sondern erst, wenn das Wissen des Unternehmens vollständig elektronisch aufbereitet ist (Chats, Wiki, Enterprise Social Media, etc).[781] IBM Watson wird dabei im Arbeitsleben als Digitaler Assistent für Beschäftigte beim Priorisieren von E-Mails sowie bei der proaktiven Terminplanung helfen und zahlreiche andere Funktionen autonom übernehmen können. Es lernt aus der persönlichen Arbeitsweise des Nutzers, liest bei Mails mit und macht auf Basis dieses Wissens individuelle Handlungsvorschläge für den Nutzer. [782] Der virtuelle Assistent von IBM soll bspw. die Fähigkeiten haben proaktiv eine Besprechung im Terminplaner anzulegen oder zu einem in einer E-Mail erwähnten Thema, das autonom von IBM Watson analysiert wurde, unaufgefordert Hintergrundmaterial zur Verfügung zu stellen.[783] Es handelt sich dabei um ein sogenanntes kognitives System (cognitive system). Als ein kognitives System wird eine Technologie bezeichnet, die durch die tiefgehende Verarbeitung und das Verständnis der natürlichen Sprache Fragen beantworten kann und Rat und Anleitung bieten kann. Das kognitive System stellt dabei Hypothesen auf und formuliert mögliche Antworten anhand der verfügbaren Hinweise. Ein kognitives System wird durch die Analyse großer Mengen an Inhaltsdaten (Content-Mengen) trainiert und ist in der Lage aus Fehlern und Misserfolgen zu lernen. Kognitive System Plattformen arbeiten dabei mit unstrukturierten bzw. semistrukturierten Informationen, um daraus eine kuratierte Informationsbasis und Wissenskarte zu erzeugen. Diese Informationen können durch künstliche Intelligenz (KI) und Algorithmen (maschinelles Lernen, neuronale Netze, deep learning) analysiert werden. Die auf Basis der KI erstellten Empfehlungen und Prognosen stellen den Anwendern Antworten und Unterstützung in einer breiten Palette von Applikationen und Anwendungsfällen zur Verfügung. Mit Hilfe kognitiver Systeme lassen sich:

- das menschliche Urteilsvermögen erweitern;
- Recherche und Ermittlungen umfassend beschleunigen;

781 *Schütt,* Der Weg zum Digitalen Unternehmen[2] (2015) 50 ff.

782 *Bremmer* in computerwoche.de (23.09.2016), IBM Watson wird digitaler Büro-Assistent, abrufbar unter: https://www.computerwoche.de/a/ibm-watson-wird-digitaler-buero-assistent,3323791 (abgerufen am 20.06.2019).

783 *Bremmer* in computerwoche.de (23.09.2016), IBM Watson wird digitaler Büro-Assistent, abrufbar unter: https://www.computerwoche.de/a/ibm-watson-wird-digitaler-buero-assistent,3323791 (zuletzt abgerufen am 20.06.2019).

- die Anwender durch Vorschläge der prognostizierten bestmöglichen Schritte unterstützen;
- das unternehmensweite Knowledge-Management automatisieren;
- best practices durch die Möglichkeit des Lernens durch Erfahrung zusammenfassen und systematisieren.[784]

Forbes ist der Ansicht, dass kognitive Systeme den Arbeitsplatz der Zukunft in einer Art verändern werden, wie wir uns das jetzt nicht vorstellen können und schreibt: *„Cognitive systems can parse all that data, learn what employees need to do their job better – even if they don't yet know it themselves. They can do it in nanoseconds, and they can help automate routine tasks.* (…) *Imagine having an intelligent assistant draw on the recorded knowledge of your profession as well as real-time data from your environment, helping to inform your decisions and describe probabilities to your range of choices for a given task. Imagine that assistant can also then learn over time, through real-life interactions with you and others in your profession, expanding knowledge and offering more precise assistance.“*[785] IBM Watson soll das Ziel verfolgen, jedem Nutzer die Grundlagen für seine Entscheidungen aufzubereiten. Die Analyse zur Erstellung von Handlungsempfehlungen erfolgt bei IBM Watson in zwei Schritten:

- Im ersten Schritt extrahiert IBM Watson entscheidungsrelevante Daten in Echtzeit aus allen verfügbaren Dokumenten (Notizen, ausgetauschte Texte, Tabellen, SMS, E-Mails, etc.). Die KI von IBM Watson ordnet Aufgaben und Arbeitsabläufe, informiert über für den Nutzer relevante Sachverhalte und adressiert an Nutzer anschließend Fragen und Empfehlungen.
- Im zweiten Schritt erstellt IBM Watson auf Basis dieser Analyse eine Liste anstehender Aufgaben für den Mitarbeiter. Der Mitarbeiter soll die Informationen dabei so aufbereitet bekommen, dass er letztlich nur noch primär Entscheidungen zu treffen hat. Dabei hat die KI von IBM Watson die spezifische Rolle des Mitarbeiters, sein Fachgebiet und seine individuelle persönliche Arbeitsweise zu beachten (IBM Watson lernt die persönlichen Präferenzen des Anwenders kennen). Je nachdem wo der Mitarbeiter gerade arbeitet, bestimmen unterschiedliche Zwänge und Prioritäten den Alltag; die KI von IBM Watson sollte dies daher berücksichtigen und lernen.

IBM Watson hat dabei die Fähigkeit die individuelle Kommunikation zu analysieren und kann erkennen, dass bspw. eine E-Mail eine dringende und wichtige Bitte eines Kunden beinhaltet. Dies ergibt sich für IBM Watson aus folgenden Gründen:

- Die Dringlichkeit einer Anfrage kann IBM Watson u.a. dadurch ableiten, dass es natürliche Sprache, Situationen, Schlüsselwörter, Emotionen, Anfragen, Aufgaben und andere handlungsrelevante Inhalte identifizieren kann und Unbedeutendes herausfiltern kann (Watson AlchemyLanguage – Latent Semantic Analyses). Latent Semantic Analyses (LSA) basieren dabei auf Algorithmen, welche die Nähe eines Wortes zu einem

784 *Thorenz* in computerwoche.de (09.08.2016), Warum kognitive Systeme wichtig werden, abrufbar unter: https://www.computerwoche.de/a/print/warum-kognitive-systeme-wichtig-werden,3315459 (zuletzt abgerufen am 20.06.2019).

785 *Forbes Insights*, The Digital Workplace in the Cognitive Era (2016) 3 ff; 7, abrufbar unter: https://www.ibm.com/downloads/cas/ZQPDGNNX (zuletzt abgerufen am 20.06.2019).

Konzept berechnen können („Bank“ wird bei IBM Watson bspw. sowohl als Sitzgelegenheit als auch als Organisation verstanden). IBM schaffte diese Möglichkeit durch die Definition einer allgemeinen „Grundwahrheit“ mit Hilfe des Bereitstellens von Tausenden Beispieltexten.

- Die Wichtigkeit des Kunden selbst leitet IBM Watson bspw. aus dem unternehmerischen SAP System ab, zusätzlich könnte die Priorität weiter erhöht werden, weil IBM Watson bspw. erkennt, dass in einem anderen Service System weitere Tickets für den Kunden noch offen sind. Zusätzlich erkennt Watson die fachliche Anfrage, dass es sich hier bspw. um ein Thema in der von einem Unternehmen strategisch priorisierten Pharmabranche handelt und die Kundenfrage sich auf eine gesetzliche Neuerung bezieht. Aufgrund der analysierten Dringlichkeitsstufen kommt die KI von IBM Watson zum Ergebnis, dass der konkrete Kunde innerhalb der nächsten zwei bis drei Stunden eine Antwort bekommen sollte und fügt die entsprechend hohe Priorität hinzu.[786]

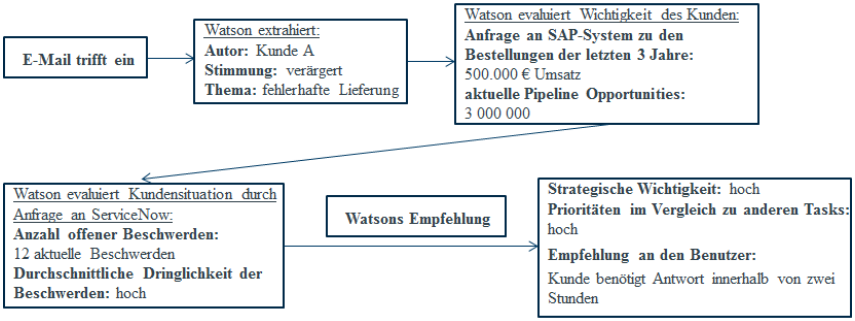


Abbildung 4: *Söldner/Volk* in heise.de (iX 4/2017, S. 70) IBMs Watson für den Arbeitsplatz, abrufbar unter: https://www.heise.de/select/ix/2017/4/1490442995260423 (zuletzt abgerufen 20.06.2019).

IBM Watson funktioniert dabei von der IT-Infrastruktur über eine sogenannte Cloud Plattform, welche Daten aus verschiedenen Quellen unter Berücksichtigung der jeweiligen regulatorischen Voraussetzungen verarbeitet. Es handelt sich dabei um Public bzw. Hybride Clouds auf welche von IBM die IBM Watson Technologie als Service in die Cloud gebracht

786 *Söldner/Volk* in heise.de (iX 4/2017, S. 70) IBMs Watson für den Arbeitsplatz. Ausgewertet. abrufbar unter: https://www.heise.de/select/ix/2017/4/1490442995260423 (zuletzt abgerufen am 20.06.2019).

wird. Nach Angaben von IBM befindet sich eines der IBM Watson Rechenzentren in Frankfurt am Main.[787] Auf Wunsch soll es aber auch möglich sein die IBM Watson Technologie im Unternehmen auch als Private Cloud einzuführen.[788]

Amazon Inc. bietet seinen berühmten Digitalen Assistenten „Alexa" auch als „Alexa for Busines" an. Der Digitale Assistent „Alexa for Busines" kann über Sprachanweisung Kalendereinträge überprüfen, er kann E-Mails vorlesen, Telefonanrufe automatisiert per Sprachbefehl ablaufen lassen, Videokonferenzen anschieben, etc.[789] Zudem lassen sich Konferenzräume und Meetings leichter mit „Alexa for Busines" organisieren, der Mitarbeiter sagt bspw.: „*Alexa, ist dieser Raum frei?*" oder „*Alexa, buch diesen Raum*". Meetings können gestartet werden, indem der Mitarbeiter sagt: „*Alexa, tritt meinem Meeting bei*".[790] Die Cloud-Computing-Tochter AWS (Amazon Web Services, Inc.) der amazon.com, Inc. stellt dabei den Rahmen für „Alexa for Business" bereit.[791]

5.2.2 Cloud Computing

Unter Cloud Computing wird eine Reihe von Technologien und Service Modellen verstanden, die sich auf eine internetbasierte Nutzung und Lieferung von IT-Anwendungen bzw. auf die Verarbeitungsfähigkeit, die Aufbewahrung und den Speicherplatz konzentrieren.[792] Ein Digitaler Assistent „lebt" insofern in dieser Cloud. Cloud Computing bedeutet dabei, dass Daten nicht mehr lokal von einem Verantwortlichen bearbeitet bzw. gespeichert werden, sondern auf einer externen Infrastruktur. Beim Cloud Computing werden Software- und Hardwarefunktionen je nach Beauftragung auf einen externen Dienstleister ausgelagert. Es handelt sich um ein Netzwerk verschiedener Computer, die ihre Rechenleistung bündeln und bei dem sich mehrere Benutzer diese Rechenleistungen teilen. Die benötigen Rechner werden nicht mehr lokal, sondern extern bei Anbietern betrieben. In vielen Fällen ist bei

787 *Koederitz* in ibm.com (25.07.2017), Kognitive Technologie: Sichere Landung auf dem kognitiven Planeten, abrufbar unter: https://www.ibm.com/de-de/blogs/think/2017/07/25/banking-4-0/ (zuletzt abgerufen am 20.06.2019); *Bremmer* in computerwoche.de (23.09.2016), IBM Watson wird digitaler Büro-Assistent, abrufbar unter: https://www.computerwoche.de/a/ibm-watson-wird-digitaler-buero-assistent,3323791 (zuletzt abgerufen am 20.06.2019).

788 *Söldner/Volk* in heise.de (iX 4/2017, S. 70) IBMs Watson für den Arbeitsplatz. Ausgewertet. abrufbar unter: https://www.heise.de/select/ix/2017/4/1490442995260423 (zuletzt abgerufen am 20.06.2019).

789 *Finnegan/Maier* in computerwoche.de (02.02.2018), Alexa for Business – So macht KI Ihr Büroleben leichter, abrufbar unter: https://www.computerwoche.de/a/so-macht-ki-ihr-bueroleben-leichter,3332223 (zuletzt abgerufen am 20.06.2019).

790 *amazon Inc.*, Alexa for Business, abrufbar unter: https://aws.amazon.com/de/alexaforbusiness/ (zuletzt abgerufen am 20.06.2019).

791 *Postinett* in handelsblatt.com (01.12.2017), Sprachgesteuertes Büro – Alexa muss jetzt arbeiten gehen, abrufbar unter: https://www.handelsblatt.com/unternehmen/it-medien/sprachgesteuertes-buero-alexa-muss-jetzt-arbeiten-gehen/20658226.html (zuletzt abgerufen am 20.06.2019); *Postinett* in handelsblatt.com (25.06.2018), Sprachassistenten Hotels, Banken, Autos – Alexa erobert die Unternehmenswelt, abrufbar unter: https://www.handelsblatt.com/technik/thespark/sprachassistenten-hotels-banken-autos-alexa-erobert-die-unternehmenswelt/22730722.html (zuletzt abgerufen am 20.06.2019).

792 *Art 29 Datenschutzgruppe*, WP 196 (2012) 5.

Cloud-Computing dadurch gar nicht mehr genau feststellbar, wo die Daten örtlich gespeichert sind bzw. wo die Anwendungen genau laufen; sie liegen nämlich einfach in der „Cloud". Die dem Cloud Computing zugrundeliegende Informationstechnik selbst ist nicht neu, sie kann sich durch leistungsfähige Internetverbindungen im kommerziellen Bereich aber jetzt erst richtig verwirklichen. IT-Leistungen werden beim Cloud Computing in Echtzeit als Service über das Internet bereitgestellt. Der Zugriff auf die Cloud durch den Anwender selbst erfolgt in der Regel über eine allgemeine verfügbare Standardanwendung, bspw. einen Webbrowser oder eben durch einen Digitalen Assistenten.[793] *Barnitzke* beschreibt Cloud Computing als die nach Bedarf abgerechnete partielle Nutzung flexibler, skalierbarer und virtualisierter IT-Dienstleistungen, die sofort abrufbar und ständig über Internettechnologien verfügbar sind.[794] Man unterscheidet beim Cloud Computing grundsätzlich zwischen:

- *Public Cloud*

Cloud Anbieter und Cloud Nutzer gehören verschiedenen Organisationseinheiten an. Dabei werden Daten verschiedener Cloud Nutzer innerhalb der gleichen Hardwareressourcen verarbeitet (Virtualisierung). Die Public Cloud steht einer Vielzahl von Personen und Unternehmen zur Nutzung zur Verfügung, der Zugriff erfolgt meist über ein Webportal. Werden die einzelnen virtuellen Instanzen der Cloud Nutzer aber nicht ausreichend abgeschirmt, bzw. wenn ein funktionsfähiges Rechtemanagement oder Authentifizierungssystem fehlen, besteht die Gefahr, dass Dritte auf die Daten des Cloud Nutzers ohne dessen Wissen und Zustimmung zugreifen können. Der Cloud Nutzer ist daher vollständig diesen bestehenden Sicherheits- und Verfügbarkeitsrisiken technisch ausgeliefert und kann nur mit rechtlichen Möglichkeiten nachträglich gegensteuern. Die Schwierigkeit besteht insofern darin, dass Cloud Nutzer faktisch nicht erkennen können und damit in der Regel auch nicht beeinflussen können, wo ihre Daten verarbeitet werden.[795]

- *Hybrid Clouds*

Hybrid Clouds bieten die Möglichkeit Private- und Public Cloud Elemente zu kombinieren. Dabei kann bei Nachfragespitzen eine Private Cloud durch eine Public Cloud unterstützt werden und durch externe Ressourcen ergänzt werden, indem man weniger sensible Daten extern in der Public Cloud verarbeiten lässt.[796] Umgekehrt besteht auch die Möglichkeit standardmäßig die Public Cloud zu verwenden, während nur gewisse sensible Daten in der Private Cloud verarbeitet werden.[797]

---

793 *Singer*, Wissenschaftliche Dienste Deutscher Bundestag (Fachbereich WD 10), Aktueller Begriff Cloud Computing, abrufbar unter: https://www.bundestag.de/blob/191178/22a7553089d81c2e06866e15fc354a0e/cloud_computing-data.pdf (zuletzt abgerufen am 20.06.2019); Barnitzke, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 25; 27.

794 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 43.

795 *Jotzo,* Der Schutz personenbezogener Daten in der Cloud (2013) 23; *Balaha/Marka/Zellhofer/Liebel,* Rechtsfragen des Cloud Computing (2011) 21; *Art 29 Datenschutzgruppe*, WP 196 (2012) 30; *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 6.

796 *Jotzo,* Der Schutz personenbezogener Daten in der Cloud (2013) 23; *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 6.

797 *Balaha/Marka/Zellhofer/Liebel,* Rechtsfragen des Cloud Computing (2011) 22; *Art 29 Datenschutzgruppe*, WP 196 (2012) 30.

Die Bestandteile von Cloud Computing lassen sich auf drei Ebenen charakterisieren, wobei jede Ebene auf der anderen aufbaut. Eine höhere Ebene weist alle Merkmale der niedrigsten Ebene auf:

- *Infrastructure as a Service (IaaS)*

Dabei vermietet ein Anbieter eine technische Infrastruktur (virtuellen Remote Server).[798] Das bedeutet, dass einem Cloud Nutzer Rechenleistung und Speicherplatz auf virtuellen Servern zur Verfügung gestellt wird ohne dbzgl. Applikationssoftware.[799] Die Art und Weise der zur Verfügung gestellten Dienstleistungen reichen von Festplattenspeicher bis hin zu vollständigen virtuellen Computer.[800] Die wichtigsten Infrastrukturelemente sind Speicher, Rechnerkapazität, Netzwerkkomponenten sowie Stromversorgung. Beim IaaS werden die entsprechenden Hardware Ressourcen nicht unmittelbar, sondern mittelbar (virtualisiert) verfügbar gemacht. Es handelt sich demnach um die Bereitstellung einer virtualisierten IT-Infrastruktur (Speicher, Rechenkapazität, Netzwerk und sonstige Rechenzentrumsinfrastruktur) über das Internet als jederzeit abrufbare und skalierbare Dienstleistung, welche nutzungsabhängig abgerechnet wird.[801]

- *Platform as a Service (PaaS)*

Neben der virtuellen Rechnerumgebung wie beim IaaS wird dem Kunden beim PaaS eine Entwicklungsplattform geboten, um eigene Anwendungen für die Plattform zu programmieren. Für Entwickler besteht der Vorteil, dass sie eine moderne Entwicklerplattform erhalten, ohne selbst die erforderliche Hard- und Software vorhalten zu müssen.[802] Der Cloud Anbieter bietet Lösungen für die fortgeschrittene Entwicklung und das Hosting von Anwendungen.[803] SaaS Anwendungen werden meist auf einer – eine Abstraktionsebene darunter liegenden PaaS-Ebene entwickelt. Unter PaaS versteht man Cloud-basierte Entwicklungs- und Laufzeitumgebungen für Endbenutzer.[804] Der Entwickler kann sich vollständig auf die Entwicklung der Anwendung konzentrieren und muss sich nicht um den Betrieb des Programms bzw. die darunter liegende Infrastruktur kümmern. Der Cloud Provider von PaaS stellt hier alles bereit.[805]

- *Software as a Servie (SaaS)*

Durch SaaS wird dem Cloud Nutzer die Nutzung von Software ermöglicht, die auf der Infrastruktur des Cloud Providers installiert ist. Für den Cloud Nutzer ist keine lokale Installation einer Client-Software mehr erforderlich.[806] Ein Cloud Anbieter liefert dabei verschiedene Anwendungsdienste über das WWW und macht sie dem Endnutzer verfügbar (webbasierte Officeanwendungen, Tabellen, Textverarbeitungstools, etc.).[807] Es handelt

798 *Art 29 Datenschutzgruppe*, WP 196 (2012) 31.
799 *Balaha/Marka/Zellhofer/Liebel*, Rechtsfragen des Cloud Computing (2011) 20 f.
800 *Jotzo*, Der Schutz personenbezogener Daten in der Cloud (2013) 24.
801 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 47 ff; *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 7.
802 *Jotzo*, Der Schutz personenbezogener Daten in der Cloud (2013) 24.
803 *Art 29 Datenschutzgruppe*, WP 196 (2012) 31.
804 *Balaha/Marka/Zellhofer/Liebel*, Rechtsfragen des Cloud Computing (2011) 20 f.
805 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 49 f; *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 7.
806 *Balaha/Marka/Zellhofer/Liebel*, Rechtsfragen des Cloud Computing (2011) 20 f.
807 *Art 29 Datenschutzgruppe*, WP 196 (2012) 31.

sich bei SaaS um den nach Nutzung abgerechneten Einsatz von Applikationen durch Internettechnologie über einen Browser. Es muss ggf. keine Software auf dem Rechner des Nutzers installiert werden. Das Service beinhaltet alle für eine erfolgreiche Nutzung erforderlichen Bestandteile (gesamte Infrastruktur zum Betrieb der Software, Lizenzen, Wartung des Systems). Für die Nutzung ist lediglich ein internetfähiges Endgerät erforderlich und SaaS wird meist in Form von Abonnements nach verschiedenen Preismodellen zur Verfügung gestellt. Anwendungsfall von SaaS sind Geschäftsanwendungen wie bspw. Customer Relationsship Management (CRM), Personalwesen, die Nutzung von Kollaborationssoftware und eMail. Es kommt damit zu einer Verarbeitung von personenbezogenen Daten. Zudem kann bei SaaS auch enthalten sein, Daten für den Auftraggeber zu analysieren und auszuwerten.[808]

Wird ein digitaler Assistent als komplette Software verwendet, liegt SaaS vor. Ist es noch möglich selbst bestimmte Services einzubinden, kann auch PaaS oder IaaS vorliegen.

5.3 Datenschutz und Digitaler Assistent in der Cloud

5.3.1 Überblick

Ein Digitaler Assistent ist – wie beschrieben – eine Plattform an intern und extern genutzten Applikationen und Bots, die in den Arbeitsprozess eingebunden werden. Dabei orchestriert der Digitale Assistent insofern den Zugriff auf viele bestehende Systeme (z.B. Enterprise Search Suchmaschine, Enterprise Social Network, Enterprise Wiki, etc.). Die Interaktion mit dem Nutzer erfolgt u.a. auch mit Sprachsteuerung oder über Tastatur. Der Digitale Assistent beobachtet den Nutzer, passt sich an ihn an, macht autonome Handlungsvorschläge und führt eigene Aufgaben autonom aus, der Assistent adaptiert sich insofern an den Nutzer. Dahinter steckt Big Data und künstliche Intelligenz.[809] Der Digitale Assistent selbst „lebt" in der Cloud. Digitale Assistenten vereinen zahlreiche Informatik-Fortschritte der vergangenen Jahrzehnte: akustische Erkennung menschlicher Sprache, inhaltliche Verarbeitung der gesprochenen Sätze, die Einschätzung des Kontextes und die Suche nach einer passenden Antwort, schließlich die Sprachsynthese, um das Rechenergebnis in verständliche Worte zu packen.[810] Datenschutzrechtlich ist insbesondere zu betrachten:

- *Sprachaufzeichnung und Umwandlung in Textform* (siehe auch **Kapitel 5.3.2**).
- *Profiling des Nutzers* (je präziser die Kenntnis über den Nutzer, desto besser die Unterstützungsmöglichkeiten des Digitalen Assistenten unmittelbar im Interesse des Nutzers

808 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 50 ff; *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 7.

809 *Schmitt* in zeit.de (09.02.2017) Künstliche Intelligenz: Verstehst du, was ich will? Besser, als du glaubst, abrufbar unter: http://www.zeit.de/2017/05/kuenstliche-intelligenz-chatbots-alexa-siri-kommunikation (zuletzt abgerufen am 20.06.2019).

810 *Håkansson*, KTH Royal Institute of Technology (Königliche Technische Hochschule Stockholm), AI and privacy GDPR seminar (2017), abrufbar unter: https://www.youtube.com/watch?v=L6vK3deWG4A (zuletzt abgerufen am 20.06.2019); *Schmitt* in zeit.de (09.02.2017) Künstliche Intelligenz: Verstehst du, was ich will? Besser, als du glaubst, abrufbar unter: http://www.zeit.de/2017/05/kuenstliche-intelligenz-chatbots-alexa-siri-kommunikation (zuletzt abgerufen am 20.6.2019).

z.B. bei Informationssuche und proaktiver Informationsbereitsstellung; automatisierte Terminplanung; Dienstreisebuchungen; Identifizierung der Wichtigkeit von Personen für den Nutzer; Enterprise Helpdesk EHD Funktionalitäten; Sprach- und Textschnittstelle; Mehrsprachenunterstützung; etc.).
- *Cloud Computing* (siehe auch **Kapitel 5.2.2**).

Möchte ein Arbeitgeber für Zwecke des Beschäftigtenverhältnisses einen Digitalen Assistenten einführen, bedarf es der insofern datenschutzrechtlichen Prüfung:

5.3.2 Rechtmäßigkeit

Sprachaufzeichnung und Spracherkennung

Im Rahmen der Prüfung von Sprachsteuerungen sind straf- und datenschutzrechtliche Fragen hinsichtlich der Zulässigkeit zu klären:

Bei der Spracherkennung erfolgt zu Beginn eine Aufzeichnung des Sprachbefehls. Dabei wird die gesprochene Sprache mit einem Mikrophon aufgenommen und das analoge Sprachsignal wird digitalisiert, also in eine Folge von binären Zahlen umgewandelt.[811] Anschließend wird mit Hilfe von künstlicher Intelligenz (neuronale Netze) analysiert, welche Worte es in geschriebener Sprach sein können.[812] Aus der Analyse der digitalen Sprachaufzeichung lässt sich die Wahrscheinlichkeit ermitteln, dass eine digitale Stimmaufzeichnung einen bestimmten Wort oder Satz entspricht.[813] Die finale Spracherkennung in Form eines komplizierten Prozesses erfolgt – hier stark vereinfacht zusammengefasst – durch Klassifikation mit Hilfe künstlicher Intelligenz dank neuronaler Netze. Dabei liegen gesprochene Signale an der Eingangsschicht eines neuronalen Netzes vor und werden dann auf den Zwischenschichten des neuronalen Netzes verarbeitet, bis sie an der Ausgangsschicht als erkannte Worte vorliegen.[814] Dies geschieht durch einen Suchalgorithmus, der ermittelt mit welcher Wahrscheinlichkeit welche Laute aufeinander folgen. Voraussetzungen für eine erfolgreiche Spracherkennung sind:

- phonetische Wörterbücher (Aussprachewörterbücher) und riesige Datenmengen aus bereits korrekt transkribierten Aufnahmen; und
- Programme (neuronale Netze), die anschließend den eingegangenen Sprachbefehl prüfen, mit welcher Wahrscheinlichkeit welche Worte aufeinander folgen. Die neuronalen

811 *fask.uni-mainz.de*, Künstliche Intelligenz: Spracherkennung und Sprachverstehen, abrufbar unter: http://www.fask.uni-mainz.de/user/warth/Ki.html (zuletzt abgerufen am 20.06.2019).

812 *Håkansson*, KTH Royal Institute of Technology (Königliche Technische Hochschule Stockholm), AI and privacy GDPR seminar (2017), abrufbar unter: https://www.youtube.com/watch?v=L6vK3deWG4A (zuletzt abgerufen am 20.06.2019).

813 *Schönberger*, Big Data – Die Revolution, die unser Leben verändern wird (2014) 134.

814 *fh-wedel.de*, Begriff Künstliche Intelligenz – Spracherkennung auf, abrufbar unter: http://www.fh-wedel.de/~si/seminare/ss01/Ausarbeitung/a.sprache/gdlgsprerk35.htm (zuletzt abgerufen am 20.06.2019).

Netze werden dabei mit Datenbanken mit gigantischen Mengen korrekt transkribierter Texte trainiert.[815]

Am Ende wird der transkribierte und vom System in richtige Wörter der geschriebenen Sprache umgewandelte Sprachbefehl vom Programm umgesetzt. In der umgekehrten Situation, nämlich bei der gesprochenen Antwort des Digitalen Assistenten wird das Ergebnis wiederum dem Nutzer durch das System in der Form vorgelesen.[816] Aus einer groben informationstechnischen Perspektive passiert folgendes:

- Der Digitale Assistent wird aktiviert durch einen Sprachbefehl wie "computer", "Siri", "Alexa", "Echo" or "Jarvis", wobei der Assistent den Sprachbefehl mit Hilfe von künstlicher Intelligenz (neuronales Netz[817]) versteht. Alternativ kann der Digitale Assistent auch über Knopfdruck (Fernbedienung) aktiviert werden.
- Nach der Aktivierung über den Aktivierungsbefehl oder Knopfdruck, zeichnet der Digitale Assistent den dann folgenden Sprachbefehl des Nutzers auf, komprimiert die aufgezeichnete Sprachdatei und übermittelt diese komprimierte Sprachdatei in die Cloud. Mit Hilfe von künstlicher Intelligenz (2. Neuronales Netz) wird in der Cloud das gesprochene Wort des Nutzers (komprimierte Sprachdatei) in Textform umgewandelt. Anschließend erfolgt eine Speicherung in der Cloud.
- Der in Textform umgewandelte Sprachbefehl wird mit Hilfe von künstlicher Intelligenz (3. Neuronales Netz) hinsichtlich seines Inhalts und Kontextes analysiert, mit dem Ziel eine Antwort für den Nutzer zu finden. Die letztlich gefundene Antwort wird aus der Cloud wieder zurück an den Digitalen Assistenten übermittelt und von diesem an den Nutzer weiterkommuniziert. Ein Digitaler Assistent kann auch autonom Vorschläge machen und dem Nutzer in der jeweiligen Situation, in der er sich befindet, unterstützen. Dies hängt davon ab, über wieviel Informationen der Digitale Assistent über den Nutzer verfügt und welche Applikationen an den Digitalen Assistenten angebunden sind.[818]

---

815 *Meineck* in spiegel.de (09.04.2017), Funktioniert Sprechen so gut wie Tippen?, abrufbar unter: http://www.spiegel.de/netzwelt/apps/spracherkennung-fuer-ios-und-android-im-test-wie-gut-funktioniert-das-a-1134324.html (zuletzt abgerufen am 20.06.2019).

816 *Drösser* in zeit.de (19.03.2015), Künstliche Intelligenz: Sie haben verstanden, abrufbar unter: http://www.zeit.de/2015/10/kuenstliche-intelligenz-computer-simultan-dolmetscher (zuletzt abgerufen am 20.06.2019).

817 Stark vereinfacht kann der Aufbau und die Funktionsweise eines neuronalen Netzes folgendermaßen beschrieben werden: Das abstrahierte Modell eines neuronalen Netzes besteht aus Neuronen, auch Units oder Knoten genannt. Sie können Informationen von außen oder von anderen Neuronen aufnehmen und modifiziert an andere Neuronen weiterleiten oder als Endergebnis ausgeben (vgl. Definition – Was ist ein Neuronales Netz?, abrufbar unter: https://www.bigdata-insider.de/was-ist-ein-neuronales-netz-a-686185/ (zuletzt abgerufen am 20.06.2019).

818 *Damaschke*, Siri Handbuch (2016) 13 ff; Öffentliche Diskussion: „Licht und Schatten der Digitalisierung" mit Y. Hofstetter, U. Schäfer und B. Baginski (veröffentlicht am 23.06.2017): https://www.youtube.com/watch?v=fBYpp2AyLRs (zuletzt abgerufen am 20.06.2019).

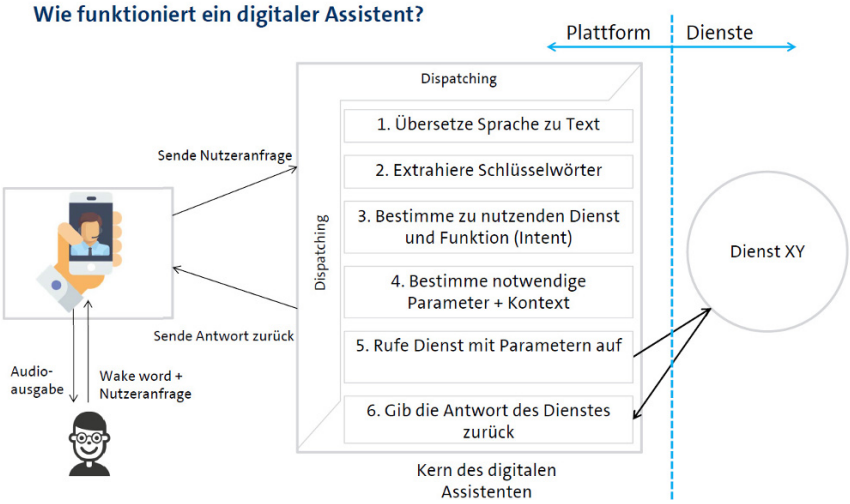


Abbildung 5: *Meier/Klein*, Die Zukunft der Büroarbeit bei Volkswagen – Der digitale Assistent, Vortrag Volkswagen AG (2017).

Strafrechtliche Anforderungen Deutschland

In Deutschland existieren zwei zu beachtende Strafbestimmungen:

- § 201 Abs 1 StGB (Verletzung der Vertraulichkeit des Wortes);
- § 90 iVm. § 148 Abs 1 Nr 2 TKG 2004 (Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen).

§ 201 Abs 1 StGB pönalisiert das unbefugte (z.B. heimliche) Aufnehmen unmittelbarer Äußerungen in reproduzierbare Aufzeichnungen (§ 201 Abs 1 Nr 1 StGB: Aufnahme des nicht-öffentlich gesprochenen Wortes; § 201 Abs 1 Nr 2 StGB: Gebrauchen der Aufnahme und Weitergabe an Dritte). Im subjektiven Tatbestand reicht bei § 201 StGB bedingter Vorsatz (dolus eventualis).[819] Bei § 201 Abs 1 StGB wird nicht auf die Heimlichkeit der Aufzeichnung, sondern auf die Unbefugtheit iSv. Rechtswidrigkeit abgestellt. Hintergrund ist der Fall, dass eine Aufnahme bzw. ein Abhören zwar mit Wissen, aber gegen den Willen des Betroffenen erfolgt. Auch in solchen Fällen ist der Betroffene strafrechtlich schutzwürdig. Insofern ist nicht nur „heimliches" Aufzeichnen strafrechtlich iSd. § 201 StGB relevant sondern auch ein rechtwidriges („unbefugtes") Aufzeichnen mit Wissen aber gegen den ersichtlichen Willen des Opfers.[820] Dies ist bei der Ausgestaltung von Sprachsteuerung am Arbeitsplatz mitzuberücksichtigen, in dem einem Nutzer (Beschäftigten) in jedem Fall eine

819 *Fischer* in Fischer (Hrsg), Strafgesetzbuch[66] (2019) § 201 Rn 14; *Heuchemer* in v. Heintschel-Heinegg (Hrsg), BeckOK StGB[42. Edition] (Stand 01.05.2019) § 201 Rn 16; *Kargl* in Kindhäuser/Neumann/Paeffgen (Hrsg), Strafgesetzbuch[5] (2017) § 201 Rn 21.

820 *Kargl* in Kindhäuser/Neumann/Paeffgen (Hrsg), Strafgesetzbuch[5] (2017) § 201 Rn 10; *Heuchemer* in v. Heintschel-Heinegg (Hrsg), BeckOK StGB[42. Edition] (Stand 01.05.2019) § 201 Rn 6 f.

Alternative zur Sprachsteuerung geboten wird. Der Nutzer soll auch immer über reine Tastaturbefehle mit dem Digitalen Assistenten kommunizieren können, wenn er nicht will, dass seine Stimme aufgezeichnet wird. Spricht ein Beschäftigter als Nutzer trotz der Möglichkeit die entsprechenden Anfragen oder Arbeitsaufträge auch per Tastatur einzugeben, trotzdem mit seinem Digitalen Assistenten per Sprachbefehl, liegt kein Fall des unbefugten Aufzeichnens der Sprache mit Wissen, aber gegen den ersichtlichen Willen des Opfers vor. Im Regelfall ist ein Nutzer (Beschäftigten) über die Funktionsweise der Sprachsteuerung umfassend informiert (Art 13 f. DSGVO) inklusive der Möglichkeit alternativ mit Hilfe der Tastatur mit dem Digitalen Assistenten zu kommunizieren. Spricht der Beschäftigte als Nutzer trotzdem bewusst mit dem Digitalen Assistenten, besteht kein Strafbarkeitsrisiko, weil nicht „unbefugt". Es liegt dann zugleich eine strafrechtlich wirksame Einwilligung des Nutzers in die Sprachaufzeichnung vor. Bei § 201 StGB kommt neben der ausdrücklichen auch eine konkludente Einwilligung in Betracht.[821]

Zudem ist wichtig, dass der Status einer aktivierten Sprachsteuerung durch entsprechende technische und organisatorische Maßnahmen für jedermann ausreichend ersichtlich gemacht wird (z.B. blinkende Lichter oder spezielle Lichtfarbe am Lautsprecher zur Anzeige der aktivierten Sprachsteuerung, etc.). Die *Deutsche Bundesregierung* antwortet zur Frage, wenn unbeteiligte Dritte durch eine Sprachsteuerung erfasst werden, die gar nicht wissen, dass eine solche eingeschaltet ist (am Bsp. der Sprachsteuerung der Puppe „Cayla"): *„Fehlt die Einwilligung Dritter, ist die Erhebung ihrer Daten mangels Erlaubnisnorm unzulässig."*[822]

Aktiviert der Verantwortliche (Arbeitgeber) die Sprachaufzeichung in Situationen, wo der Beschäftigte nicht damit rechnet, also heimlich und damit klar „unbefugt" und hört der Verantwortliche mit Hilfe der Sprachsteuerung des Digitalen Assistenten den Beschäftigten rechtswidrig ab (§ 201 Abs 2 Nr 1 StGB) und/oder zeichnet dabei auch seine Stimme rechtswidrig auf (§ 201 Abs 1 Nr 1 StGB), sind beide Tatbestände des § 201 StGB vollständig einschlägig und Strafbarkeit für den Arbeitgeber ist gegeben.[823]

Bei der zweiten zu prüfenden Strafbestimmung **§ 90 iVm. § 148 Abs 1 Nr 2 TKG 2004** (Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen) handelt es sich um eine zu § 201 StGB begleitende Strafvorschrift.[824] Mit § 90 TKG 2004 (ex § 65 TKG 1996) wird die Strafbarkeitsgrenze gegenüber § 201 StGB vorverlagert.[825] Die Bestimmung zielt auf sendefähige und als Alltagsgegenstände getarnte Geräte ab, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und aufgrund dieser Umstände oder aufgrund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht-öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen. Die Bestimmung soll den Missbrauch von Sendeanlagen und sonstigen Telekommunikationsanlagen zum unbemerkten Abhören fremder Gespräche (z.B. Feuerzeuge oder Kugelschreiber mit eingebauten Mikrofonen, Lasermikrofone, Minisender in

821 *Kargl* in Kindhäuser/Neumann/Paeffgen (Hrsg), Strafgesetzbuch[5] (2017) § 201 Rn 23 f; *Heuchemer* in v. Heintschel-Heinegg (Hrsg), BeckOK StGB[42. Edition] (Stand 01.05.2019) § 201 Rn 19.

822 BT-Drs 18/8317, 5 (Antwort auf Frage 8).

823 *Fischer* in Fischer (Hrsg), Strafgesetzbuch[66] (2019) § 201 Rn 2 ff.

824 BT-Drs 17/5707, 78 f.

825 *Dierlamm/Cordes* in Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018) § 90 Rn 2 ff.

der Sprechmuschel eines Telefonapparates oder in einem Lampenschirm, etc.) oder der heimlichen Anfertigung von Videoaufzeichnungen (z.B. Gürtelkameras, PenCams oder TeddyCams) verhindern und bestimmt, dass der Besitz, die Herstellung, der Vertrieb und die Einfuhr solcher Anlagen im Geltungsbereich des TKG 2004 verboten ist. Bei § 90 TKG 2004 muss eine Sende- oder sonstige Telekommunikationsanlage vorliegen, die in einem Gegenstand des täglichen Gebrauchs verkleidet ist. Verkleidet ist eine Sende- oder sonstige Telekommunikationsanlage mit dem Gegenstand des täglichen Gebrauchs stets dann, wenn sie von außen nicht ohne weiteres erkannt werden kann, sie somit als getarnt anzusehen ist. Ob die Anlage tatsächlich zum Abhören eingesetzt werden soll, ist unbeachtlich; Maßstab ist die objektive Geeignetheit. Die Anlage muss dazu auch „bestimmt" sein. Der Gesetzgeber hat den Begriff der „Bestimmtheit" nicht definiert, sondern führt als konkretes Beispiel Mobiltelefone an, wo § 90 TKG 2004 eindeutig nicht einschlägig ist, weil nicht iSd. § 90 TKG 2004 dazu „bestimmt". Daraus lässt sich schlussfolgern, dass es dem Deutschen Gesetzgeber darum geht, Alltagsgegenstände, die zwar zum Abhören missbraucht werden können, die sich aus dem Gegenstand ergebende Gefahr dem Bürger aber gleichwohl bekannt ist (iSv. abhörfähige Alltagsgegenstände), vom Verbot des § 90 TKG 2004 klar auszunehmen. Ein Mobiltelefon lässt sich bspw. zum Abhören des nicht-öffentlich gesprochenen Wortes sehr leicht verwenden, dieses Risiko ist allerdings allgemein bekannt. Der Bürger kann daher diese Gefahr „Mobiltelefon" erkennen, einschätzen und bspw. verlangen, dass ein Mobiltelefon während eines vertraulichen Gesprächs aus dem Raum gebracht wird. Es handelt sich also bei einem Mobiltelefon nicht um eine Sende- bzw. Telekommunikationsanlage, die einen anderen Gegenstand vortäuscht bzw. nicht um eine Sende- bzw. Telekommunikationsanlage, die mit einem Gegenstand des täglichen Gebrauchs „verkleidet" ist. Umgekehrt gilt § 90 TKG 2004 aber dort, wo Alltagsgegenstände typischerweise nicht über Abhörfunktionen verfügen und daher der Bürger objektiv damit auch nicht rechnen muss, dass ein solches Abhörrisiko besteht.[826]

§ 90 TKG 2004 betrifft Digitale Assistenten insofern, als die Sprachsteuerung u.a. über Lautsprecher, die im Raum platziert werden, erfolgt. So könnte begründet vertreten werden, dass Menschen in Lautsprechern (vgl. Amazon Alexa) noch keine gleichzeitigen Abhöranlagen (Mikrophone) für Sprachsteuerungen vermuten, sondern auf diese zusätzliche Funktion immer speziell hingewiesen werden müssen, dass nicht nur ein Alltagsgegenstand in Form eines gewöhnlichen „Lautsprechers" vorliegt, sondern zugleich eine Sprachsteuerung mit Mikrophonen zur Aufzeichnung der Sprechbefehle. Erst durch eine solche Sensibilisierung und transparente Information würde vollkommen rechtssicher keine Sendeanlage bzw. Telekommunikationsanlage vorliegen, die mit einem Gegenstand des täglichen Gebrauchs (Lautsprecher) iSd. § 90 Abs 1 TKG 2004 „verkleidet" ist. Dasselbe kann für Smart TVs mit versteckten Mikrophonen, bzw. Smart Glasses mit Kameras und Mikrophonen gelten.[827]

---

826 *Dierlamm/Cordes* in Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018) § 90 Rn 2 ff; BT-Drs 17/5707, 78 f; *Vogelgesang/Hessel*, Spionagegeräte im Kinderzimmer? ZD 2017, 269 (272); *Hessel*, „My friend Cayla" – eine nach § 90 TKG verbotene Sendeanlage, abrufbar unter: http://www.jurpc.de/jurpc/show?id=20170013 (zuletzt abgerufen am 20.06.2019); *Piepenbrock* in Büchner/Ehmer/Geppert et al (Hrsg), TKG[2] (2000) § 65 Rn 8 f.

827 *Schwenke*, § 90 TKG – Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte, K&R 5/2017, 297 ff.

Die BNetzA vertritt als Aufsichtsbehörde (§ 115 TKG 2004) zu § 90 TKG 2004 folgende Anforderungen an Digitale Assistenten und deren Lautsprecher zur Sprachsteuerung (Prüfkriterien digitale Assistenzsysteme[828]):

*„**a.** Der Nutzer muss Kenntnis davon haben, dass die Sendeanlage Audiodateien an den Hersteller oder andere Unternehmen weiterleitet.*

Der Hersteller hat hier die Obliegenheit der eindeutigen Aufklärung. Eine bloß beiläufige und nicht ohne weiteres erkennbare Erwähnung der Aufnahme und Weiterleitung an den Hersteller reicht nicht aus. Der Hersteller muss vielmehr offensiv aufklären. So ist es erforderlich, dass die Weiterleitung der Audiodateien durch die Sendeanlage an den Hersteller in der Produktbeschreibung eindeutig herausgestellt wird. Erfolgt die Produktbeschreibung an mehreren Stellen, also als Beilage in der Verpackung, auf der Verpackung und im Internet, so muss der Hinweis auf die Weiterleitung der Audiodateien an den Hersteller und weitere Unternehmen an allen Stellen gegeben werden.

Wenn der Hersteller/Verkäufer in dieser Art öffentlich über die Aufnahmefunktion informiert und ist die Nutzung des Gegenstandes nur bewusst möglich, wird hier die Gefahr, dass Dritte heimlich aufgenommen werden, als gering betrachtet. Zum einen erfolgt eine Aufnahme nur bei der bewussten Nutzung des Stichwortes (s. u.), so dass eine zufällige Aufnahme weitestgehend ausgeschlossen ist. Zum anderen ist zu konstatieren, dass wenn der Dritte ein solches Gerät bewusst bei dem Besitzer nutzt, es in seiner Verantwortung liegt, sich entweder über die öffentlichen Quellen des Herstellers/ Verkäufers oder beim Besitzer über die Übertragung der Audiodateien kundig zu machen. Von einem heimlichen Abhören durch den Hersteller kann in diesen Fällen nicht gesprochen werden.

***b.** Der Besitzer/Nutzer der Sendeanlage muss bestimmen können, was von ihm aufgenommen wird. Hierzu gehört, dass er Einfluss darauf nehmen kann,*

***(1)** ob eine Aufnahme gemacht wird.*

Die Sendefunktion muss erkennbar ausschaltbar sein. Es muss dem Nutzer bekannt sein, wie dies möglich ist. Das Gerät muss anzeigen, dass es ausgeschaltet ist.

***(2)** wann die Aufnahme beginnt*

- *Einsatz von Signalwörtern*

Der Hersteller kann dies dadurch gewährleisten, indem er die Weiterleitung der Audiodateien an ein eindeutiges vorher kommuniziertes Signalwort knüpft. Das Signalwort muss dazu geeignet sein, die Aufnahme durch den Besitzer/ Nutzer zu kontrollieren. Wenn das Signalwort so gewählt wird, dass dieses im allgemeinen Sprachgebrauch derart verankert ist, dass es bei Unterhaltungen ohne besonders aufzufallen häufig verwendet

wird, ist es kein geeignetes Signalwort. Der Begriff ist so zu wählen, dass er vom Nutzer/Besitzer und anderen in der Nähe befindlichen Personen bewusst als Signalwort eingesetzt werden kann und nur dann ausgesprochen wird, wenn tatsächlich die Sendeanlage angesprochen werden soll.

---

828 *BNetzA*, Prüfkritieren digitale Assistenzsysteme – Z21e6216-Grundsatz v. 11.04.2017, abrufbar unter: https://fragdenstaat.de/anfrage/alexa-siri-co-kunstliche-intelligenz-uberprufungs unterlagen/#nachricht-82803 (zuletzt abgerufen am 20.06.2019).

Am geeignetsten ist ein Signalwort, wenn mit ihm unmittelbar beim Besitzer/ Nutzer die Assoziation mit dem Aufnahmegegenstand verbunden ist.

- *Einsatz von Tastendruckverfahren*

Wenn der Hersteller den Beginn der Aufnahme an das Drücken einer Taste (sei es am Gerät oder einer Fernbedienung) knüpft, ist gewährleistet, dass der Besitzer/ Nutzer weiß, dass eine Aufnahme seiner Audiodatei in diesem Moment beginnt

***(3)** und weiß, wann die Aufnahme endet.*

- *Tastendruckverfahren*

Wenn die Sendeanlage mittels Tastendruckverfahrens so gesteuert wird, dass eine Taste während der Audioaufnahme gedrückt werden muss und die Aufnahme dann endet, wenn die Taste losgelassen wird, weiß der Nutzer/ Besitzer eindeutig, dass seine Aufnahme beendet ist.

- *durch eindeutige optische/ akustische Signale*

Die Sendeanlage zeigt durch optische Signale wie gut sichtbare Lichtsignale oder gut wahrnehmbare akustische Signale das Ende der Aufnahme an."[829]

Hält man sich an diese von der BNetzA aufgestellten Kriterien zum Einsatz von Digitalen Assistenten – entsprechend angepasst an den konkreten Einzelfall im Unternehmen – ist die Verwirklichung des § 90 iVm. § 148 Abs 1 Nr 2 TKG 2004 als unwahrscheinlich anzusehen, weil trotz des Einsatzes von Lautsprechern, die zugleich Mikrophone sind, insofern kein „getarnter" Alltagsgegenstand mehr vorliegt.[830]

Strafrechtliche Anforderungen Österreich

In Österreich existiert iZh mit Sprachsteuerung mit § 120 öStGB nur eine zu beachtende Strafbestimmung.[831] § 120 Abs 1 öStGB pönalisiert die unbefugte Benutzung eines Tonaufnahme- oder Abhörgerätes zum Festhalten bzw. zum Abhören einer nicht öffentlichen und nicht zu seiner Kenntnisnahme bestimmten Äußerung eines anderen in der Absicht, sich oder einem anderen Unbefugten davon Kenntnis zu verschaffen. Nach § 120 Abs 1 StGB kann nie bestraft werden, wer nach dem Willen des Sprechenden der Empfänger der Äußerung sein sollte, insbesondere auch dann nicht, wenn dieser Empfänger die Tonaufnahme heimlich herstellte. Wenn der nach dem Willen des Sprechenden korrekte Empfänger, die heimlich ohne Einverständnis des Sprechenden gemachte Aufzeichnung dann aber weitergibt oder veröffentlicht, macht sich dann nach § 120 Abs 2 StGB (Weitergabe oder Veröffentlichung) strafbar.[832] In die Aufnahme des Gesprochenen kann ausdrücklich oder konkludent vom Sprechenden zugestimmt werden, allerdings bedeutet ein solches

829 *BNetzA*, Prüfkritieren digitale Assistenzsysteme – Z21e6216-Grundsatz v. 11.04.2017 , abrufbar unter: https://fragdenstaat.de/anfrage/alexa-siri-co-kunstliche-intelligenz-uberprufungsunterlagen/#nachricht-82803 (zuletzt abgerufen am 20.06.2019).

830 *Dierlamm/Cordes* in Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018) § 90 Rn 7.

831 *Bagre* in diepresse.com (17.02.2017), Deutschland verbietet Verkauf von Puppe Cayla, abrufbar unter: https://diepresse.com/home/techscience/technews/5171332/Deutschland-verbietet-Verkauf-von-Puppe-Cayla (zuletzt abgerufen am 20.06.2019).

832 *Fabrizy*, StGB[13] (2018) § 120 Rn 2 ff.

Einverständnis noch kein Einverständnis zur Weiter- oder Wiedergabe.[833] Insofern gilt Vergleichbares wie beim deutschen § 201 StGB:

Im Regelfall ist ein Nutzer (Beschäftigter) über die Funktionsweise der Sprachsteuerung umfassend informiert (Art 13 f. DSGVO) inklusive der Möglichkeit, alternativ mit Hilfe der Tastatur mit dem Digitalen Assistenten zu kommunizieren. Spricht der Beschäftigte als Nutzer trotzdem bewusst mit dem Digitalen Assistenten in Form von Sprachbefehlen, besteht für den Arbeitgeber kein Strafbarkeitsrisiko:

- Es liegt eine zumindest konkludente strafrechtliche Einwilligung des Nutzers (Beschäftigten) in die Sprachaufzeichnung vor. Die Aufzeichnung durch den Digitalen Assistenten (Arbeitgeber) erfolgt nicht unbefugt.
- Darüberhinaus wäre auch eine Aufzeichnung ohne (konkludentem) Einverständnis des Nutzers – anders als beim deutschen § 201 dStGB – in Österreich wahrscheinlich noch gar nicht strafbewehrt, da der Beschäftigte bei (zumindest dienstlichen) Sprachbefehlen an den Digitalen Assistenten (bspw. Dienstreisebuchung mittels Sprachsteuerung), welcher dem Arbeitgeber zuzurechnen ist (Eigentum), faktisch mit dem Arbeitgeber selbst kommuniziert und damit auch das zusätzliche Tatbestandsmerkmal „nicht zu seiner Kenntnisnahme bestimmten Äußerung“ gemäß § 120 Abs 1 öStGB insofern nicht erfüllt wäre. Das Aufnehmen einer Äußerung eines anderen durch jemanden „für den sie bestimmt“ ist, erfüllt nicht das strafrechtliche Tatbild des § 120 Abs 1 öStGB.[834]
- Auch ein zufälliges Abhören unbeteiligter Dritter (sich unterhaltende Kollegen betreten den Raum während die Sprachsteuerung durch den Nutzer aktiviert ist) wird in den wenigsten Fällen strafrechtsrelevant sein, da § 120 Abs 1 StGB Absicht (§ 5 Abs 2 öStGB) verlangt, sich und einem anderen Unbefugten von einer nicht öffentlichen und nicht zu seiner Kenntnis bestimmten Äußerung eines anderen Kenntnis zu verschaffen. Fehlt es im Tatzeitpunkt an dieser Absicht (§ 5 Abs 2 StGB), ist der subjektive Tatbestand nicht erfüllt. Bei Sprachaufzeichnungen von unbeteiligten Dritten liegt eine solche Absicht in der Regel nicht vor.[835] In Deutschland reicht bei § 201 dStGB hingegen bereits bedingter Vorsatz.[836]

Ein Strafbarkeitsrisiko nach § 120 Abs 1 öStGB besteht grundsätzlich also nur dann, wenn der Arbeitgeber die Mikrophone der Sprachsteuerung heimlich aktiviert mit der Absicht (§ 5 Abs 2 öStGB) den Beschäftigten dadurch mit Hilfe der Sprachsteuerungsmikrofone „unbefugt“ rechtswidrig abzuhören bzw. seine nichtöffentlichen Äußerungen mit einem

833 *Lewisch/Reindl-Krauskopf* in Höpfl/Ratz (Hrsg), WK StGB[2] (Stand 17.10.2017) § 120 Rn 14; *Tipold* in Leukauf/Steininger (Hrsg), StGB[4] (2017) § 120 Rn 13 ff; *Thiele* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch[22 Lfg] (Stand Mai 2010) § 120 Rn 70 ff.

834 *Thiele* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch[22 Lfg] (Stand Mai 2010) § 120 Rn 42; *Tipold* in Leukauf/Steininger (Hrsg), StGB[4] (2017) § 120 Rn 8.

835 *Lewisch/Reindl-Krauskopf* in Höpfl/Ratz (Hrsg), WK StGB[2] (Stand 17.10.2017) § 120 Rn 2; *Tipold* in Leukauf/Steininger (Hrsg), StGB[4] (2017) § 120 Rn 14; *Thiele* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch[22 Lfg] (Stand Mai 2010) § 120 Rn 66.

836 *Fischer* in Fischer (Hrsg), Strafgesetzbuch[66] (2019) § 201 Rn 14.

Tonaufnahmegerät aufzuzeichnen (§ 120 Abs 1 öStGB). In diesem Fall liegt weder ein Einverständnis des Beschäftigten vor, noch sind die Äußerungen des Beschäftigten in diesen Fällen für den dann heimlich abhörenden Arbeitgeber bestimmt.[837]

Damit sind in Österreich – auch mangels einer vergleichbaren Bestimmung wie § 90 dTKG 2004 – die Strafbarkeitsrisiken und Anforderungen deutlich geringer als in Deutschland.

Datenschutzrechtliche Anforderungen

Da sowohl in Deutschland als auch in Österreich für die Aufzeichnung der Sprache eine zumindest konkludente Einwilligung erforderlich ist (§ 201 dStGB[838], § 120 öStGB[839]), bedarf es auch der informierten datenschutzrechtlichen Einwilligung für die Aufzeichnung des konkreten Sprachbefehls. Zudem ist hinsichtlich der Rechtsgrundlage (Art 6 bzw. Art 9 DSGVO) noch zu prüfen, ob Sprachdateien bereits als besondere Kategorien personenbezogener Daten, nämlich als biometrische Daten (Art 4 Nr 14 DSGVO) anzusehen sind oder nicht. Akustische Stimmprofile fallen grundsätzlich unter den Begriff der biometrischen Daten, denn es ist mittels akustischer Identifikationsverfahren der Stimmerkennung eine Sprechererkennung möglich.[840] *Feiler/Forgó* präzisieren mit Verweis auf ErwGr 51 Satz 3 DSGVO insofern, als sie auf den Verwendungszweck der biometrischen Daten abstellen: Biometrische Daten iSd. Art 4 Nr 14 iVm. Art 9 Abs 1 DSGVO liegen immer nur dann vor, wenn die Daten nicht nur zur Identifizierung einer natürlichen Person geeignet sind sondern, wenn sie auch tatsächlich konkret zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden sollen (Art 4 Nr 14 DSGVO). Es kommt also auf den Verarbeitungszweck an, ob biometrische Daten als besondere Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO) anzusehen sind oder nicht. Werden insofern die aufgezeichneten Sprachbefehle der Nutzer nicht für eine Identifizierung des Sprechers verwendet, liegen trotz der bestehenden Identifizierbarkeit, aber aufgrund der Nicht-Verarbeitung zu diesem Zweck „Identifizierung", bei Sprachbefehlen keine besonderen Kategorien personenbezogener Daten vor.[841] Nach einer Studie der *Arbeiterkammer Wien* zu Digitalen Assistenten vom Juni 2019 ist es aber aus Gründen der Datensicherheit unbedingt erforderlich, dass Nutzer von Digitalen Assistenten ein Stimmprofil zur Authentifizierung anlegen, damit der Zugang auf die Informationen des Digitalen Assistenten technisch sicher ein-

837 *Fabrizy*, StGB[13] (2018) § 120 Rn 2 ff.

838 *Kargl* in Kindhäuser/Neumann/Paeffgen (Hrsg), Strafgesetzbuch[5] (2017) § 201 Rn 23 f; *Heuchemer* in v. Heintschel-Heinegg (Hrsg), BeckOK StGB[42. Edition] (Stand 01.05.2019) § 201 Rn 19.

839 *Lewisch/Reindl-Krauskopf* in Höpfl/Ratz (Hrsg), WK StGB[2] (Stand 17.10.2017) § 120 Rn 14; *Tipold* in Leukauf/Steininger (Hrsg), StGB[4] (2017) § 120 Rn 13 ff; *Thiele* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch[22 Lfg] (Stand Mai 2010) § 120 Rn 70 ff.

840 *Weichert* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) Art 4 Rn 3 f.

841 *Feiler/Forgó*, EU-DSGVO (2017) Art 9 Rn 3; Art 4 Rn 32 f.

schränkt werden kann, weil ohne Stimmprofil jedermann Anfragen an den Digitalen Assistenten richten könnte.[842] Wird die Stimme in einem solchen akustischen Identifikationsverfahren zur Sprechererkennung eingesetzt, liegen folglich auch dann besondere Kategorien personenbezogener Daten vor.[843]

Die Verarbeitung der Sprachbefehle als Audiodateien durch die Nutzer (Beschäftigte) inklusive der Sprecheridentifizierung[844] als erforderliche Maßnahme zur Datensicherheit stützt sich auf die ausdrückliche Einwilligung gemäß ErwGr 51 Satz 3 iVm. Art 9 Abs 2 lit a DSGVO bzw. in Deutschland auf § 26 Abs 2 iVm. Abs 3 Satz 2 BDSG (ErwGr 155 DSGVO). Gemäß Art 4 Nr 11 DSGVO ist eine datenschutzrechtliche Einwilligung eine Erklärung oder eine sonstige als eindeutige bestätigende Handlung abgegebene Willensbekundung, die freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben wird. Die betroffene Person gibt mit einer datenschutzrechtlichen Einwilligung zu verstehen, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.[845] Das online Anklicken einer entsprechend gekennzeichneten Checkbox ist nach *Feiler/Forgó* bspw. bereits als ausdrückliche Einwilligung zu beurteilen.[846] Folglich ist diese ausdrückliche Einwilligung gemäß Art 9 Abs 2 lit a DSGVO in Sprachaufzeichnung bzgl. der aufgezeichneten Stimme vom Arbeitgeber bei den Beschäftigten vor Inbetriebnahme des Digitalen Assistenten als Arbeitsmittel einzuholen und sicher zu archivieren (Art 5 Abs 2 DSGVO). Durch das 2. DSAnpUG-EU wurde nun auch in Deutschland das strenge Schriftlichkeitserfordernis bei der Einwilligung im Arbeitsverhältnis durch eine alternativ mögliche elektronische Einwilligung des Beschäftigten ersetzt (§ 26 Abs 2 Satz 3 BDSG idF. 2. DSAnpUG-EU).[847] Es liegt iZh. mit der Einwilligung zur Sprachaufzeichnung und Sprecheridentifizierung auch Freiwilligkeit vor, weil der Beschäftigte bei nicht Erteilung der Einwilligung zur Sprachaufzeichnung und Sprecheridentifizierung keine Nachteile erleidet, sondern mit dem Digitalen Assistenten dann schlicht nur mit Tastatur kommunizieren kann und damit wie auch bisher in der Bildschirmarbeit tätig sein kann. ErwGr 42 DSGVO definiert: *„Es sollte nur dann davon ausgegangen werden, dass [die betroffene Person] ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.“*[848] Eine Freiwilligkeit bei einer Einwilligung ist dann gegeben, wenn die betroffene Person (Beschäftigter) tatsächlich eine Wahlmöglichkeit hat, also ohne Nachteile auf die Erteilung der Einwilligung verzichten kann.[849] Insofern ist die Einwilligung zur Sprachaufzeichnung mA hier eindeutig freiwillig.

---

842 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten“ (2019) 24; 35.

843 ErwGr 51 Satz 3 iVm. Art 9 Abs 1 DSGVO; *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten“ (2019) 30 f; *Feiler/Forgó*, EU-DSGVO (2017) Art 9 Rn 3.

844 *Feiler/Forgó*, EU-DSGVO (2017) Art 9 Rn 3; Art 4 Rn 32 f.

845 *Art 29 Datenschutzgruppe,* WP 249 (2017) 6 ff.

846 *Feiler/Forgó*, EU-DSGVO (2017) Art 9 Rn 7.

847 BT-Drs. 19/11181, 7 (Beschlussempfehlung Nr. 1 lit b); BGBl. 2019 I. 1626.

848 ErwGr 42 Datenschutz-Grundverordnung (EU) 2016/679.

849 ErwGr 42 Datenschutz-Grundverordnung (EU) 2016/679; *Brodil*, Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 4; *Brodil*, ecolex 2018, 486 ff.

Zu beachten gilt noch, dass sich die Rechtsgrundlage der ausdrücklichen Einwilligung (Art 9 Abs 2 lit a DSGVO; § 26 Abs 2 iVm. Abs 3 Satz 2 BDSG) nur auf die aufgezeichnete Stimme (Sprachverarbeitung = digitale Sprache) des Beschäftigten bezieht. Die Verarbeitung der vom digitalen Assistenten transkribierten und verschriftlichten Inhalte (= reiner digitaler Text) der aufgezeichneten Sprachbefehle, kann sich – wie die sonstige elektronische Kommunikation im Betrieb – mA auf die Rechtsgrundlage Art 6 Abs 1 lit f DSGVO bzw. § 26 Abs 1 Satz 1 BDSG stützen.[850]

Nutzerprofiling und Automatisierte Einzelentscheidungen

Beim Betrieb eines Digitalen Assistenten ist die datenschutzkonforme Erstellung eines Nutzerprofils eines Beschäftigten zu prüfen (siehe **Kapitel 5.2.1**). Das Nutzerprofil ist für die Funktionsfähigkeit des Digitalen Assistenten erforderlich. Beim „Profiling" werden personenbezogenen Daten eines Beschäftigten verarbeitet (Art 4 Nr 4 DSGVO), um bestimmte persönliche Aspekte, die sich auf den Beschäftigten beziehen, mit Hilfe des Digitalen Assistenten zu bewerten, z.B. um Aspekte wie berufliche Schwerpunkte, persönliche Vorlieben, allgemeine Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Ein Digitaler Assistent erstellt ein Nutzerprofil und auf Basis dieses Profils trifft der Digitale Assistent eigenständig Entscheidungen für den Nutzers z.B. in Form von proaktiver Informationsbereitstellung (interessens- und vorliebenbasierte Bereitstellung an den Nutzer); automatisierter Terminplanung (Priorisierung von Terminen nach unterschiedlichen Parametern); Dienstreisebuchungen (Entscheidungen über die Gestaltung der Dienstreise entsprechend vorhandener Kenntnisse über Vorlieben des Nutzer).

Die *Art 29 Datenschutzgruppe* unterscheidet beim Profiling klar zwischen:

- Profiling als reine personenbezogene Datenverarbeitung (ErwGr 72 iVm. Art 6 Abs 1 DSGVO);
- Entscheidungen (mit menschlicher Letztentscheidung), die auf Profiling gestützt werden (ErwGr 72 iVm. Art 6 Abs 1 DSGVO);
- ausschließlich automatisierte Entscheidungen – z.B. auf Profiling gestützt -, die rechtliche Wirkung für Betroffene entfalten oder Betroffene in ähnlicher Weise erheblich beeinträchtigen (ErwGr 72 iVm. Art 6 Abs 1 iVm. Art 22 DSGVO).[851]

Profiling, welches nicht in einer ausschließlich automatisierten Entscheidung mündet, unterliegt nur den allgemeinen Anforderung an eine Datenverarbeitung gemäß den Art 5 ff DSGVO.[852]

Profiling mit anschließender (automatisierter) Entscheidungsfindung beinhaltet drei Stufen wobei auf der letzten Stufe die Anwendung des Art 22 DSGVO zu prüfen ist:

a. *Sammeln der Nutzerdaten zu einem Profil;*

---

850 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten" (2019) 10; 24 ff.

851 *Art 29 Datenschutzgruppe*, WP 251rev.01 (2018) 8 f.

852 ErwGr 72 Datenschutz-Grundverordnung (EU) 2016/679; *Art 29 Datenschutzgruppe*, WP 251rev.01 (2018) 5 ff; *Martini* in Paal/Pauly (Hrsg), DS-GVO BDSG^2 (2018) Art 22 Rn 22.

b. *Modellentwicklung;*

c. *(Automatisierte) Einzelentscheidung.*[853]

a. *Sammeln der Nutzerdaten zu einem Profil:* Das reine Profiling (Art 4 Nr 4 DSGVO) als eine Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass personenbezogene Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, fällt nicht unter die Verbotsregel des Art 22 DSGVO.[854]

Beispielsweise sammelt Apple Inc. im Rahmen des Profilings Informationen über Personen mit welchen der Nutzer Kontakt hatte, das Nutzungsverhalten bei Apps, etc. Aus diesen Informationen kreiert Apple ein Profil, was es Apple ermöglich den Nutzer bei der Erfüllung einer Aufgaben zu unterstützen bspw. um vorherzusagen, welche Informationen ein Nutzer als nächstes brauchen könnte.[855] Apple sichert sich zudem in Verträgen den Zugang zu einem großen Teil der Nutzerdaten. Durch die Kombination der Nutzungsdaten aus zahlreichen Mobilfunknetzen weltweit, kann sich Apple ein genaues Bild über die Gewohnheiten der Anwender machen.[856]

b. *Modellentwicklung:* Mit Hilfe von Machine Learning Algorithmen wird es möglich Korrelationen und persönliche Benutzerattribute herauszufinden. Die Daten werden dabei nicht nur verarbeitet um ein beschreibendes Profil des Nutzers zu erhalten, sondern es erfolgt auch ein Abgleich mit vordefinierten Mustern des durchschnittlichen Verhaltens zahlreicher anderer Personen um daraus weitere Informationen festzustellen, z.B. ob das Profil dem normalen Verhalten entspricht oder davon abweicht und daraus entsprechende Schlüsse ziehen.[857]

c. *(Automatisierte) Einzelentscheidungen:* Letztlich werden auf dieser Informationsbasis dann Entscheidungen getroffen. Die finale Letztentscheidung trifft entweder ein Mensch – unterstützt durch Vorschläge seines Digitalen Assistenten – oder der Digitale Assistent alleine. Fällt die zu treffende Entscheidung final ein Mensch, bleibt es bei der Anwendung der allgemeinen datenschutzrechtlichen Normen (Art 6 DSGVO, § 26 BDSG). Wird die Entscheidung jedoch ausschließlich von einem Computer (Digitaler Assistent), also einer Maschine getroffen, ist die zusätzliche Anwendbarkeit des Art 22 DSGVO zu prüfen:

853 *Kamarinou/Millard/Singh*, Machine Learning with Personal Data (2016) 8 ff.

854 Erwägungsgrund 72 Datenschutz-Grundverordnung (EU) 2016/679; *Kamarinou/Millard/Singh*, Machine Learning with Personal Data (2016) pages 8 ff; *Buchner* in in Kühling/Buchner (Hrsg), DS-GVO BDSG^2 (2018) Art. 22 Rn 38.

855 *Damaschke*, Siri Handbuch (2016) 35.

856 *Schönberger*, Big Data – Die Revolution, die unser Leben verändern wird (2014) 184.

857 *Kamarinou/Millard/Singh*, Machine Learning with Personal Data (2016) 8 ff.

Art 6 Abs 1 lit f DSGVO (EU, Österreich)[858]	**§ 26 Abs 1 Satz 1 BDSG (Deutschland)[859]**
Liegen berechtigte Interessen vor? Effizienzsteigerung durch Automatisierung, bessere Arbeitsergebnisse, etc. durch Digitale Assistenten. *Ist die Verarbeitung zur Verfolung des berechtigten Zwecks erforderlich?* Ohne die Verarbeitung ist der Einsatz eines Digitalen Assistenten nicht möglich. Weniger stark in die Privatssphäre eingreifende Mittel sind nicht möglich. *Abwägung der Interessen, also ob die Grundrechte und Grundfreiheiten oder Interessen des Betroffenen die berechtigten Interessen des Verantwortlichen überwiegen.* Im Rahmen dieser Abwägung überwiegen aufgrund der hohen Eingriffsintensität und Risiken die Interessen des Betroffenen. Ohne weitere Maßnahmen kann eine solche Verarbeitung nicht auf berechtigte Interessen gestützt werden. *Herstellung eines letztendlichen Gleichgewichts der Interessen durch Berücksichtigung zusätzlicher Schutzmaßnahmen (Einsatz von Technologien und Maßnahmen zur Stärkung der Privatssphäre).* Durch entsprechende Maßnahme (z.B. nicht umfassende Profile, sondern nur jeweils Teilaspekte des beruflichen Wirkens des Betroffenen, das Level der Detailliertheit des Profils, Pseudonymisierung, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen und Verschlüsselung der pseudonymen Nutzerprofile, etc.) wird es nach *Art 29 Datenschutzgruppe* möglich ein Gleichgewicht herzustellen, womit die schutzwürdigen Interessen der Betroffenen nicht mehr überwiegen und die Verarbeitung auf Art 6 Abs 1 lit f DSGVO gestützt werden kann.[860]	*Berechtigte Zwecke (Ziele) auf Seiten des Arbeitgebers im Zusammenhang mit der Durchführung des Beschäftigtenverhältnisses?* Effizienzsteigerung durch Automatisierung, bessere Arbeitsergebnisse, etc. durch Digitale Assistenten. *Geeignetheit (Erheblichkeit)* Die Einführung einer Verarbeitungstätigkeit „Digitaler Assistent“ ist geeignet, den angestrebten Zweck zu erreichen und fördert die Zweckerreichung. *Erforderlichkeit im engeren Sinne* Es geht hier darum, ob Maßnahmen gleicher Eignung bestehen anstatt der geplanten. Das ist nicht der Fall, denn für den erfolgreichen Einsatz eines Digitalen Assistenten ist diese Verarbeitung auch im engeren Sinn konkret erforderlich. *Angemessenheit (Verhältnismäßigkeit im engeren Sinn)* Hier erfolgt eine Abwägung der widerstreitenden Interessen. Die eintretende Beeinträchtigung der Persönlichkeitsrechte des Arbeitnehmers darf nicht außer Verhältnis zu dem angestrebten Zweck stehen. Dies wäre bei einem Profiling ohne weitere entsprechende technische und organisatorische Maßnahmen der Fall. Die Interessen der Betroffenen überwiegen hier klar. Durch entsprechende Maßnahme (z.B. nicht umfassende Profile, sondern nur jeweils Teilaspekte des beruflichen Wirkens des Betroffenen, das Level der Detailliertheit, Pseudonymisierung, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen und Verschlüsselung der pseudonymen Nutzerprofile, etc.) wird es nach *Art 29 Datenschutzgruppe* möglich ein Gleichgewicht herzustellen, womit die schutzwürdigen Interessen der Betroffenen nicht mehr überwiegen und die Verarbeitung auf § 26 Abs 1 Satz 1 BDSG gestützt werden kann.[860]

Art 22 Abs 1 DSGVO enthält ein Verbot der automatisierten Einzelentscheidungen (= eine Maschine entscheidet final über Menschen) und ist in der DSGVO als „Recht“ des Betroffenen ausgestaltet. Der Betroffene hat bei Zuwiderhandlung einen Unterlassungsanspruch gegenüber dem Verantwortlichen.[861] Art 22 DSGVO möchte die ungeprüfte Unterwerfung des

858 *Art 29 Datenschutzgruppe,* WP 217 (2014) 70 ff.
859 *Oberthür* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel B Rn 427 f.
860 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 14; *Kroschwald*, Informationelle Selbstbestimmung in der Cloud (2016) 219 ff.
861 *Taeger,* Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017/1, 3 ff.

Individuums unter die alleinige Entscheidung von Maschinen verhindern. Geregelt wird das Verfahren der automatisierten Einzelentscheidung, es wird also vorausgesetzt, dass eine Entscheidung durch eine Maschine getroffen wird. Es muss also ein gestaltender Akt mit abschließender Wirkung vorliegen.[862] Automatisierte Vorentscheidungen (Vorauswahl) vor der eigentlichen finalen Entscheidung sind grundsätzlich nicht von Art 22 DSGVO erfasst.[863] Art 22 Abs 1 DSGVO befasst sich – wie seine Vorgängerbestimmung Art 15 EG-Datenschutzrichtlinie 95/46/EG und deren nationale Umsetzungen in § 6a BDSG aF in Deutschland bzw. § 49 DSG 2000 aF in Österreich – also nicht mit der Frage, ob personenbezogene Daten, die zur Bewertung einer Person beitragen können, überhaupt verarbeitet werden dürfen (Rechtsgrundlage; ErwGr 72), sondern allein mit automatisierten Entscheidungen selbst, welche – auf solchen bereits als rechtmäßig eingestuften Verarbeitungen – gestützt werden sollen (Nutzung bestimmter Ergebnisse einer Datenverarbeitung).[864] Durch Art 22 DSGVO wird die Nutzung von rein maschinellen Ergebnisse einer automatisierten Datenverarbeitung einer Reihe von Voraussetzungen und Einschränkungen unterworfen in Form von zusätzlichen Rechtmäßigkeitsvoraussetzungen für die Entscheidungsfällung, die zu den allgemeinen Regelungen zur Rechtmäßigkeit einer Datenverarbeitung hinzutreten.[865]

Die Voraussetzungen, dass Art 22 Abs 1 DSGVO greift, sind:

- Vorliegen einer auf einer Verarbeitung personenbezogener Daten – einschließlich Profiling – beruhenden ausschließlich automatisierten Entscheidung;
- diese ausschließlich automatisierte Entscheidung entfaltet gegenüber dem Betroffenen rechtliche Wirkung; oder
- diese ausschließlich automatisierte Entscheidung beeinträchtigt den Betroffenen erheblich in ähnlicher Weise wie eine Entscheidung mit rechtlicher Wirkung.

Eine Erlaubnis zu einer solchen rein automatisierten Einzelentscheidung besteht nur dann, wenn diese automatisierte Einzelentscheidung (Art 22 Abs 2 DSGVO):

- für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist;
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten mit geeigneten Garantien vorgesehen wird; oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Keine automatisierte Einzelentscheidung im Sinne des Art 22 Abs 1 DSGVO liegt vor, wenn die Entscheidung nur teilweise oder nur überwiegend auf eine maschinelle Bewertung zurückgeht, weil es sich damit nicht um eine ausschließlich automatisierte Entscheidung handelt. Bloße Vorentscheidungen, Vorauswahlen, etc., wo ein Mensch die Letztentscheidung trifft und damit vom maschinellen Vorschlag abweichen kann, fallen nicht unter Art

862 *von Lewinski* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019) Art 22 Rn 1 ff.

863 BT-Drs 14/4329, 37.

864 *von Lewinski* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] [aF] (Stand: 01.05.2018) § 6a BDSG 2003 [aF] Rn 1 f; *Scholz* in Simitis (Hrgs), Bundesdatenschutzgesetz[8] (2014) § 6a Rn 4; *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 8/66 ff; *Art 29 Datenschutzgruppe*, WP 251rev.01 (2018) 5 ff; *Schulz* in Gola (Hrsg), DS-GVO[2] (2018) Art 22 Rn 3 f.

865 *Buchner* in Kühling/Buchner (Hrsg), DSGVO BDSG[2] (2018) Art 22 Rn 11 f; Rn 23.

22 Abs 1 DSGVO. Dies setzt allerdings als menschlichen Letztentscheider eine Person voraus, die mit entsprechender Entscheidungskompetenz ausgestattet und instruiert ist und die Intervention der natürlichen Person vor der Entscheidungsfindung erfolgt. Damit fällt das bloße Berechnen einer Wahrscheinlichkeit oder das Ergebnis einer Suchmaschine nicht unter Art 22 Abs 1 DSGVO.[866] Voraussetzung ist allerdings, dass die natürliche Person auch tatsächlich Einfluss auf die finale Entscheidung nehmen kann. Liegt keine Kompetenz vor, eine Computerentscheidung durch menschliches Eingreifen der natürlichen Person zu beeinflussen, liegt trotz Einbindung eines Menschen weiterhin eine automatisierte Entscheidung iSd. Art 22 Abs 1 DSGVO vor.[867] Das heißt, eine ausschließlich automatisierte Entscheidung z.B. über einen Beschäftigten liegt immer dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person mehr stattfindet.[868]

Beim Einsatz eines Digitalen Assistenten am Arbeitsplatz z.B. mit pseudonymen Nutzerprofilen findet einerseits ein pseudonymes Profiling der betrieblichen Vorlieben und Tätigkeiten des Beschäftigten durch den Digitalen Assistenten statt (Art 4 Nr 4 DSGVO). Auf Basis dieses Profiling fällt der Assistent gestützt auf künstliche Intelligenz seine Entscheidungen für den Nutzer. Diese automatisierten Entscheidungen in Form von Vorschlägen, die der Digitale Assistent für den Nutzer produziert (z.B. „Informationssuche und proaktive Informationsbereitstellung"; „Enterprise Helpdesk EHD Funktionalitäten"; „Sprach- und Textschnittstelle"; „Kommunikation mit Personen", „Mehrsprachenunterstützung"; etc.), sind nicht in der Art und Weise, dass sie dem betroffenen Beschäftigten gegenüber rechtliche Wirkung entfalten würden oder in ähnlicher Weise den Betroffenen als Beschäftigten erheblich beeinträchtigen würden. Damit scheidet die Anwendung des Art 22 Abs 1 DSGVO für solche Funktionalitäten eines Digitalen Assistenten aus. Es bleibt bei der Anwendung der allgemeinen datenschutzrechtlichen Grundlagen (Art 5 ff DSGVO, § 26 BDSG).[869]

Hinsichtlich der Funktionalitäten der „Dienstreisebuchungen" und „automatisierten Terminplanung" ist die Anwendung des Art 22 DSGVO im Einzelfall zu prüfen. Führt der Digitale Assistent nur die entsprechende Buchung für den Nutzer durch (Reise nach Amsterdam mit Flug um 12:00 Uhr) bzw. erstellt – in automatisiertem Abgleich diverser Terminkalender – automatisiert Besprechungstermine, ist ebenfalls keine Anwendbarkeit des Art 22 DSGVO gegeben. Fließen im Rahmen der „Dienstreisebuchung" bzw. der „Terminplanerstellung" jedoch noch andere Parameter ein, sodass der Beschäftigte dadurch Nachteile erleidet, wäre Art 22 DSGVO ggf. anwendbar. Mögliche erhebliche Beeinträchtigungen durch die automatisierten Entscheidungen des Digitalen Assistenten wären bspw. starke Reiseunannehmlichkeiten aufgrund einer automatisiert gefällten Kostenentscheidung, gestützt auf die niedrige Stellung des Beschäftigten im Unternehmen; oder, der Beschäftigte bekommt aus denselben Gründen der niedrigen Stellung im Unternehmen vom Digitalen Assistenten defacto keine Termine bei seinen Vorgesetzten eingestellt, mit damit verbundenen erheblichen Beeinträchtigungen im beruflichen Fortkommen für den Beschäftigten.

866 *Schulz* in Gola (Hrsg), DS-GVO[2] (2018) Art 22 Rn 12 ff; BT-Drs 14/4329, 37.
867 *Art 29 Datenschutzgruppe*, WP 251rev.01 (2018) 20 f.
868 BT-Drs 16/10529, 13.
869 *Art 29 Datenschutzgruppe*, WP 251rev.01 (2018) 19 ff.

Der Betrieb des Digitalen Assistenten wäre – wenn in die Entscheidung potentiell diskriminierende Parameter (niedrige berufliche Stellung) einfließen sollten – dann nur unter der Voraussetzung des Art 22 Abs 2 lit c DSGVO (ausdrückliche Einwilligung der Beschäftigten) erlaubt.

Soll der Digitale Assistent jedoch lediglich Unterstützungsleistungen (z.B. „automatisierte profilbasierte Informationssuche und proaktive Informationsbereitstellung"; „Enterprise Helpdesk EHD Funktionalitäten"; „Sprach- und Textschnittstelle"; etc.) erbringen, ist Art 22 DSGVO nicht anwendbar und es bleibt bei der alleinigen Prüfung der Verarbeitung anhand der Art 5 ff DSGVO. Hintergrund ist, dass das Profiling als auch die darauf gestützte automatisierte Entscheidungsfindung durch den Digitalen Assistenten nicht in der Form stattfindet, dass sie gegenüber dem betroffenen Beschäftigten eine rechtliche Wirkung entfalten und sie die Beschäftigten auch nicht in ähnlicher Weise erheblich beeinträchtigen.

Eine anderweitige arbeitsrechtliche Einsicht in das Nutzerprofil des Digitalen Assistenten über den Beschäftigten, abseits des Betriebs des Digitalen Assistenten, z.B. zur Leistungskontrolle durch den Arbeitgeber oder Big Data „People Analytics", lässt sich ohne informierte Einwilligung nicht begründen, denn es stellt einen äußerst schweren Eingriff in das Persönlichkeitsrecht dar, wodurch in der Regel eine Unzulässigkeit vorliegt.[870]

Es ergibt sich folgendes Ergebnis:

- Wird der Digitale Assistent so ausgestaltet, dass ein personenbezogenes Nutzerprofil erstellt wird und zugleich vom Digitalen Assistenten automatisierte Einzelentscheidungen gefällt werden, die den betroffenen Beschäftigten gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, darf ein Betrieb nur nach ausdrücklicher informierter Einwilligung (Art 6 Abs 1 lit a DSGVO bzw. § 26 Abs 2 BDSG iVm. Art 22 Abs 1 lit c DSGVO) erfolgen. Hier stellen sich Fragen hinsichtlich der Freiwilligkeit von datenschutzrechtlichen Einwilligungen im Arbeitsverhältnis womit ein rechtssicherer Betrieb nicht immer gewährleistbar wäre.
- Ist Art 22 DSGVO nicht anwendbar, weil der Digitale Assistent nur Vorschläge erstellt, aber keine maschinellen Letztentscheidungen trifft und erfolgt das Profiling der Beschäftigten durch den Digitalen Assistenten ausschließlich in pseudonymer Form am Stand der Technik mit geringer Eingriffsintensität, d.h. es werden nur Teilaspekte des Arbeitslebens (und keinesfalls im Rahmen privater Nutzung – Abschaltbarkeit) erfasst und es wird eine verschlüsselte Speicherung des pseudonymen Profils vorgenommen, ergibt sich mA eine Erlaubnis zum Betrieb auch aus Art 6 Abs 1 lit f DSGVO bzw. in Deutschland gemäß § 26 Abs 1 Satz 1 BDSG.[871]

Cloud Computing

Überblick:

Wichtig für die Rechtmäßigkeit ist beim Cloud Computing vorab die korrekte datenschutzrechtliche Rolle (Verantwortlicher, Auftragsverarbeiter) jedes einzelnen Akteurs im Rahmen des Cloud Computings zu definieren. Die Sprachbefehle und das (pseudonyme) Nutzerprofil werden in der Cloud (verschlüsselt) gespeichert. Zudem befindet sich, vereinfacht

870 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 299 ff.
871 *Art 29 Datenschutzgruppe*, WP 251rev.01 (2018) 14 f.

dargestellt, der digitale Assistent selbst – also die dbzgl. Software – in der Cloud. Wird ein Digitaler Assistent als komplette Software verwendet, liegt SaaS vor. Ist es noch möglich selbst bestimmte Services einzubinden, liegt entweder PaaS oder IaaS vor (siehe **Kapitel 5.2.2**). Das Cloud Computing besteht aus einer Reihe von Technologien und Service Modellen, die sich auf eine internetbasierte Nutzung und Lieferung von IT-Anwendungen, auf die Verarbeitungsfähigkeit, die Aufbewahrung und den Speicherplatz konzentrieren (siehe **Kapitel 5.2.2**).[872]

- *Private Cloud*

Erfolgt ein Cloud Computing im Rahmen einer Private Cloud, ermöglicht das Unternehmen die interne Nutzung eigener Rechenzentren auf Basis des Cloud Computing, ist Verantwortlicher iSd. Art 4 Nr 7 DSGVO allein das Unternehmen (Arbeitgeber) selbst.[873]

- *Hybrid Cloud Architektur*

Liegt eine Hybrid Cloud Architektur vor (Private Cloud und Public Cloud) ist das Unternehmen (Public Cloud Anwender) und zugleich Private Cloud Betreiber und in beiden Fällen Verantwortlicher (Art 4 Nr 7 DSGVO). Der Public Cloud Anbieter, der nur herangezogen wird für Lastspitzen und damit für rein technische Dienstleistungen ohne jede Form des Entscheidungsbefugnis über Zwecke oder wesentliche Aspekte der Mittel, ist mangels einer solchen nur reiner Auftragsverarbeiter (Art 4 Nr 8 DSGVO).[874]

- *Public Cloud Konstellationen*

In reinen Public Cloud Konstellationen ist die Definition der datenschutzrechtlichen Rolle deutlich schwieriger, denn es liegt ggf. nicht in jedem Fall eine Auftragsverarbeitung vor[875]:

Im klassischen Fall legt der Cloud Anwender (Arbeitgeber) die Zwecke der Verarbeitung fest und entscheidet über die Auslagerung der Verarbeitung in die Cloud auch die wesentlichen Aspekte der Mittel. Damit ist der Cloud Anwender datenschutzrechtlich Verantwortlicher (Art 4 Nr 7 DSGVO). Der Cloud Anbieter ist Auftragsverarbeiter (Art 4 Nr 8 DSGVO), da dieser nur eine rein technische Dienstleistungen ohne jede Form der Entscheidungsbefugnis über Zwecke oder wesentliche Aspekte der Mittel erbringt. Der Cloud Anwender (Verantwortliche) kann den Cloud Anbieter damit beauftragen, die konkreten technischen oder organisatorischen Maßnahmen für das Erreichen der Zwecke des Verantwortlichen auszuwählen.[876] Liegt diese Konstellation vor, ist ein Vertrag zur Auftragsverarbeitung gemäß Art 28 DSGVO (siehe **Kapitel 3.6.3**) abzuschließen mit dem ge-

872 *Art 29 Datenschutzgruppe*, WP 196 (2012) 5; *Böhm/Wybitul*, Arbeitnehmerdaten in der Cloud, ArbRAktuell 2015, 539.

873 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 209 ff.

874 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 209 ff.

875 *Art 29 Datenschutzgruppe*, WP 196 (2012) 10; *Düsseldorfer Kreis*, Orientierungshilfe Cloud Computing (2014) 9 ff; *Kroschwald,* Informationelle Selbstbestimmung in der Cloud (2016) 120 ff; *Kroschwald,* Kollektive Verantwortung für den Datenschutz in der Cloud, ZD 2013, 388; *Hofmann*, Anforderungen aus DS-GVO und NIS-RL an das Cloud Computing, ZD-Aktuell 2017, 05488; *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 185 ff; *Weichert*, Cloud Computing und Datenschutz, DuD 2010, 679 (682 ff); *Art 29 Datenschutzgruppe*, WP 169 (2010) 16.

876 *Art 29 Datenschutzgruppe*, WP 196 (2012) 10.

setzlich erforderlichen Inhalt. Die Rechtmäßigkeit der Verarbeitung des Auftragsverarbeiters beim Cloud Computing wird durch den vom Verantwortlichen erteilten Auftrag bestimmt (Art 28 DSGVO).[877]

Es kann jedoch Cloud-Lösungen geben, wo der Cloud Anbieter selbst zum Verantwortlichen (Art 4 Nr 7 DSGVO) wird mit den entsprechenden datenschutzrechtlichen Konsequenzen. Dies geschieht in folgenden Situationen:

Eigenmächtige Datenverarbeitung durch den Cloud Anbieter:

Der Cloud Anbieter verarbeitet die vom Cloud Anwender bereitgestellten Daten zusätzlich rechtswidrig zu eigenen Zwecken (Art 28 Abs 10 DSGVO).[878] Die *Art 29 Datenschutzgruppe* hebt hervor, dass sie das Risiko als äußerst hoch ansieht, dass beim Cloud Computing personenbezogene Daten von den diversen Auftrags- und Unterauftragsverarbeitern zu nicht vereinbarten Zwecken weiterverarbeitet werden.[879]

Ausübung tatsächlicher Kontrolle durch den Cloud Anbieter:

Die rein formelle Betrachtungsweise zwischen Verantwortlichem als Cloud Anwender (Art 4 Nr 7 DSGVO) und Auftragsverarbeiter als Cloud Anbieter (Art 4 Nr 8 DSGVO) kann bei bestimmten Cloud Lösungen nicht mit der tatsächlich vorliegenden Umständen der Realität übereinstimmen. Dies kann bei Cloud Lösungen der Fall sein, wenn einer Stelle formal die Rolle des Verantwortlichen zugewiesen wird, obwohl sie Daten faktisch gar nicht mehr „kontrolliert" bzw. „kontrollieren" kann („Controller"). Aus der Definition des Verantwortlichen gemäß Art 4 Nr 7 DSGVO zeigt sich, dass der Verantwortliche zu jedem Zeitpunkt der Datenverarbeitungsvorgänge einen hohen Grad an Einfluss auf die Datenverarbeitungsvorgänge ausüben muss. Das heißt, der Verantwortliche muss die faktische Entscheidungskompetenz über Zwecke und wesentliche Aspekte Mittel der Verarbeitung haben, die Ziele und Zwecke sowie die wesentlichen technischen und organisatorischen Aspekte determinieren können.[880] Folglich ist der Verantwortliche auf Grundlage einer Analyse der Fakten und nicht auf Basis eines rein formellen Ansatzes zu bestimmen. Wenn die Kontrolle über die Verwendung der Daten, die sich beim Cloud Anbieter befinden, von dem Verantwortlichem nicht mehr sichergestellt werden kann, sondern der Cloud Anbieter selbstständig maßgeblich über die Datenverarbeitung entscheiden kann, rückt auch der Cloud Anbieter in die Rolle des Verantwortlichen (Art 4 Nr 7 DSGVO). Es handelt sich um einen funktionellen Ansatz zur Bestimmung der datenschutzrechtlichen Rolle.[881] Entscheidendes Merkmal für das Vorliegen einer reinen Auftragsverarbeitung beim Cloud Provider

877 *Art 29 Datenschutzgruppe*, WP 169 (2010) 31.

878 *Art 29 Datenschutzgruppe*, WP 196 (2012) 10 ff; 24; *Art 29 Datenschutzgruppe*, WP 169 (2010) 31; *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 185 ff; *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 17.

879 *Art 29 Datenschutzgruppe*, WP 196 (2012) 14; *Jotzo*, Der Schutz personenbezogener Daten in der Cloud (2012) 83 ff.

880 *Art 29 Datenschutzgruppe*, WP 196 (2012) 10 f; *Kroschwald*, ZD 2013, 388 (390 ff.); *Kroschwald*, Informationelle Selbstbestimmung in der Cloud (2016) 120 ff; *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 185 ff; 195 ff; *Weichert*, DuD 2010, 679 (682 ff); *Jotzo*, Der Schutz personenbezogener Daten in der Cloud (2012) 73 ff.

881 *Art 29 Datenschutzgruppe*, WP 169 (2010) 33.

ist also, dass der jederzeitige Zugriff des Cloud Anwenders auf die Daten besteht und gewährleistet ist und Daten nicht ohne sein Wissen und ohne weiteres in Staaten ohne angemessenem Datenschutzniveau gelangen. Wird also sichergestellt, dass die Daten im Anwendungsbereich der DSGVO bleiben und dort jederzeit für den Verantwortlichen verfügbar sind, ist der Kontrollgrad des Cloud Anwenders als Verantwortlicher als hoch zu bewerten, sodass die formelle Bestimmung der datenschutzrechtlichen Rollen auch der der Realität entspricht.[882] Dies ist aber nicht immer der Fall.

Zwei Beispiele:

Rollenproblematik in Federated Cloud Architekturen („Single Point of Contact"):

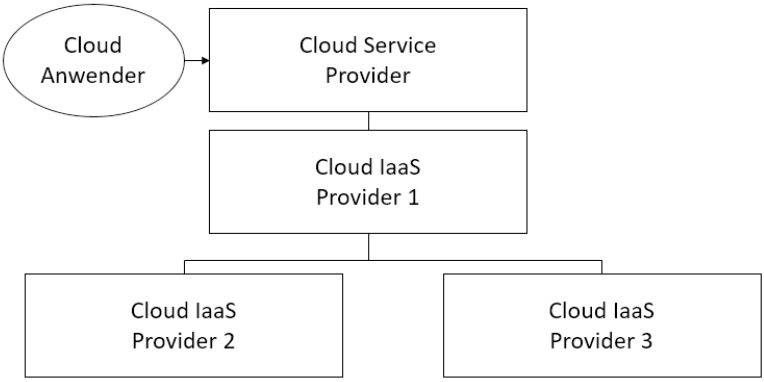


Abbildung 6: *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 197 - Federated Cloud Architekturen („Single Point of Contact").

In einer Federated Cloud („Single Point of Contact") nimmt der Cloud Anwender einen Cloud Anbieter (z.B. SaaS Cloud Anbieter) in Anspruch, der selbst wieder die Infrastruktur eines anderen IaaS Cloud Providers nutzt. In dieser Konstellation sind also neben dem Cloud Anwender (Verantwortlicher) mehrere weitere Cloud Provider beteiligt, wobei der erste SaaS Cloud Anbieter entscheidet, welche zusätzlichen IaaS Cloud Provider er nutzen will. Der Cloud Anwender (Verantwortlicher) selbst hat nur einen Vertrag mit dem ersten SaaS Cloud Anbieter. Der SaaS Anbieter hat ebenso nur einen Vertrag mit dem ihm unmittelbar nachgeschaltetem IaaS Anbieter. Mit wie vielen weiteren Anbietern der nachgeschaltene IaaS Provider in Kooperation ist, ist beiden ggf. unbekannt. Insofern treten die jeweiligen Vertragspartner zueinander in Form von Generalunternehmen auf, die die verschiedenen Leistungen gemeinsam mit dem anderen erbringen. Nach *Barnitzke* handelt es sich in dieser Situation beim SaaS Cloud Provider um einen klassischen Auftragsverarbeiter, weil sich an den Entscheidungsbefugnissen hinsichtlich Zwecke und Mittel nichts

882 *Hofmann,* ZD-Aktuell 2017, 05488; *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 185 ff; 195 ff; *Kroschwald*, ZD 2013, 388 (390 ff.); *Kroschwald*, Informationelle Selbstbestimmung in der Cloud (2016) 120 ff; *Art 29 Datenschutzgruppe*, WP 196 (2012) 10 f; *Weichert*, DuD 2010, 679 (682 ff).

ändert. Bei den nachgeschalteten IaaS Cloud Providern sehe die Lage differenzierter aus[883]: Der vom SaaS Provider ausgewählte erste IaaS Cloud Provider entscheidet zwar nicht über die konkreten Zwecke der Verarbeitung (iSv. Zweckidentität), nach Auffassung des EuGH ist es aber bereits ausreichend, dass eine natürliche oder juristische Person aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt. Es ist dabei auf jedes mittelbare oder unmittelbare Ziel der Datenverarbeitung abzustellen, es genüge ein adäquatkausaler Beitrag zur Datenverarbeitung.[884] Nach dieser EuGH Rechtsprechung wird insofern bereits eine Einheit der Zwecke (z.B. gemeinsame „wirtschaftliche Interessen") als ausreichend angesehen. Der EuGH fordert hingegen keine Identität der von den beteiligten Akteuren jeweils verfolgten Zwecke.[885] Hinsichtlich der Mittel entscheidet der erste IaaS Cloud Provider weitgehend allein über die technischen Mittel der Verarbeitung, insbesondere ob weitere IaaS Cloud Provider hinzugezogen werden. Problematisch ist hier, dass der erste IaaS Provider alleine über die Zugangsberechtigungen zu den Daten, den Ort ihrer Verarbeitung und die Speicherdauer der Daten entscheidet. Dies wäre jedoch eigentlich dem datenschutzrechtlich Verantwortlichem vorbehalten. Es hängt insofern in Federated Cloud Architekturen von der faktischen Ausübung der tatsächlichen Kontrolle ab. Entscheidet der IaaS Cloud Provider alleine und unabhängig nach vorheriger Konsultation hinsichtlich der Einschaltung weiterer IaaS Cloud Provider als seine Subdienstleister, können weder der Cloud Anwender noch der mit dem Cloud Anwender in einem Vertragsverhältnis stehenden SaaS Cloud Anbieter als erster Auftragsverarbeiter die Datenverarbeitung faktisch kontrollieren („Controller"). Ohne eine solche Kontrollmöglichkeit mangelt es an der erforderlichen Einflussfähigkeit, die die DSGVO für einen alleinigen „Controller" voraussetzt. Insofern könnte ein gemeinsames Entscheiden über die Mittel im Cloud Computing vorliegen, denn es besteht eine stark verringerte faktische Kontrollmöglichkeit für den Verantwortlichen (Cloud Anwender).[886] Nach der neuesten Rechtsprechung des EuGH ist jede Phase einer Datenverarbeitung (z.B. „erheben", „speichern", „auslesen", „übermitteln", „löschen", etc.) im konkreten Einzelfall unter Berücksichtigung aller maßgeblichen Umstände hinsichtlich einer gemeinsamen Entscheidung über Zwecke (keine Zweckidentität erforderlich, es reicht eine schlichte Einheit der Zwecke wie bspw. gemeinsame „wirtschaftliche Interessen") und Mittel (gemeinsame Entscheidung über die eingesetzten Mittel) durch die jeweils beteiligten Akteure zu prüfen und dann die konkrete (ggf. gemeinsame) Verantwortlichkeit pro Verarbeitungsphase festzustellen.[887] *Barnitzke* sieht die Rollen in Federated Cloud Architekturen in der Variante „Single Point of Contact" wie folgt:

---

883 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 196 ff.

884 *Specht-Riemenschneider/Schneider*, Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, 503 (505); EuGH Urteil v. 10.7.2018, C-25/17 Rn 68 ff.

885 EuGH Urteil v. 29.07.2019, C-40/17 Rn 80 ff: als Einheit der Zwecke gelten gemäß EuGH Urteil bereits gemeinsame „wirtschaftliche Interessen"; EuGH GA v. 19.12.2018, C-40/17 Rn 104 f: der Generalanwalt des EuGH stellt auf „kommerzielle und werbliche Zwecke" bei der Einheit der Zwecke ab; EuGH Urteil v. 10.07.2018, C-25/17 Rn 68 ff: „Eigeninteresse auf die Verarbeitung personenbezogener Daten" (Rn 68).

886 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 196 ff; *Jotzo*, Der Schutz personenbezogener Daten in der Cloud (2012) 81 ff; EuGH Urteil v. 29.07.2019, C-40/17 Rn 70 ff.

887 EuGH Urteil v. 29.07.2019, C-40/17 Rn 70 ff; EuGH GA v. 19.12.2018, C-40/17 Rn 104 f.

- Erster SaaS Cloud Provider als Vertragspartner des Cloud Anwenders (Verantwortlichen) ist klassischer Auftragsverarbeiter (Art 4 Nr 8 DSGVO).
- Erster IaaS Cloud Provider in Federated Cloud Architekturen ist, sobald dieser die wesentlichen Aspekte der Mittel der Datenverarbeitung faktisch eigenständig entscheiden darf (Zugangsberechtigungen zu den Daten, den Ort ihrer Verarbeitung und die Speicherdauer) und eine Einheit der Zwecke (z.B. gemeinsame „wirtschaftliche Interessen") objektiv vorliegt, Verantwortlicher (Art 4 Nr 7 DSGVO). Insofern wäre dann zwischen dem ersten IaaS Cloud Provider und dem Cloud Anwender ein Joint-Controller Vertrag (Art 26 Abs 1 Satz 2 DSGVO) abzuschließen.
- Die weiteren nach dem ersten IaaS Cloud Provider hinzugezogenen IaaS Cloud Provider sind idR Subauftragsverarbeiter iSd. Art 4 Nr 8 iVm. Art 28 Abs 4 DSGVO.[888]

Rollenproblematik in Federated Cloud Architekturen („Multivendor" – Strategie):

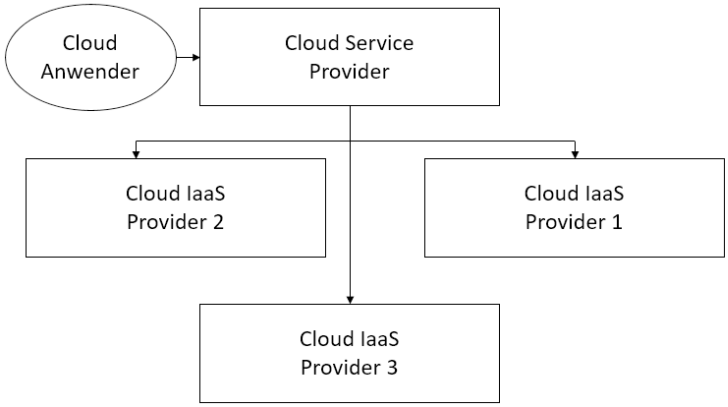


Abbildung 7: *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 203 - Federated Cloud Architekturen („Multivendor" – Strategie).

Im Unterschied zu Federated Cloud Architekturen mit „Single Point of Contact" (siehe oben), liegt bei einer „Mulitvendor"-Strategie der Fall vor, dass der SaaS Cloud Provider als Cloud Anbieter und Vertragspartner des Cloud Anwenders (Verantwortlicher) sich gleich mehrerer IaaS Cloud Provider bedient. Der SaaS Cloud Service Provider als Vertragspartner des Cloud Anwenders (Verantwortlicher) überwacht hier die Auswahl der geeigneten IaaS Cloud Provider und geht mit mehreren IaaS Cloud Provider eine vertragliche Beziehung ein. In dieser Konstellation hat der SaaS Cloud Provider (Vertragspartner des Cloud Anwenders) deutlich mehr Einfluss. Das liegt darin, dass er selbstständig über den Einsatz der diversen IaaS Cloud Provider entscheidet. Der SaaS Cloud Provider hat zwar weiterhin keinen besonderen Einfluss auf die Zwecke der Verarbeitung des Verantwortlichen, es könnte aber in bestimmten Verarbeitungsphasen durchaus eine Einheit der jeweils

888 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 201 ff; EuGH Urteil v. 29.07.2019, C-40/17; EuGH GA v. 19.12.2018, C-40/17; EuGH Urteil v. 10.07.2018, C-25/17.

verfolgten Zwecke vorliegen („wirtschaftliche Interessen"; „kommerzielle Zwecke"; „Eigeninteressen"[889]). Der Einfluss auf die technischen Mittel der Verarbeitung ist zudem erheblich. Es ist im Einzelfall zu prüfen, ob der Einfluss des SaaS Cloud Providers in Federated Cloud Architekturen mit „Mulitvendor"-Strategie das Level erreicht, dass man davon sprechen kann, dass der SaaS Cloud Provider über wesentliche Aspekte der Mittel der Datenverarbeitung entscheidet (Zugangsberechtigungen zu den Daten, den Ort ihrer Verarbeitung und die Speicherdauer). Der SaaS Cloud Provider als Vertragspartner des Cloud Anwenders verfügt hier über erhebliche Einflussmöglichkeiten auf die Datenverarbeitung (hohe Intensität der faktischen Kontrolle). In diesem Fall würde – eine gewisse Einheit der verfolgten Zwecke vorausgesetzt (EuGH: gemeinsame „wirtschaftliche Interessen") – der SaaS Cloud Provider zum datenschutzrechtlichen Verantwortlichen, womit eine gemeinsame Verantwortlichkeit dann vorliegen könnte. Es wäre dann für die Verarbeitungsphasen der gemeinsamen Verantwortlichkeit ein Joint Controller Vertrag gemäß Art 26 Abs 1 Satz 2 DSGVO abzuschließen. Die nachgeschalteten IaaS Cloud Provider sind in Federated Cloud Architekturen mit „Mulitvendor"-Strategie aufgrund der viel geringen Einfluss- und Entscheidungsmöglichkeiten in der Regel als reine (Sub-)Auftragsverarbeiter anzusehen (Art 4 Nr 8 iVm. Art 28 Abs 4 DSGVO).[890]

Ergebnis:

- Mit als Auftragsverarbeiter (Art 4 Nr 8 DSGVO) identifizierten Cloud Providern (SaaS, IaaS) sind Verträge gemäß Art 28 DSGVO (**Kapitel 3.6.3**) abzuschließen. [891]
- Für Cloud Provider, die als Verantwortliche (Art 4 Nr 7 DSGVO) identifiziert wurden, bedarf es für die Übermittlung der Daten einer Rechtsgrundlage (Art 6 Abs 1 lit f DSGVO, § 26 Abs 1 BDSG) und des Abschlusses eines Joint Controller Vertrages gemäß Art 26 Abs 1 Satz 2 DSGVO (siehe **Kapitel 3.6.5**).[892]

Es ist also eine detaillierte datenschutzrechtliche Analyse der angebotenen Cloud Konzepte erforderlich. Während für die meisten Cloud Konstellationen die Privilegierung nach Art 28 DSGVO als Auftragsverarbeitung greift, ist dies bei einigen Cloud Konstellationen nicht der Fall und es kommt zu einer rechtfertigungsbedürtigen Datenübermittlung.[893]

Ergebnis einer Rechtmäßigkeit aus Straf- und Datenschutzsicht

- Für die *Sprachsteuerung* und die damit verbundene Verareitung von Audiodateien inkl. Sprecherindentifikation zum Zweck der Datensicherheit ergibt sich aufgrund der parallelen strafrechtlichen Voraussetzungen (§ 201 dStGB; § 120 öStGB) nur die ausdrückliche informierte Einwilligung gemäß Art 9 Abs 2 lit a DSGVO bzw. § 26 Abs 2 BDSG.

889 EuGH Urteil v. 29.07.2019, C-40/17 Rn 80 ff; EuGH GA v. 19.12.2018, C-40/17 Rn 104 f; EuGH Urteil v. 10.07.2018, C-25/17 Rn 68 ff.

890 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 202 ff.

891 *Art 29 Datenschutzgruppe*, WP 169 (2010) 31.

892 EuGH Urteil v. 29.07.2019, C-40/17 Rn 70 ff; EuGH Urteil v. 10.07.2018, C-25/17 Rn 68 ff; *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 213; *Kroschwald,* ZD 2013, 388 (390 ff.); *Jotzo*, Der Schutz personenbezogener Daten in der Cloud (2012) 81 ff; *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 17 letzer Satz.

893 *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 214; 248 ff.

Wird dem Beschäftigten als Nutzer auch eine Alternative zur Sprachsteuerung angeboten (Tastatur), liegt Freiwilligkeit der Einwilligung hinsichtlich der Erhebung und Verarbeitung der Audiodateien im Rahmen der Sprachsteuerung vor.[894]

- Für das *Nutzerprofiling* im Rahmen des Betriebs des Digitalen Assistenten kommt aufgrund der hohen Eingriffsintensität grundsätzlich ebenso nur eine informierte Einwilligung (Art 6 Abs 1 lit a DSGVO bzw. § 26 Abs 2 BDSG) in Betracht. Trifft der Verantwortliche aber geeigente technische und organisatorische Maßnahmen (Verschlüsselung und effektive Pseudonymisierung, Proflings nur zu tatsächlich erforderlichen Teilaspekten der beruflichen Tätigkeit und nicht in jeder Situation und keinesfalls hinsichtlich privater Aspekte; sichergestellt durch entsprechende technische und organisatorische Maßnahmen – Abschaltbarkeit des Digitalen Assistenten), kann dadurch die Eingriffsintensität gesenkt werden und bei einem begründbaren berechtigten Interesse des Arbeitgebers (Art 6 Abs 1 lit f DSGVO) bzw. einer konkreten Erforderlichkeit (§ 26 Abs 1 Satz 1 BDSG) für das Beschäftigtenverhältnis (höhere Wirtschaftlichkeit, schnellere Suchergebnisse, bessere Arbeitsergebnisse) kann sich dann die Verarbeitung auch auf eine solche Rechtsgrundlage abseits der Einwilligung stützen.[895] Zu beachten ist, dass wenn der Digitale Assistent diese Voraussetzungen sicherstellt und damit nicht über die Einwilligung des Beschäftigten gerechtfertigt wird, der Einsatz des Digitalen Assistenten über das Direktionsrecht des Arbeitgebers erfolgt, in dessen Rahmen der Arbeitgeber die Arbeitsmittel vorgibt. Trotzdem muss der Beschäftigte die Möglichkeit haben, seine Entscheidungsfreiheit auszuüben, also in die Datenverarbeitungsvorgänge des Digitalen Assistenten einzugreifen und im Einzelfall abzubrechen bzw. abzuschalten, z.B. wenn der Beschäftigte zu privaten Zwecken etwas machen möchte. Das heißt die Entscheidungsfreiheit des Beschäftigten darf – trotz des Direktionsrechts des Arbeitgebers – nicht durch softwaretechnische Sachzwänge vollständig ausgeschlossen sein. Diese Selbstbestimmung muss durch den Digitalen Assistenten (jederzeitige Abschaltbarkeit durch den Beschäftigten) sichergestellt sein.[896]
- Beim *Cloud-Computing* liegt grundsätzlich Auftragsverarbeitung vor (Art 28 DSGVO Auftragsverarbeitungsvertrag). Trifft der Cloud Provider Entscheidungen über wesentliche Aspekte der Mittel der Verarbeitung und liegt eine gewisse Einheit der Zwecke mit dem Cloud Anwender vor, wird auch der Cloud Provider zum Verantwortlichen. In einem solchen Fall ist ein Joint Controller-Vertrag gemäß Art 26 Abs 1 Satz 2 DSGVO mit dem Cloud Anwender abzuschließen.[897]

894 ErwGr 42 Datenschutz-Grundverordnung (EU) 2016/679; *Brodil*, Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 4; *Brodil*, ecolex 2018, 486 ff.

895 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 14; *Kroschwald*, Informationelle Selbstbestimmung in der Cloud (2016) 219 ff.

896 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 325 f.

897 EuGH Urteil v. 29.07.2019, C-40/17 Rn 70 ff; *Art 29 Datenschutzgruppe*, WP 196 (2012) 10; *Düsseldorfer Kreis*, Orientierungshilfe Cloud Computing (2014) 9 ff; *Kroschwald,* Informationelle Selbstbestimmung in der Cloud (2016) 120 ff; *Kroschwald,* ZD 2013, 388; *Art 29 Datenschutzgruppe*, WP 169 (2010) 16.

5.3.3 Treu und Glauben und Transparenz

Überblick

- *Begriffe Treu und Glauben und Transparenz*

Art 5 Abs 1 lit a DSGVO verlangt, dass personenbezogene Daten nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise (Transparenz) verarbeitet werden müssen. ErwGr 38 DSRL 95/46/EG führte zum Grundsatz von „Treu und Glauben" aus: *„Datenverarbeitung nach Treu und Glauben setzt voraus, daß die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden."*[898] In der DSGVO (EU) 2016/679 führt ErwGr 39 zum neuen Datenschutzgrundsatz der „Transparenz" aus: *„Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet wer-den und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können."*[899]

Wie sich aus dem früheren Erwägungsgrund 38 zur DSRL 95/46/EG und dem neuen Erwägungsgrund 39 zur DSGVO (EU) 2016/679 zeigt, sind die Regelungsziele der Grundsätze „Treu und Glauben" und „Transparenz" in der DSGVO auf dem ersten Blick sehr ähnlich.[900] Es bedarf daher einer gewissen Präzisierung und einer Abgrenzung zwischen beiden Anforderungen:

Der **Grundsatz von Treu und Glauben** in der DSGVO ist schwerpunktmäßig als Rücksichtnahmepflicht zu verstehen. Das bedeutet, dass vom Verantwortlichen die Verhältnismäßigkeit zu wahren ist und die betroffene Person nicht in der Ausübung ihrer Rechte getäuscht oder behindert werden darf.[901] Die Anforderung einer Datenverarbeitung nach Treu und Glauben bedeutet somit, dass der Verantwortliche hinsichtlich Informations- (Art 13 – Art 14 DSGVO), Auskunfts- (Art 15 DSGVO) und Meldepflichten (Art 33 –

898 ErwGr 38 EG-Datenschutzrichtlinie 95/46/EG.
899 ErwGr 39 Datenschutz-Grundverordnung (EU) 2016/679.
900 *Kastelitz*, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogender Daten in Knyrim (Hrsg), Datenschutz-Grundverordnung (2016) 100 f.
901 *Breyer*, Verarbeitungsgrundsätze und Rechenschaftspflicht nach Art. 5 DS-GVO, DuD 5/2018, 311 ff.

Art 34 DSGVO), etc. so zu handeln hat, wie es nach dem Verständnis des redlichen Verkehrs geboten ist.[902] In der ErläutRV zum früheren österreichischen § 6 Abs 1 Z 2 DSG 2000 aF wird unter Treu und Glauben verstanden, dass ein Betroffener nicht über die Umstände des Datengebrauchs und das Bestehen und die Durchsetzbarkeit seiner Rechte irregeführt oder im Unklaren gelassen wird. Zur Sicherstellung des Grundsatzes der Verarbeitung nach Treu und Glauben dienen insbesondere die Vorschriften zur Publizität einer Verarbeitung.[903] Historisch betrachtet findet sich Grundsatz der Verarbeitung nach Treu und Glauben erstmals in Art 5 lit a der Europäische Datenschutzkonvention des Europarats vom 28. Januar 1981 (Konvention Nr 108)[904]: *„Personenbezogene Daten, die automatisch verarbeitet werden: (a) müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden;"*[905] Im Sinne einer historischen Interpretation aus dem Text der Datenschutzkonvention 1981 (Konvention Nr 108) bedeutet Verarbeitung nach Treu und Glauben mit Blick auf die englische und französische Fassung der Datenschutzkonvention 1981 (Konvention Nr 108) „fair", „gerecht" oder „angemessen". In der englischen Fassung heißt es *„obtained and processed fairly and lawfully"*, in der französischen Fassung heißt es *„obtenues et traitées loyalement et licitement"*. Sowohl der englische Begriff „fairly" als auch der französische Begriff „loyalement", die in der deutschen Sprachfassung seit 1981 mit „Treu und Glauben" übersetzt werden, deuten auf ein Verständnis im Sinne von „fair", „gerecht" oder „angemessen" hin.[906] In Art 6 Abs 1 lit a DSRL 95/46/EG fanden sich in der englischen und französischen Sprachfassung wieder die Begriffe „fairly" und „loyalement", die 1995 erneut in der deutschen Sprachfassung mit „Treu und Glauben" übersetzt wurden. Dieses „Wording" und die damit verbundene Übersetzung wurde in Art 5 Abs 1 lit a DSGVO (EN: „fairly and in a transparent manner"; FR: „loyale et transparente") im Jahr 2016 in der DSGVO beibehalten.[907] Ein typischer Anwendungsfall eines Verstoßes gegen Treu und Glauben im Sinne eines Verständnisses einer Rücksichtnahmepflicht („fair", „loyal", „gerecht") liegt vor, wenn Fehlvorstellungen bei Betroffenen über die stattfindende Datenverarbeitung provoziert bzw. in Kauf genommen oder ausgenutzt werden. Dies wäre bspw. der Fall, wenn die Einwilligung einer betroffenen Person eingeholt wird (Art 6 Abs 1 lit a DSGVO), obwohl auch eine andere Rechtsgrundlage vorliegt, und dies der betroffenen Person aber nicht mitgeteilt wird. Die betroffene Person hätte so bei der Abgabe der Einwilligung und der Preisgabe ihrer Daten den irrigen Eindruck, sie behalte die Kontrolle über die Daten, weil sie Einwilligung jederzeit widerrufen könne.[908] Nach *Roßnagel* ist „Treu und Glauben" mit „Fairness" zu verstehen. Gegen den Grundsatz der Fairness wird verstoßen, wenn Vertrauen missbraucht wird, also wenn Vertrauen in

902 *Ennöckl*, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014) 356.
903 ErläutRV 1613 BlgNR 20 GP 39 (Datenschutzgesetz 2000 – DSG).
904 Deutschland: BGBl. 1985 II. 539; Österreich: BGBl. Nr. 317/1988.
905 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten v. 28.01.1981, abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b38 (zuletzt abgerufen 20.06.2019).
906 *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017) 161.
907 *Roßnagel* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 3 Rn 53 ff.
908 *Schantz* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.02.2019) Art 5 Rn 8; *Breyer*, DuD 5/2018, 311 ff (312).

Absprachen bzw. vorausgegangenes Verhalten bzw. aus Verkehrs-, Handels- oder Berufsregelungen enttäuscht wird, also berechtigte Erwartungen nicht erfüllt werden. Über ErwGr 47 DSGVO wird bei der Interessensabwägung gemäß Art 6 Abs 1 lit f DSGVO auf die vernünftigen Erwartungen der Betroffenen hinsichtlich einer potentiellen Weiterverarbeitung abgestellt (was wurde vom Verantwortlichen an Betroffene kommuniziert?). Damit treffen der Fairness-Grundsatz und der Rechtmäßigkeits-Grundsatz im Rahmen der Interessensabwägung gemäß Art 6 Abs 1 lit f DSGVO eng zusammen.[909]

Als konkretes Beispiel zu einer Diskussion über den Grundsatz von Treu und Glauben kann in diesem Zusammenhang mA die Ankündigung von facebook Inc. aus dem Jahr 2014 im Rahmen der Übernahme der WhatsApp Inc. angeführt werden. Facebook erklärte an alle europäischen Nutzer der Dienste, dass die jeweiligen Datenbestände nicht ausgetauscht werden. Diese Ankündigung geschah einerseits zur Einhaltung des Europäischen Wettbewerbsrechts, andererseits um zu verhindern, dass Nutzer von facebook oder WhatsApp aus Datenschutzsorgen ihre Nutzerkonten nicht löschen. Tatsächlich wurde – Medienberichten folgend – der Datenaustausch aber kurze Zeit nach der Übernahme gestartet, das Vertrauen der WhatsApp Nutzer, die ihr Konto gerade deshalb nicht gelöscht hatten, weil ein Datenaustausch ausgeschlossen war, wurde insofern enttäuscht.[910]

Eine Datenverwendung nach Treu und Glauben liegt demnach vor, wenn Betroffene über die Umstände des Datengebrauchs, das Bestehen und die Durchsetzbarkeit ihrer Rechte nicht irregeführt oder im Unklaren gelassen werden. Dies gilt auch hinsichtlich der vernünftigen Erwartungen der Betroffenen an potentielle Weiterverarbeitung (ErwGr 47). Betroffene sollen immer erkennen können, was mit ihren Daten geschieht und wer Daten über sie verwendet. Eine „Täuschung" der Betroffenen über Zwecke einer Datenverarbeitung sowie der ihnen zustehenden Datenschutzrechte werden als Verstoß gegen das Prinzip von „Treu und Glauben" qualifiziert und machen eine Verarbeitungstätigkeit rechtswidrig.[911]

Der neue **Grundsatz der Transparenz** stellt schwerpunktmäßig auf die Art und Weise der zu gebenden datenschutzrechtlichen Information ab. Eine Transparenz wird – neben den detaillierten Informationspflichten – auch durch datenschutzgerechte Systemgestaltung und entsprechende datenschutzfreundliche Voreinstellungen iSd. Art 25 DSGVO gewährleistet. *Roßnagel* definiert Tranparenz wie folgt: *„Transparenz in diesem Sinn bedeutet, dass mit angemessenem Aufwand durchschaubar ist, was das System einschließlich aller Betriebs-*

909 *Roßnagel* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 3 Rn 53 ff.

910 *Fuest/Jüngling/Kaiser* in welt.de (23.02.2014), WhatsApp-Nutzer fürchten Analyse ihrer Daten, abrufbar unter: https://www.welt.de/wirtschaft/article125102992/WhatsApp-Nutzer-fuerchten-Analyse-ihrer-Daten.html (zuletzt abgerufen am 20.06.2019); *hade./dpa/Reuters* in faz.net (18.05.2017), Facebook hat doch gelogen, abrufbar unter: http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/der-facebook-boersengang/facebook-hat-bei-uebernahme-von-whatsapp-doch-gelogen-15021650.html (zuletzt abgerufen am 20.06.2019); *spiegel.de* (27.09.2016), Datenschützer geht gegen Facebook vor, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/whatsapp-und-facebook-datenschuetzer-droht-wegen-datenabgleich-a-1114120.html (zuletzt abgerufen am 20.06.2019).

911 *Jahnel,* Handbuch Datenschutzrecht (2010) Rn 4/99 f; *Ennöckl*, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014) 355 ff.

und Anwendungssoftware genau tut und tun kann und wie sich das System in der Zeit verändern kann.“[912] Alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten müssen vom Verantwortlichen leicht zugänglich, verständlich und in klarer und einfacher Sprache abgefasst und bereitgestellt werden. Diese Informationen können auch über Multi-Layer Techniken transparent gegeben werden. Der Grundsatz der Transparenz wird durch die Art 12 – Art 15, Art 30, Art 33 – Art 34, Art 35 Abs 9, Art 37 Abs 7, Art 38 Abs 4 DSGVO sichergestellt. Aus diesen Bestimmungen lässt sich ableiten, dass die Informationen grundsätzlich eine Bringschuld des Verantwortlichen sind. Der Transparenzgrundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können.[913]

- *Informationspflichten des Arbeitgebers*

Der Arbeitgeber muss seine Mitarbeiter über Datenverarbeitungen und stattfindende Kontrollen informieren (Art 5 Abs 1 lit a iVm. Art 12 ff DSGVO) und darf sie nicht im Unklaren lassen. Es darf demgemäß keine absolut verdeckten Datenverarbeitungen von Beschäftigtendaten bzw. absolut verdeckte Kontrollen im Unternehmen geben. Bei verdeckten Überwachungsmaßnahmen ist hinsichtlich Treu und Glauben zu unterscheiden:

- Es wird allgemein vom Arbeitgeber verschleiert, dass Datenverarbeitungen und Kontrollen im Unternehmen stattfinden. Werden also die betroffenen Beschäftigten ganz grundsätzlich darüber im Unklaren gelassen, dass personenbezogene Daten verarbeitet werden, liegt ein klarer Verstoß gegen Treu und Glauben aufgrund unfairer Datenverarbeitung vor. Die *Europäische Kommission* begründete im Jahr 1992 ihren Änderungsvorschlag zu Art 6 DSRL 95/46/EG hinsichtlich Treu und Glauben wie folgt: *"Die Bestimmung in* [Art 5 Abs 1 lit a DSGVO] *schließt insbesondere die Verwendung verborgener Geräte aus, mit denen heimlich und ohne Wissen der betroffenen Person beispielsweise durch Abhören des Telefons der betroffenen Person und andere Mittel Daten gesammelt werden können. Die Bestimmung untersagt ferner den Verantwortlichen einer Verarbeitung, heimlich eine Verarbeitung personenbezogener Daten vorzunehmen und diese zu benutzen."*[914] Dem entspricht auch die Rechtsprechung des EGMR zur Arbeitnehmerüberwachung, die ebenso klare Transparenz verlangt.[915]
- Wird hingegen über das allgemeine Stattfinden von Kontrollen und Datenverarbeitungen und auch deren Umfänge und Intensität entsprechend ausreichend transparent im Unternehmen vorab aufgeklärt und nur die konkrete Durchführung im Einzelfall dann ggf. nicht sofort offen, sondern anfangs verdeckt durchgeführt, liegt kein Verstoß gegen Treu und Glauben vor. In der Literatur ist strittig, ob hier überhaupt bzw. ab wann hier ggf. bei dann tatsächlich stattfindenden konkreten Maßnahmen (die sich aber in Art und

912 *Roßnagel* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 3 Rn 57.
913 ErwGr 39 Datenschutz-Grundverordnung (EU) 2016/679; *Breyer*, DuD 5/2018, 311 ff (312 f.).
914 *Ehmann/Helfrich*, EG-Datenschutzrichtlinie Kurzkommentar (1999) Art 6 Rn 4.
915 EGMR Urteil v. 05.09.2017, Az. 61496/08 („Bărbulescu“); *Brodil,* ZAS 2018/33, 203 (204).

Umfang an das allgemein an Beschäftigte Kommunizierte halten) extra nochmals individuell informiert werden muss. Nach *Rebhahn* reiche die allgemeine Information zu den in einem Unternehmen stattfinden Verarbeitungen und Kontrollen an Beschäftigten aus. Solche dann konkret im informierten Umfang stattfindende Kontrollen durch Arbeitgeber sind dann für Beschäftigte nicht mehr „verdeckt" im Sinne „von darüber im Unklaren gelassen zu werden", weshalb der Betroffene dann aus dem Grundsatz von Treu und Glauben heraus nicht mehr nochmals informiert werden müsste.[916]

Der Grundsatz von Treu und Glauben und Transparenz verlangt gemäß Art 13 Abs 3 bzw. Art 14 Abs 4 DSGVO zusätzlich, dass die Betroffenen vor einer vom Verantwortlichen beabsichtigten Weiterverarbeitung für einen anderen Zweck (Art 6 Abs 4 DSGVO) auch über diesen anderen neuen Zweck zu informieren sind und dazu alle anderen maßgeblichen Informationen zur Verfügung gestellt bekommen, was insofern zeitlich mit der gesetzlich geforderten Erstinformation gemäß Art 13 Abs 1 u. Abs 2 bzw. Art 14 Abs 1 u. Abs 2 DSGVO auseinanderfallen kann.[917]

Die Grundsätze von Treu und Glauben und Transparenz werden in der DSGVO iZh mit der Informationspflicht durch Art 14 Abs 5 DSGVO (Einschränkung der Informationspflichten) sowie durch nationales Recht – gestützt auf Art 23 DSGVO – gegenüber Betroffene begrenzt. Für das Beschäftigtenverhältnis sind folgende Ausnahmebestimmungen von Relevanz:

- *Art 13 Abs 4 bzw. Art 14 Abs 5 lit a DSGVO*: Die betroffene Person verfügt bereits über die Informationen.
- *Art 14 Abs 5 lit b Alt 3 DSGVO*: Die Erteilung der Informationen würde voraussichtlich die Verwirklichung der Ziele der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen. In diesen Fällen muss der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person ergreifen, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit.
- *§ 29 Abs 1 Satz 1 BDSG Deutschland*: Durch die Informationserteilung nach Art 14 DSGVO würden Informationen offenbart werden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.
- *§ 33 Abs 1 Nr 2 lit a BDSG Deutschland*: Durch die Informationserteilung nach Art 14 DSGVO würde die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen werden bzw. die Verarbeitung beinhaltet Daten aus zivilrechtlichen Verträgen und dient der Verhütung von Schäden durch Straftaten und das berechtigte Interesse der betroffenen Person an der Informationserteilung überwiegt nicht.

Österreich hat im DSG keine Einschränkungen der Informationspflichten der DSGVO für private Stellen vorgesehen.

916 *Rebhahn,* Mitarbeiterkontrolle am Arbeitsplatz (2009) 82.

917 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 6 Rn 48 ff; *Knyrim* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 13 Rn 65 ff; Art 14 Rn 41.

- *Auskunftsrechte des Beschäftigten*

Der Gesetzestext der DSGVO selbst kennt im Sinne des Transparenzgrundsatzes keine Beschränkung des Auskunftsrechts gemäß Art 15 DSGVO. Lediglich der Erhalt einer Kopie der Daten wird in Art 15 Abs 4 DSGVO eingeschränkt. *Stollhoff* vertritt nun die Ansicht, dass auch der Auskunftsanspruch selbst (und nicht nur der Erhalt von Kopien) ebenso zu begrenzen sei, als Rechte und Freiheiten anderer Personen dadurch beeinträchtigt werden würden. Ein Recht des Betroffenen auf Auskunft (und nicht nur auf Erhalt einer Kopie der Daten) nach Art 15 DSGVO sollte daher nur in dem Umfang bestehen, soweit dadurch nicht die Rechte und Freiheiten anderer Personen – inklusive des Verantwortlichen selbst – beeinträchtigt werden. Dies umfasst bspw. Geschäftsgeheimnisse oder Rechte des geistigen Eigentums wie das Urheberrecht an Software, aber auch Datenschutzrechte anderer Betroffenen. Solche Informationen müssten und dürften nicht vom Verantwortlichen beauskunftet werden. Dies darf jedoch nicht dazu führen, dass jegliche Auskunft verweigert wird.[918]

National wird das Auskunftsrecht der DSGVO für private (nicht-öffentliche) Stellen – gestützt auf Art 23 Abs 1 DSGVO – stark beschränkt; für Beschäftigte relevant sind dabei:

Deutschland:

- *§ 29 Abs 1 Satz 2 BDSG*: Kein Auskunftsrecht bei Geheimhaltungspflichten aufgrund überwiegender berechtigten Interessen eines Dritten;
- *§ 34 Abs 1 Nr 2 lit a BDSG*: Kein Auskunftsrecht bei Daten, die aufgrund gesetzlicher Aufbewahrungspflichten nicht gelöscht werden dürfen und nur zu diesen Zwecken gespeichert sind und [1.] die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie [2.] eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist;[919]
- *§ 34 Abs 1 Nr 2 lit b BDSG:* Kein Auskunftsrecht bei Daten, die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle (IT-Sicherheit) dienen und [1.] die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie [2.] eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Werden diese Logdateien aber auch für andere Zwecke verwendet (z.B. Leistungskontrolle, Compliance Maßnahme), greift die Ausnahme des § 34 Abs 1 Nr 2 lit b BDSG nicht mehr.[920]

Österreich:

- *§ 4 Abs 6 DSG:* Das Recht auf Auskunft gemäß Art 15 DSGVO besteht gegenüber einem Verantwortlichen in der Regel dann nicht, wenn durch die Erteilung dieser Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen bzw. Dritter gefährdet würde.

---

918 *Stollhoff* in Eßer/Kramer/v. Lewinski (Hrsg), DSGVO BDSG[6] (2018) Art 15 Rn 32 ff; ErwGr 63 Datenschutz-Grundverordnung (EU) 2016/679.

919 *Stollhoff* in Eßer/Kramer/v. Lewinski (Hrsg), DSGVO BDSG[6] (2018) § 34 BDSG Rn 23 ff.

920 *Stollhoff* in Eßer/Kramer/v. Lewinski (Hrsg), DSGVO BDSG[6] (2018) § 34 BDSG Rn 23 ff.

Gemäß Art 15 Abs 4 DSGVO sowie gemäß § 29 Abs 1 Satz 2 BDSG in Deutschland bzw. § 4 Abs 6 DSG in Österreich hat ein ausgeschiedener Mitarbeiter in der Regel keinen Anspruch auf Herausgabe von Kopien der rein betrieblichen (elektronischen) Korrespondenz und Daten (eMails, Chats, Präsentationen, etc). Die Geheimhaltungsinteressen des Arbeitgebers überwiegen eindeutig dem Auskunftsinteresse des betroffenen ehemaligen Beschäftigten. Nur in besonderen Einzelfällen kann eine Herausgabe von einzelnen Kopien betrieblicher elektronischer Korrespondenz an einen ehemaligen Beschäftigten doch geboten sein (z.B. Abwehr von Rechtsansprüchen).[921] Zudem greifen noch die angeführten nationalen Einschränkungen.

War die Privatnutzung der IT für den ausgeschiedenen Beschäftigten erlaubt, befinden sich am Endgerät bzw. am Laufwerk des Arbeitgebers folglich auch private Daten des ausgeschiedenen Mitarbeiters. Der Arbeitgeber hat an diesen rein privaten Daten in der Regel kein datenschutzrechtlich berechtigtes Interesse (§ 26 Abs 1 Satz 1 BDSG bzw. Art 6 Abs 1 lit f DSGVO), womit gemäß Art 17 Abs 1 lit a DSGVO nach Ausscheiden des Mitarbeiters diese Daten grundsätzlich sofort zu löschen wären. Trotzdem darf der Arbeitgeber nach Rechtsprechung des OLG Dresden diese privaten Daten nicht einfach sogleich löschen (Art 17 DSGVO) sondern muss sie für einen gewissen Zeitraum für eine Auskunft an den Betroffenen bereit halten – OLG Dresden: „*Wird im Rahmen eines Vertragsverhältnisses von einem Vertragspartner für den anderen ein E-Mail account angelegt, auf dem dieser auch private Mails speichert, entspricht es den vertraglichen Nebenpflichten, von einer Löschung des accounts nach Beendigung des Vertragsverhältnisses solange abzusehen, bis klar ist, dass die andere Partei an der Nutzung des accounts kein Interesse mehr hat.*“[922] Ein nicht mehr bestehendes Interesse beim ehemaligen Beschäftigten an den privaten Daten zeigt sich dann, wenn dieser in Kenntnis des privaten Datenbestandes über mehrere Monate nach Beendigung des Arbeitsverhältnis sich nicht mit dem Ersuchen um Datenherausgabe (Auskunft) an den ehemaligen Arbeitgeber wendet. Ein Arbeitgeber kann rein private Daten nämlich nicht dauerhaft für ausgeschiedene Beschäftigte aufbewahren. Eine Möglichkeit bieten Vereinbarungen zu konkreten Löschungsfristen z.B. im Arbeitsvertrag (z.B. Löschung innerhalb von 6 Wochen, wenn kein Auskunftsersuchen hinsichtlich der privaten Daten kommt).[923]

Sprachaufzeichnung und Spracherkennung

Neben den oben genannten allgemeinen Informationspflichten gemäß Art 13 und Art 14 DSGVO wird der Grundsatz von Treu und Glauben und Transparenz im Rahmen von Sprachaufzeichnungen und Sprachbefehlen insbesondere beim Digitalen Assistenten folgendesmaßen sichergestellt:

---

921 *Prankl*, Umgang mit Arbeitnehmerdaten bei Beendigung des Arbeitsverhältnisses, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 84 ff.

922 OLG Dresden Beschluss v. 05.09.2012, Az. 4 W 961/12.

923 *Prankl,* Umgang mit Arbeitnehmerdaten bei Beendigung des Arbeitsverhältnisses, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 84 ff; *Thiele*, Rechtssicherer Umgang mit elektronischen Accounts ausgeschiedener Mitarbeiter, jusIT 2014, 1 ff (5); *Ertel* in datenschutz-notizen.de (19.02.2013), Löschen des E-Mail-Accounts ausgeschiedener Beschäftigter, abrufbar unter: https://www.datenschutz-notizen.de/loeschen-des-e-mail-accounts-ausgeschiedener-beschaeftigter-343254/ (zuletzt abgerufen am 20.06.2019).

- Der Lautsprecher für die Sprachbefehle wird nach außen hin so dargestellt und positioniert, dass es sich um keine „getarnte“ Sende- und Telekommunikationsanlage iSd. § 90 TKG 2004 handelt. Der Nutzer wird dabei ausreichend über das Vorhandensein eines Lautsprechers mit Mikrofonen im Raum und dem Verantwortlichen informiert.
- Die Funktionsweise wird dem Nutzer exakt dargestellt. Es werden die konkreten Stichworte, die dazu führen, dass die Sprachbefehle aufgezeichnet werden, genannt. Es wird dargelegt, welche optischen und akustischen Signale der Lautsprecher zeigt, wenn er aktiviert ist und welche optischen und akustischen der Lautsprecher macht, wenn die Aufnahme beendet ist und der Lautsprecher auf passiv schaltet und der Lautsprecher nicht mehr aufzeichnet. Zusätzlich wird die Alternative mit dem Tastendruckverfahren erklärt.
- die Nutzer werden informiert, an welche konkreten „Empfänger“ (Verantwortliche und Auftragsverarbeiter oder Dritte) die Audiodateien ihrer Sprachbefehle gehen, insbesondere ob diese auch in ein Drittland außerhalb der EU übermittelt werden.[924] Durch diese Information wird sichergestellt, dass nicht nur die Aufnahme der Sprache durch informiert (konkludente) Einwilligung erfolgt, sondern zugleich auch die rechtskonform aufgezeichneten Sprachbefehle ohne strafrechtliche Risiken gemäß § 201 Abs 1 Nr 2 dStGB (hergestellte Aufnahme unbefugt einem Dritten zugänglich machen) bzw § 120 Abs 2 öStGB (ohne Einverständnis des Sprechenden, die Sprachaufnahme einem Dritten, für den sie nicht bestimmt ist, zugänglich macht) an einen Auftragsverarbeiter (z.B. Cloud Dienstleister) gehen dürfen. So vertreten *Lewisch/Reindl-Krauskopf* die Meinung, dass ein Fall eines (konkludenten) strafrechtlichen Einverständnisses vorliegt, wenn der Anrufer bspw. in einem Call-Center darüber informiert wird, dass eine Gesprächsaufzeichnung erfolgt (z.B. zu Qualitätssicherungszwecken) und es sei dabei ohne Bedeutung, ob die Gesprächsanalyse innerhalb des Call Centers oder durch ein Outsourcing (Auftragsverarbeiter) erfolge. Das (konkludente) Einverständnis – vorhergehende Information vorausgesetzt – umfasse nach *Lewisch/Reindl-Krauskopf* auch die Weitergabe der Sprachdaten im Outsourcing.[925]
- die Rechtsgrundlage und die Zwecke werden konkret genannt. Dies ist hinsichtlich der Sprachdateien (= digitale Sprache) inklusive der Verarbeitung zur Sprecheridentifizierung als Maßnahme zur Datensicherheit die ausdrückliche Einwilligung gemäß Art 9 Abs 2 lit a DSGVO bzw. § 26 Abs 2 iVm. Abs 3 Satz 2 BDSG. Für die vom Digitalen Assistenten anschließend aus den Sprachbefehlen transkribierten Inhalte (= digitale Texte) ist es das berechtigte Interesse des Verantwortlichen gemäß Art 6 Abs 1 lit f DSGVO bzw. die Erforderlichkeit für das Beschäftigtenverhältnis iSd. § 26 Abs 1 Satz 1 BDSG.[926]
- Die Dauer der Speicherung der Sprachbefehle als Audiodateien (= digitale Sprache) ist bekannt zu geben und der Nutzer erhält über eine Online-Schnittstelle die Möglichkeit seine in Form von Audiodateien vorliegenden Sprachbefehle jederzeit löschen zu können. Zudem wird dem Nutzer bekannt gegeben, dass die transkribierten Sprachbefehle,

924 *BNetzA*, Prüfkritieren digitale Assistenzsysteme – Z21e6216-Grundsatz v. 11.04.2017 , abrufbar unter: https://fragdenstaat.de/anfrage/alexa-siri-co-kunstliche-intelligenz-uberprufungsunterlagen/#nachricht-82803 (zuletzt abgerufen am 120.06.2019).

925 *Lewisch/Reindl-Krauskopf* in Höpfl/Ratz (Hrsg), WK StGB^2 (Stand 17.10.2017) § 120 Rn 14.

926 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten“ (2019) 24; 29 ff.

die zugleich als digitale Texte vorliegen gemäß den internen Löschfristen z.B. für die betriebliche elektronische Kommunikation gespeichert werden.

Nutzerprofiling und Automatisierte Einzelentscheidungen

Neben den allgemeinen Informationen gemäß Art 13 und Art 14 DSGVO wird der Nutzer gemäß Art 13 Abs 2 lit f bzw. Art 14 Abs 2 lit g DSGVO darüber informiert, ob ein Profiling erfolgt und ob automatisierte Einzelentscheidungen bestehen können und die Nutzer erhalten auch Informationen über die involvierte Logik und die Tragweite und die angestrebten Auswirkungen derartiger Verarbeitungen. Das heißt der Verantwortliche muss beschreiben, worüber aufgrund der Datenverarbeitung entschieden werden soll, welche Entscheidungsmöglichkeiten bestehen und welche Verarbeitungsergebnisse zu welcher Entscheidung führen oder führen können.[927] Da der Profiling Prozess sehr oft unsichtbar ist für die Betroffenen, vor allem weil neue personenbezogene Daten hinzukommen, die nicht beim Betroffenen erhoben wurden, ist es wichtig, dass die Betroffenen die komplexen Techniken mit Profiling und automatisierten Einzelentscheidungen verstehen. Profiling verstößt zudem gegen Treu und Glauben, wenn es unfair ist, also bspw. Betroffenen Zugang zu beruflichen Chancen aufgrund des Profilings verwehrt werden.[928] Ebenso sind die Rechtsgrundlagen des Profilings zu nennen. Wenn ausreichende technische und organisatorische Maßnahmen (Pseudonymisierung und Verschlüsselung) gesetzt wurden und zudem ausschließlich nur berufliche fachspezifische Teilaspekte des Beschäftigten dem informierten Profiling unterliegen, kann man grundsätzlich das berechtigte Interesse des Verantwortlichen gemäß Art 6 Abs 1 lit f DSGVO bzw. die Erforderlichkeit für das Beschäftigtenverhältnis iSd. § 26 Abs 1 Satz 1 BDSG als gültige Rechtsgrundlage ansehen.[929]

Dem Nutzer sind zur Sicherstellung der Transparenz insbesondere auch die organisatorischen und infrastrukturellen Beziehungen zu den unterschiedlichen angebundenen Diensten bekannt zu geben und welche Daten hier verarbeitet werden. Die Datenschutzinformationen sollten dem Nutzer klar und verständlich anzeigbar zur optionalen jederzeitigen Abrufbarkeit zur Verfügung gestellt werden. Darüberhinaus sollte gemäß dem Grundsatz von Treu und Glauben und Transparenz der Digitale Assistent so gestaltet sein, dass der Beschäftigte als Nutzer die Funktion des Digitalen Assistenten durchschauen kann und wesentliche Abläufe auch beeinflussen kann.[930]

Cloud Computing

Neben der Sicherstellung der allgemeinen Informationen gemäß Art 13 und Art 14 DSGVO liegt der Schwerpunkt der Transparenzpflichten beim Cloud Computing an der genauen Kenntnis der Datenflüsse.

Zur Sicherstellung einer Verarbeitung nach Treu und Glauben und Transparenz bedarf es der Information über die Empfänger oder Kategorien von Empfänger (Art 13 Abs 1 lit e

927 *Bäcker* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 13 Rn 53 ff.
928 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 9 ff.
929 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 14; *Kroschwald*, Informationelle Selbstbestimmung in der Cloud (2016) 219 ff.
930 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 325; 331.

bzw Art 14 Abs 1 lit e DSGVO). Der Begriff „Empfänger" umfasst sowohl weitere Verantwortliche (Dritte), Auftragsverarbeiter und Subauftragsverarbeiter. Hintergrund ist, dass der Cloud Anwender als Verantwortlicher die Rechtmäßigkeit der Verarbeitung nur dann überprüfen kann, wenn ihn der Cloud Anbieter über alle einschlägigen Fragen informiert. Das heißt, der Cloud Anwender ist über alle Unterauftragsverarbeiter zu informieren (Art 28 Abs 2 DSGVO), da der Cloud Anwender als Verantwortlicher selbst darüber gemäß Art 13 Abs 1 lit e bzw. Art 14 Abs 1 lit e DSGVO informieren bzw. gemäß Art 15 Abs 1 lit c DSGVO Auskunft geben muss.[931]

5.3.4 Grundsatz der Zweckbindung

Überblick

Ein Arbeitgeber als Verantwortlicher (Art 4 Nr 7 DSGVO) und Hauptadressat der DSGVO darf personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erheben, verarbeiten und benötigt für den definierten Zweck eine anwendbare Rechtsgrundlage, die diese zweckgebundene Verarbeitung legitimiert. Das heißt ein Verantwortlicher muss bereits bei Verarbeitungsbeginn einen konkreten Zweck bzw. konkrete Zwecke vorab definiert haben (Art 5 Abs 1 lit b DSGVO – „festgelegter Zweck") und eine solche Verarbeitung zu einem solchen klar definierten Zweck muss sich zusätzlich auf eine dazu geeignete konkrete Rechtsgrundlage stützen können (Art 5 Abs 1 lit a DSGVO – „Rechtmäßigkeit"). Der Zweck muss „eindeutig" sein, das heißt eine allgemeine und vage Beschreibung des Gegenstands der Verarbeitung ist ebenso wie eine gänzlich fehlende Zweckdeterminierung unzulässig.[932] „Legitimer Zweck" bedeutet dabei, dass damit alle von der Rechtsordnung erlaubten Zwecke gemeint sind, das heißt der beabsichtigte Zweck darf nicht gegen andere Vorschriften der Rechtsordnung verstoßen (z.B. Arbeits- oder Verbraucherschutzrecht).[933] Eine mangelnde Legitimität des Zwecks liegt bspw. vor, wenn Arbeitgeber Daten von Beschäftigten erheben, um diese unzulässig zu diskriminieren.[934] Die eindeutige Zweckbestimmung einer Verarbeitung personenbezogener Daten ist quasi der Dreh- und Angelpunkt des Datenschutzes hinsichtlich „Rechtmäßigkeit", „Erforderlichkeit", „Angemessenheit", „Vollständigkeit" und „Dauer" einer konkreten Verarbeitung. Der Zweck legitimiert eine Datenverarbeitung und begrenzt sie zugleich. Der Zweck ist die steuernde Größe für die Auswahl der Daten und die Prozessschritte der Datenverarbeitung.[935] Aus Art 5 Abs 1 DSGVO und der Anforderung an die Rechtmäßigkeit und der eindeutigen Zweckbindung soll sich nach hM ein „Verbot mit Erlaubnisvorbehalt" („Rechtmäßigkeit") und ein Anforderungsschema, welches weitgehend einer grundrechtlichen Verhältnismäßigkeitsprüfung

931 *Art 29 Datenschutzgruppe*, WP 196 (2012) 13.

932 *Ennöckl*, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014) 359; *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 4/101 f.

933 *Herbst* in Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018) Art 5 Rn 37; *Art 29 Datenschutzgruppe*, WP 203 (2013) 12; 19 ff.

934 *Breyer*, DuD 5/2018, 311 ff. (313).

935 *Frenzel* in Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018) Art 4 Rn 23; *Roßnagel* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 3 Rn 62 f; *Ennöckl*, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014) 358.

entspricht, ergeben.[936] *Roßnagel* widerspricht und sieht in den Rechtmäßigkeitsnormen der DSGVO gerade kein Verbot mit Erlaubnisvorbehalt, sondern eher eine reine Erlaubnisregel zur Erfüllung der primärrechtlichen Anforderungen aus Art 8 Abs 1 iVm. Art 52 Abs EU-GRC (Eingriffe in das Grundrecht auf Datenschutz unter Vorbehalt des Gesetzes). Die Rechtmäßigkeitsvorschriften der DSGVO seien nämlich keine im Technikrecht übliche Regelungen, die ein konkretes Verhalten z.B. zur präventiven behördlichen Überprüfung verbieten würden, sondern im Gegenteil, die DSGVO begrenze die Datenverarbeitung kaum und gebe sie stattdessen weitgehend frei, weshalb mit der DSGVO insofern eine reine Erlaubnisregel und keine Verbotsnorm vorliegen würde.[937]

Sprachaufzeichnung und Spracherkennung

Der Zweck der Sprachaufzeichnung ist die Möglichkeit per Sprachbefehl mit dem Digitalen Assistenten zu arbeiten. Ein Zweck liegt in der Sprecheridentifizierung als Maßnahme zur Datensicherheit, damit nicht Unbefugte Sprachbefehle an den Digitalen Assistenten erteilen.[938] Andererseits erfolgt eine Aufzeichnung des gesprochenen Wortes zum Zweck, dass die gesprochene Sprache (Audiodaten) anschließend in Textform transkribiert werden kann. Vom Zweckbindungsgrundsatz ist der Zweck der Speicherung des gesprochenen Wortes grundsätzlich ab dem Zeitpunkt der erfolgreichen Transkription in Textform erreicht. Nach Art 17 Abs 1 lit a DSGVO sind personenbezogene Daten zu löschen, wenn sie für die Zwecke, für die sie erhoben oder verarbeitet wurden, nicht mehr notwendig sind.

Möchte man die Sprachbefehle (Audiodateien) weiter speichern, hat der Verantwortliche bereits vor der Erhebung der Sprachbefehle einen weiteren Zweck zu benennen, warum die Sprachbefehle trotz Zweckerreichung (Sprecheridentifikation und Abgabe des Sprachbefehls und Beantwortung durch den Digitalen Assistenten) dennoch weitergespeichert werden sollen. Ein Beispiel dazu wäre, dass die Spracherkennung des Digitalen Assistenten auf den Nutzer trainiert wird und es so erst möglich wird, die Kommunikation zwischen Digitalem Assistenten und dem Nutzer zu verbessern. Dieser Zweck müsste dann zusätzlich transparent definiert werden inkl. der Benennung der konkret dafür erforderlichen Speicherdauer und Rechtsgrundlage. Nach *Schnaber/Krieger-Lamina/Peissl* sei eine Aufbewahrung aggregierter Daten vollkommen ausreichend. So könnte ein Stimmprofil inkrementell mit Hilfe der jeweils letzten Sprachaufnahme verbessert werden, die anschließend gelöscht wird. Hinsichtlich des transkribierten Textes könnte ggf. auch nur der Anfragetyp und der Kontext der Anfrage gespeichert werden.[939]

Nutzerprofiling und Automatisierte Einzelentscheidungen

Der Zweck des Nutzerprofilings ist der Betrieb des Digitalen Assistenten. Solange der Nutzer seinen Assistenten nutzt, benötigt dieser Informationen über seine Benutzer. Je nach

936 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 5 Rn 8; Art 6 Rn 1; *Ennöckl*, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014) 355 ff.

937 *Roßnagel* in Roßnagel (Hrsg), Das neue Datenschutzrecht (2018) § 3 Rn 50 ff.

938 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten" (2019) 35 ff.

939 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten" (2019) 39.

angeschlossener Applikation sind die diversen Zwecke des Profilings transparent zu beschreiben. Verzichtet ein Nutzer auf eine auf Profiling gestützte Applikation, ist das Profil sogleich oder nur nach kurzer Frist zu löschen. Wichtig ist, dass für zweckändernde Verarbeitungen der Daten der Kompatibilitätstest nach Art 6 Abs 4 DSGVO zu machen ist, weil die Weiterverarbeitung im Rahmen des Profilings ggf. nicht zweckkompatibel ist mit dem Primärzweck.[940]

Darüberhinaus ist als technische und organisatorische Maßnahme sicherzustellen, dass für den Betrieb des Digitalen Assistenten nur ein Zugriff von berechtigten Softwarekomponenten erfolgt. Jede sonstige Einsichtsmaßnahme durch eine nicht erforderliche Software oder Dritten ist durch entsprechende Maßnahmen (Zugriffsbeschränkungen) erfolgreich sicherzustellen.[941] Eine dazu erforderliche Maßnahme ist, dass zu unterschiedlichen Zwecken erhobene Daten getrennt gespeichert und verarbeitet werden (vgl. Nr 8 der Anlage zu § 9 BDSG aF). Nur wenn sich ein Beschäftigter darauf verlassen kann, dass seine personenbezogenen Daten (Nutzerprofil) nicht zweckfremd verwendet werden, entsteht eine Transparenz der Datenverarbeitung, die eine freie Selbstdarstellung und persönliche Entfaltungsmöglichkeit ermöglicht.[942] Die Zweckbindung durch Datentrennung nach Verwendungszusammenhängen lässt sich wie folgt sicherstellen:

- Der Digitale Assistent ist so zu gestalten, dass personenbezogene Daten nach verschiedenen Verwendungszwecken und Verwendungszusammenhängen getrennt gespeichert und verwendet werden können.
- Die technische Trennung sollte anhand der zur Verfügung stehenden Funktionen des Digitalen Assistenten erfolgen.
- Durch eine Rechteverwaltung sollten auf die physisch getrennt gespeicherten Daten variabel die Zugriffs- und Verwendungsrechte vergeben werden.[943]

Cloud Computing

Cloud Computing selbst ist, wenn es im Rahmen der Auftragsverarbeitung als virtuelle Abteilung erfolgt, kein Selbstzweck, sondern der eigentliche Zweck der Verarbeitung ist weiter das relevante Kriterium, unabhängig davon, ob die Verarbeitung direkt beim Verantwortlichen stattfindet oder in einer Public Cloud. Sicherzustellen im Rahmen des Cloud Computings ist, dass die personenbezogenen Daten nicht gesetzeswidrig für weitere Zwecke vom Cloud Anbieter oder seiner Unterauftragsverarbeiter verarbeitet werden.[944]

Beim Cloud Computing hat dabei die Anforderung der Nicht-Verkettbarkeit äußerst hohe Relevanz. Nicht-Verkettbarkeit bedeutet, dass Verfahren so zu gestalten sind, dass personenbezogene Daten nicht oder nur mit einem unverhältnismäßig hohen Aufwand für einen anderen als den ausgewiesenen Zweck verarbeitet werden dürfen.[945]

940 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 11 ff.
941 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 301.
942 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 320 ff.
943 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 341 f.
944 *Art 29 Datenschutzgruppe*, WP 196 (2012) 14.
945 *Düsseldorfer Kreis*, Orientierungshilfe Cloud Computing (2014) 24.

5.3.5 Datenminimierung

Überblick

Diese Voraussetzung verlangt, dass die personenbezogenen Daten für die konkrete Datenverarbeitung zum festgelegten, eindeutigen und legitimen Zweck von wesentlicher Bedeutung sein müssen. Das bedeutet, dass die Daten im Rahmen der Zweckbindung qualitativ und quantitativ begrenzt werden müssen. Die Formulierung „Minimierung" zielt nach *Frenzel* auf eine möglichst weitgehende Begrenzung ab.[946] Der Verantwortliche hat zu prüfen, ob alle Daten tatsächlich benötigt werden, um den festgelegten, eindeutigen und legitimen Zweck zu erfüllen. Das Anlegen eines Datenvorrats für zum Zeitpunkt der Datenermittlung jedoch noch nicht vorhersehbare Verarbeitungstätigkeiten ist rechtswidrig.[947] Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.[948] Art 5 Abs 1 lit c DSGVO enthält drei Merkmale zur Datenminimierung:

- *„angemessen"* (iSv. besteht überhaupt ein Bezug zum Verarbeitungszweck?),
- *„erheblich"* (iSv. sind die Daten geeignet, den festgelegten Zweck zu fördern?) und
- *„auf das notwendige Maß beschränkt"* (kann der Zweck der Verarbeitung trotz „Angemessenheit" und „Erheblichkeit" der Daten trotzdem auch ohne die Verarbeitung erreicht werden?).[949]

Konkret bedeutet dies, dass so wenige Daten wie möglich verarbeitet werden sollen. Die Daten müssen für den konkreten Verarbeitungszweck von wesentlicher Bedeutung sein. Die Daten sollten dabei womöglich weitgehend pseudonymisiert und anonymisiert werden.[950]

Sprachaufzeichnung und Spracherkennung

Im Oktober 2017 wurde entdeckt, dass Google Mini (eine Variante des Google Home Lautsprechers, der es ermöglicht mit dem Google Assistant per Sprachbefehl zu interagieren) die Gespräche seiner Nutzer aufzeichnete, obwohl diese den Lautsprecher nicht aktiviert hatten, weder über den Sprachbefehl "OK Google" noch über einen Tastendruck. Demgemäß wurde – nach Medienberichten – die von Nutzern gesprochene Sprache ohne ihr Einverständnis aufgezeichnet und auf die Google Server hochgeladen. Dieser Fall ist ein Beispiel, wenn im Rahmen von Datenerhebungen personenbezogene Daten (unabsichtlich) erhoben und verarbeitet werden, obwohl sie für die Verarbeitung für den festgelegten, eindeutigen und legitimen Zweck nicht von wesentlicher Bedeutung sind. Demgemäß stellt

946 *Frenzel* in Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018) Art 5 Rn 34 ff.
947 *Jahnel,* Handbuch Datenschutzrecht (2010) Rn 4/106 f.
948 ErwGr 39 Datenschutz-Grundverordnung (EU) 2016/679.
949 *Herbst* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 5 Rn 55 ff; *Jahnel,* Handbuch Datenschutzrecht (2010) Rn 4/106 f.
950 *Pötters* in Gola (Hrsg), DS-GVO[2] (2018) Art 5 Rn 21 ff.

diese Aufzeichnung einen Verstoß gegen Art 5 Abs 1 lit c DSGVO dar. Ein Digitaler Assistent sollte Sprachdateien nur dann aufzeichnen, wenn der Digitale Assistent vom Nutzer konkret aktiviert wurde.[951]

Eine ähnliche Kritik wurde an Amazon Alexa von der Verbraucherzentrale NRW geübt. Obwohl die Datenaufzeichnung via Alexa nur stattfinden sollte, wenn die Signalwörter "Alexa", "Echo" oder "Amazon", „Computer" vom Nutzer ausgesprochen wurden, zeichnet Amazon Alexa bspw. auch bei den Wörtern "Alexander", „Amazonas" und "Komm Peter" auf, womit es zu einer Datenverarbeitung kommt, die gegen das Prinzip der Datenminimierung verstößt.[952]

Nutzerprofiling und Automatisierte Einzelentscheidungen

Im Rahmen des Nutzerprofilings sollten vom Digitalen Assistenten nur solche Informationen über den Nutzer erhoben werden, die auch für den zweckgebundenen Betrieb erforderlich sind (nur die für den Betrieb des Digitalen Assistenten relevanten Teilaspekte des beruflichen Wirkens eines Beschäftigten). Andere Informationen dürfen nicht in das Profiling einfließen.

Der Grundsatz der Datenminimierung greift dabei auch hinsichtlich der innerhalb der Anwendung zu verarbeitenden Daten sowie auch der Protokolldaten. Grundsätzlich sollten im Rahmen des Profilings nur aggregierte, bzw. ausreichend pseudonymisierte Daten verwendet werden, um dem Grundsatz der Datenminimierung zu entsprechen.[953]

Eine erfolgreiche Möglichkeit zur Datenminimierung ist die Pseudonymisierung in Form von selbstgenierten Pseudonymen (Betroffener vergibt selbst), Referenz-Pseudonyme (Personenbezug kann über eine Referenzliste wiederhergestellt werden) oder Einweg-Pseudonyme (Identitätsdaten werden auf Basis asymmetrischer Verschlüsselungsverfahren errechnet – eine Rückrechnung über die mathematische Einweg-Funktion ist nicht möglich).[954] Die Datenminimierung kann insbesondere sichergestellt werden:

- Es werden nur die unbedingt für das Funktionieren des Digitalen Assistenten erforderlichen personenbezogenen Daten erhoben und verarbeitet und zugleich pseudonymisiert. Alle nicht unbedingt erforderlichen Daten sollten nur anonymisiert erhoben und verarbeitet werden.

951 *Wilkens* in heise.de (12.10.2017), Datenschutzpanne mit Google Home Mini: Einschaltknopf wird deaktiviert: https://www.heise.de/newsticker/meldung/Datenschutzpanne-mit-Google-Home-Mini-Einschaltknopf-wird-deaktiviert-3858861.html (zuletzt abgerufen am 20.06.2019); *Kling* in zdnet.de (11.10.2017), Datenschutz-Panne: Google Home Mini hört dauernd mit: http://www.zdnet.de/88315221/datenschutz-panne-google-home-mini-hoert-dauernd-mit/?inf_by=5a390395681db884538b494e (zuletzt abgerufen am 20.06.2019).

952 *Schillerhof*, Amazon Echo (2017) 26; *Verbraucherzentrale NRW* (20.12.2017), Digitaler Sprachassistent: Alexa reagiert auch ungefragt: https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/digitaler-sprachassistent-alexa-reagiert-auch-ungefragt-21363 (zuletzt abgerufen am 20.06.2019).

953 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 11 ff.

954 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 323.

- Die für das Nutzerprofil zu verarbeitenden personenbezogenen Daten sollten ebenso auf das für das erforderliche Maß zur Systemfunktionalität des Digitalen Assistenten reduziert werden. Das Anlegen von Referenzdateien ist zu vermeiden. Bei biometrischen Verfahren sollten die Daten des Nutzers nur auf Chipkarten gespeichert werden.
- Personenbezogene Daten, die für den Arbeitsablauf des Digitalen Assistenten nicht mehr erforderlich sind, sollten sogleich gelöscht werden. Der Nutzer muss aufgeklärt werden, welche Daten er selbst löschen kann und welche aufgrund des Verwendungszwecks nicht vom Nutzer selbst gelöscht werden können.[955]

Cloud Computing

Der Grundsatz der Datenminimierung betrifft das Cloud Computing insbesondere hinsichtlich der innerhalb der Anwendung zu verarbeitenden Nutzungs- bzw. Protokolldaten. Die Anwendungen müssen insofern klare Löschanweisungen erlauben.[956]

5.3.6 Richtigkeit

Der Grundsatz der Datenrichtigkeit verlangt sowohl für die aufgezeichneten Sprachbefehle, für das Profiling und für das Cloud Computing, dass Daten im Sinne einer Datenqualität auf dem korrekten Stand zu halten sind. Der Verantwortliche hat für die sachliche Richtigkeit der Daten in allen Verarbeitungsphasen (Datenerhebung, Datenanalyse, Aufbau eines Profils über einen Betroffenen, Anwendung des Profils für die Entscheidungsfindung) – insbesondere beim Profiling – zu sorgen. Das heißt der Verantwortliche hat effektive Maßnahmen zu implementieren, damit falsche Daten rasch korrigiert werden können.[957] Personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig (geworden) sind, müssen unverzüglich gelöscht oder berichtigt werden. Der Verantwortlichen hat die klare Verantwortung und die Aufgabe aktiv die Richtigkeit der verarbeiteten Daten regelmäßig zu überprüfen.[958] Neben der gesetzlichen Verpflichtung des Verantwortlichen zur sachlichen Richtigkeit der von ihm verarbeiteten Daten, haben auch Betroffenen gemäß Art 16 DSGVO einen Berichtigungsanspruch.[959] Die gesetzliche Vorgabe der Aktualisierungspflicht gegenüber dem Verantwortlichem steht unter Vorbehalt „erforderlichenfalls" (Art 5 Abs 1 lit d DSGVO). Der Verantwortliche hat durch technische und organisatorische Maßnahmen innerhalb seiner Organisation sicherzustellen, dass der Fluss von neuen Informationen seinen Weg zu den Stellen findet, welche die Richtigkeit der Daten bewerten können und – wenn erforderlich – korrigieren können. Der Grundsatz der Richtigkeit gilt nicht bei Daten, die sich auf einen bestimmten Zeitpunkt oder einen bestimmten Vorgang beziehen, wenn die inhaltliche Korrektur ihren Aussagegehalt verfälschen würde, der im Hinblick auf die Zwecke der Verarbeitung aber genau relevant ist.[960] Ausdrücklich zeitbezogene Angaben werden durch eine spätere Veränderung des tatsächlichen Zustandes nicht

955 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 339 f.
956 *Düsseldorfer Kreis*, Orientierungshilfe Cloud Computing (2014) 36.
957 *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 4/108 f; *Hoeren*, Big Data und Datenqualität – ein Blick auf die DS-GVO, ZD 2016, 459; *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 12.
958 *Pötters* in Gola (Hrsg), DS-GVO[2] (2018) Art 5 Rn 24.
959 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 5 Rn 24.
960 *Schantz* in Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (01.02.2019) Art 5 Rn 29 f.

unrichtig.[961] Zum Beispiel können objektiv betrachtet veraltete Daten zu dem Zweck der Beweissicherung weiter aktuell bleiben.[962]

Zusammengefasst bedeutet dies, dass ein Digitaler Assistent so gestaltet sein muss, dass die zur Verarbeitung erforderlichen Daten (z.B. Nutzerprofil) ohne großen Aufwand aktualisiert und auch gelöscht werden können. Nach einem gewissen Zeitraum sollten diese ganz allgemein durch den Digitalen Assistenten „vergessen" werden, also gelöscht werden, um das Risiko von unrichtigen Daten entgegen Art 5 Abs 1 lit d DSGVO zu minimieren.[963]

5.3.7 Speicherbegrenzung

Überblick

Der Grundsatz der Speicherbegrenzung verlangt, dass Daten nicht länger gespeichert werden dürfen, als dies für die Zwecke ihrer Verarbeitung notwendig ist. Der Verantwortliche hat konkrete Speicherfristen vorzusehen. Eine Vorratsdatenspeicherung von Daten für einen noch unbekannten, erst in der Zukunft sich ergebenden Zweck, ist unzulässig. Der Verantwortliche hat den Betroffenen die Dauer der Speicherung ihrer personenbezogenen Daten mitzuteilen bzw., falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (vgl. Art 13 Abs 2 lit a, Art 14 Abs 2 lit a sowie Art 15 Abs 1 lit d DSGVO).[964] ErwGr 39 Satz 12 DSGVO verlangt konkrete Fristen für die Datenlöschung und regelmäßige Überprüfungen in Form von vertretbaren Schritten, damit unrichtige personenbezogene Daten gelöscht oder zumindest berichtigt werden.[965] Eine Konkretisierung des Grundsatzes der Speicherbegrenzung findet sich in der Löschungspflicht des Verantwortlichen gemäß Art 17 Abs 1 lit a DSGVO.[966] Hinsichtlich der rechtskonformen Löschung privater Daten ehemaliger Beschäftigter ist die Rechtsprechung des *OLG Dresden* zu beachten, dass bei Vorliegen privater Daten von einer Löschung nach Beendigung des Vertragsverhältnisses solange abzusehen ist, bis klar ist, dass die andere Partei an der Nutzung der privaten Daten kein Interesse mehr hat (vgl. **Kapitel 5.3.3** – *Auskunftsrechte des Beschäftigten*).[967]

Sprachaufzeichnung und Spracherkennung

Apple Inc. bspw. speichert die Siri Spachbefehle der Nutzer in identifizierter Form für 6 Monate. Nach 6 Monaten werden die Daten zur Identifizierung gelöscht und die Sprachbefehle und Sprachdaten der Nutzers werden in nicht mehr identifizierter Form für weitere 2 Jahre gespeichert.[968] Da unbearbeitete Sprachbefehle aufgrund der weiterbestehenden Möglichkeit der Sprach- und Sprecheridentifizierung mA keine anonymen Daten sind, liegen bei Sprachdateien höchstens pseudonymisierte Daten vor. Nach *Müller-Peltzer/Franck* ist die Speicherung der Sprachbefehle für temporäre Analysen von beendeten Nutzer Inter-

961 *Jahnel*, Handbuch Datenschutzrecht (2010) Rn 4/108 f.
962 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 5 Rn 24.
963 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 327 f.
964 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 5 Rn 25.
965 ErwGr 39 Datenschutz-Grundverordnung (EU) 2016/679.
966 *Herbst* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 5 Rn 55 ff;
967 OLG Dresden Beschluss v. 05.09.2012, Az. 4 W 961/12.
968 *Damaschke*, Siri Handbuch (2016) 16 f.

aktionen mit europäischem Datenschutzrecht vereinbar, eine dauerhafte Speicherung hingegen nicht.[969] Die *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI) sieht ein hohes Datenschutzrisiko in der Speicherung solcher Sprachbefehle. Alle Wörter, die ein Nutzer ausspricht, werden in der Cloud des Providers gespeichert. Diese Speicherung sei aber nicht „notwendig". Das Problem für die *BfDI* liegt darin, dass Stunden an gesprochener Sprache (aufgezeichnete Sprachbefehle) über jeden Nutzer bei Cloud Providern vorliegen, die sehr leicht und effektiv für Identitätsdiebstähle genutzt werden können, wenn die Cloud Provider gehackt werden.[970] Eine vergleichbare Problematik sehen *Schnaber/Krieger-Lamina/Peissl*, dass von Hackern erbeutete Sprachbefehle dazu verwendet werden könnten, die Stimme der Betroffenen täuschend echt nachzuahmen. Nach dem aktuellen Stand der Technik seien dafür bereits wenige Sekunden Sprachaufnahmen ausreichend.[971]

Nutzerprofiling und Automatisierte Einzelentscheidungen

Machine Learning Algorithmen sind heute dazu ausgerichtet, große Datenvolumina zu verarbeiten und Korrelationen zu identifizieren, die sehr intensive und intime Profile über Betroffene ermöglichen. Die Nutzerprofile sollten nur solange gespeichert werden, wie der Digitale Assistent vom Nutzer genutzt wird. Mit Nutzungsende und damit verbundener Zweckerreichung sollten die Nutzerprofile gemäß Art 17 Abs 1 lit a DSGVO gelöscht werden.[972]

Cloud Computing

Im Rahmen des Cloud Computings hat der Cloud Anwender sicherzustellen, dass die Daten beim Cloud Anbieter auch tatsächlich gelöscht werden, sobald sie nicht mehr erforderlich sind. Es müssen dabei sämtliche Daten inklusive Daten auf Backups gelöscht werden, insbesondere auch wenn diese auf verschiedenen Servern an unterschiedlichsten Orten gespeichert sind. Es bedarf der unwiderruflichen Löschung. Der Cloud Anbieter muss eine solche Löschung garantieren, dies hat der Cloud Anwender sicherzustellen. Löscht der Cloud Anbieter trotz Weisung des Cloud Anwenders die Daten nicht, macht sich der Cloud Anbieter hinsichtlich dieser Weiterspeicherung gemäß Art 28 Abs 10 DSGVO zum Verantwortlichen und mangels Rechtsgrundlage und rechtmäßigem Zweck würde sofort ein Datenschutzverstoß vorliegen.[973] Hinzuweisen ist noch, dass bspw. das EU-US Privacy Shield keine Löschungsverpflichtung vergleichbar zu Art 5 Abs 1 lit e iVm. Art 17 DSGVO kennt. Nach Analyse der *Art 29 Datenschutzgruppe* unterliegt daher ein EU-US Privacy Shield zertifizierter US Cloud Anbieter – trotz Anerkennung der Grundprinzipien des europäischen Da-

969 *Müller-Peltzer/Franck,* Gruß Bot! Aktuelle Rechtsfragen zum Einsatz von Chatbots, in Taeger (Hrsg), Recht 4.0 (2017) 251 ff.

970 *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*, Sprachassistenten (2017) 2 ff.

971 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten" (2019) 37 f.

972 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 12.

973 *Art 29 Datenschutzgruppe*, WP 196 (2012) 15; *Düsseldorfer Kreis*, Orientierungshilfe Cloud Computing (2014) 27.

tenschutzrechts im EU-US Privacy Shield – keiner vergleichbar strengen Speicherbegrenzungsverpflichtung, wie ein europäischer Cloud Anbieter nach DSGVO.[974] Darüberhinaus gelten die in **Kapitel 6.2** umfangreich definierten Risiken.

5.3.8 Integrität und Vertraulichkeit

Überblick

Beim Grundsatz von Integrität und Vertraulichkeit ist zu unterscheiden zwischen:

- unbefugter oder unrechtmäßiger Datenverarbeitung;
- unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Eine *unbefugte Verarbeitung* liegt vor, wenn personenbezogene Daten unbefugt außenstehenden Dritten, also Personen, die nicht dem Verantwortlichen zuzurechnen sind, z.B. offengelegt werden und von diesen weiterverarbeitet werden. Eine *unrechtmäßige Datenverarbeitung* liegt vor, wenn personenbezogene Daten ohne Rechtsgrundlage verarbeitet werden bzw. ohne Rechtsgrundlage offen gelegt werden.[975]

Ein *unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten* liegt vor, wenn Daten verloren gehen oder derart geändert werden, dass sie nicht mehr oder nur noch eingeschränkt für den vorgesehenen legitimen Zweck verarbeitet werden können.[976]

Der Grundsatz der Integrität und Vertraulichkeit wird konkretisiert durch Art 32 Abs 2 und Abs 4, Art 29 und Art 28 Abs 3 Satz 2 lit b sowie Art 29 DSGVO. Darin wird die Verpflichtung konkretisiert, eine unbefugte Offenlegung, einen unbefugten Zugang und die unbefugte Verarbeitung personenbezogener Daten zu verhindern.[977]

Zur Dokumentation der Umsetzung des Grundsatzes der Integrität und Vertraulichkeit sowie des speziellen Art 32 DSGVO im Rahmen der Rechenschaftspflicht gemäß Art 5 Abs 2 DSGVO (Accountability) existieren folgende Standards:

- "ISO/IEC 27001:2013" ein internationaler Best Practice Standard für das Informationssicherheits-Managementsystem (ISMS);
- "ISO/IEC 27002:2013" ein international anerkannter Standard zur IT-Security;
- "Critical Security Controls for Effective Cyber Defense" des Center for Internet Security (CIS) ist ein Standard mit Best Practice Anforderungen für Computer Sicherheit;
- „IT-Grundschutz" ist ein deutscher IT-Sicherheitsstandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Es handelt sich um eine Methologie zur Identifizierung und Implementierung von IT-Security in einer Organisation.[978]

Zur Sicherstellung der Vertraulichkeit sind sämtliche Daten im Rahmen der Übertragung durch Verschlüsselungsverfahren mit ausreichend langen Schlüsseln zu sichern (Ende-zu-

974 *Art. 29 Datenschutzgruppe,* WP 238 (2016) 17.
975 *Herbst* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 5 Rn 74.
976 *Herbst* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 5 Rn 75.
977 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 5 Rn 28.
978 *Feiler/Forgó*, EU-DSGVO (2017) 27 f; *Düsseldorfer Kreis*, Orientierungshilfe Cloud Computing (2014) 23 ff.

Ende-Verschlüsselung). Die lokal am Endgerät bzw. in der Cloud gespeicherten Daten des Digitalen Assistenten sind ebenso umfassend zu verschlüsseln. Besonders wichtige Daten sollten abgeschottet von anderen verschlüsselt in einer Private Cloud / OnPremise (lokale Nutzung und lokale Lizenzierung) gespeichert werden.[979] Darüberhinaus ist eine Revisionsfähigkeit des Digitalen Assistenten sicherzustellen:

- Die Datenerhebungs- und –verarbeitungsvorgänge müssen nachvollziehbar und zur Sicherstellung der Datensicherheit (Art 32 DSGVO) kontrolliert werden können.
- Der Digitale Assistent muss daher zu Zwecken der Datensicherheit (Art 32 DSGVO) eine nachträgliche Überprüfung ermöglichen (wer, wann, was gemacht hat und welche personenbezogenen Daten verarbeitet oder gelöscht wurden). Dabei ist auch zu den Zwecken der Datensicherheit (Art 32 DSGVO) die Protokollierung so zu gestalten, dass nur die dafür unbedingt erforderlichen Protokolldaten zur Zweckerreichung der Datensicherheit erhoben und gespeichert werden.
- Zudem ist sicherzustellen, dass der Digitale Assistent auch in der Form revisionsfähig gestaltet wird, dass der tatsächliche Zustand des Systems festgestellt werden kann. Der Digitale Assistent muss manipulationsresistent sein, das heißt unbemerkte Änderungen der Funktionsfähigkeit durch technische Maßnahmen muss ausgeschlossen sein.[980]

Sprachaufzeichnung und Spracherkennung

Die Sprachsteuerung bei Digitalen Assistenten ist darauf ausgelegt, dass sie Anfragen möglichst schnell und reibungslos beantworten kann. Insofern wird häufig auf eine Authentifizierung des korrekten Nutzers verzichtet, womit theoretisch jeder Anfragen an den Digitalen Assistenten stellen könnte. Es ist aus Gründen der Datensicherheit (Art 32 DSGVO) insb. zur Vorbeugung einer unbefugten oder unrechtmäßigen Datenverarbeitung erforderlich, dass für die Nutzung des Digitalen Assistenten im betrieblichen Kontext ein Stimmprofil angelegt wird, damit nur nach erfolgter Stimm- und Sprechererkennung eines berechtigten Nutzers und der damit verbundenen Authentifizierung der Zugang zu Informationen, die der Digitale Assistent per Sprache bereitstellt, datenschutzkonform erfolgen kann. Ein vergleichbares gelinderes Mittel iZh. mit Sprachbefehlen und der mündlichen Kommunikation mit dem Digitalen Assistenten ist nicht ersichtlich.[981]

979 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 327 f.
980 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 345 f.
981 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten“ (2019) 35.

5.4 Big Data

5.4.1 Überblick

Unter Big Data versteht man gemäß den *Wissenschaftlichen Diensten des Deutschen Bundestages*[982] ein Bündel neu entwickelter Methoden und Technologien, welche die Erfassung, Speicherung und Analyse eines großen und beliebig erweiterbaren Volumens unterschiedlich strukturierter Daten ermöglicht. In Österreich definiert § 2b Z 5 Forschungsorganisationsgesetz den Begriff „Big Data" als *„die Verarbeitung großer Mengen von wenig oder nicht strukturierten Daten"*.[983] Der ErläutRV zufolge wurde auf eine Begriffsbestimmung des National Institutes of Standards and Technology (NIST) vom September 2017 zurückgegriffen.[984]

Big Data ist dabei durch vier maßgebliche Charakteristika gekennzeichnet:

- *Datenmenge (Volume)*: Durch die fortschreitende Digitalisierung praktisch aller Bereiche des modernen Lebens werden Datenmengen in bisher unvorstellbar großen Quantitäten produziert. Diese Datenmengen verdoppeln sich schätzungsweise alle zwei Jahre.
- *Geschwindigkeit (Velocity)*: Die Vernetzung und elektronische Kommunikation erfordert es, einlaufende Informationen immer schneller und in Echtzeit aufzunehmen und zu analysieren.
- *unterschiedliche Beschaffenheit (Variety)*: Daten liegen heute in vielfältiger und komplexer Form vor (soziale Netzwerke, Fotos, Videos, MP3 Dateien, Blogs, Suchmaschinen, Tweets, E-Mails, Internet-Telefonie, Musikstreaming, Sensorendaten von intelligenten Geräten wie vernetzten Fahrzeugen oder vernetzten Haushaltsgeräten). Besonders von Relevanz für Werbung, Marketing oder auch politische Wahlkämpfe sind subjektive Stimmungen oder Meinungen sowie ausdrückende Äußerungen in Texten oder Videobeiträgen aller Art. Um diese unterschiedlichen Daten maschinenlesbar zu machen, greift man auf entsprechende Programme zurück, die dies lesbar und erkennbar machen. Das besondere an Big Data ist, dass durch Kombination bisher nicht aufeinander bezogener Daten Korrelationen sichtbar werden, die sonst nie sichtbar geworden wären.[985]
- *Zuverlässigkeit, Wahrhaftigkeit („Veracity")*: Das Kriterium der Zuverlässigkeit berücksichtigt, dass die zu analysierenden Daten als Entscheidungsgrundlagen dienen sollen, es daher auf die Verlässlichkeit der Daten ankommt, denn bereits die Quelle, aus der die zu analysierenden Daten entstammen, kann unzuverlässig sein. Aber auch die Inhalte sind nicht immer präzise und können durch zahlreiche Einflussfaktoren verfälscht werden. Big Data Analysen arbeiten mit Wahrscheinlichkeiten, Statistiken und

982 *Horvath*, Wissenschaftliche Dienste Deutscher Bundestag (Fachbereich WD 10), Aktueller Begriff Big Data, abrufbar unter: https://www.bundestag.de/blob/194790/c44371b1c740987a7f6fa74c06f518c8/big_data-data.pdf (zuletzt abgerufen am 20.06.2019).

983 § 2b Z 5 Forschungsorganisationsgesetz idF. BGBl. I Nr. 31/2018.

984 ErläutRV 68 BlgNr 26. GP 19.

985 *Horvath*, Wissenschaftliche Dienste Deutscher Bundestag (Fachbereich WD 10), Aktueller Begriff Big Data, abrufbar unter: https://www.bundestag.de/blob/194790/c44371b1c740987a7f6fa74c06f518c8/big_data-data.pdf (zuletzt abgerufen am 20.06.2019).

> Prognosen, wodurch die Qualität der zu analysierenden Daten von besonderer Bedeutung ist für diejenigen, die ihre unternehmerischen Entscheidungen auf die Analyseergebnisse stützen. Die Herausforderung bei Big Data besteht folglich darin, die Zuverlässigkeit und Berechenbarkeit von Natur aus ungenauer Datentypen in den Griff zu bekommen.[986]

Big Data ist der „Treibstoff" für die künstliche Intelligenz. Künstliche Intelligenz basiert in den meisten Fällen auf sogenannten neuronalen Netzen, also einer dem menschlichen Gehirn nachempfundenen Technik und ist eigentlich seit den 1960er Jahren bekannt. Diese Technik wird allerdings erst jetzt aufgrund der immer größer werdenden gigantischen Datenmengen richtig einsetzbar, weil die neuronalen Netze mit diesen vielen vorhandenen Daten richtig trainiert werden können. Neuronale Netze speichern Daten nicht in einer Datenbank, sondern kodieren Daten als bestimmte Aktivierungszustände ihrer Neuronen. Die Neuronen des neuronalen Netzes „feuern", wenn ihr Aktivierungszustand einen bestimmten Schwellenwert überschreitet. Im menschlichen Gehirn feuern die Neuronen durch chemische Vorgänge, im neuronalen Netz der künstlichen Intelligenz geschieht dies durch Zahlenwerte (Gewichtung). Ein Effekt in der realen Welt, wird in einem neuronalen Netz als eine bestimmte Aktivität seiner Neuronen repräsentiert. Neuronale Netzte lernen ihre Aktivierung durch intensives Training mit Daten und werden aktuell u.a. für die Vorhersage von Aktienpreisentwicklungen, zur Bild- und Spracherkennung oder zum autonomen Vorlesen von Texten eingesetzt.[987]

Big Data im Zusammenhang mit künstlicher Intelligenz bedeutet im zivilen Bereich seit einigen Jahren eine technologische Revolution. Es besteht die Erwartung, dass datenbasierte Entscheidungsfindung eine Erhöhung der Produktivität bewirkt.[988] Im militärischen Bereich ist das, was im kommerziellen Bereich mit Big Data bezeichnet wird, eine seit Jahrzehnten erprobte Art und Weise der Massendatenverarbeitung. Big Data ermöglicht es, große Datenmengen bezogen auf ein konkretes Problem oder eine bestimmte Fragestellung zu analysieren und nicht mehr auf kleine Daten-Samples beschränkt zu sein, denn sobald man mit großen Datenmengen arbeiten kann, ist das Sampling nicht mehr sinnvoll. Die Berücksichtigung sämtlicher Daten befähigt zum Erkennen von Zusammenhängen und Einzelheiten (Korrelation), die in der Masse der Informationen verborgen bleiben.[989] Eine Korrelation quantifiziert eine statistische Beziehung zwischen zwei Datenpunkten. Eine starke Korrelation bedeutet, dass sich ein Datenpunkt wahrscheinlich ändert, wenn ein anderer sich ebenfalls verändert. Umgekehrt bedeutet eine schwache Korrelation, dass ein Datenpunkt sich bei Veränderungen des mit ihm korrelierten anderen Wertes wahrscheinlich nur wenig oder gar nicht ändert. Es gibt insofern hochentwickelte Computeranalysen, die diese

---

986 *Hackenberg* in Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019) Teil 16.7 Big Data Rn 5 f; *Europäisches Parlament*, Entschließung vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatssphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)) Erwägung B.

987 *Hofstetter*, Sie wissen alles. Wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen (2014) 133 f.

988 *Weichert*, Big Data und Datenschutz – Chancen und Risiken einer neuen Form der Datenanalyse, ZD 2013, 251.

989 *Schönberger*, Big Data – Die Revolution, die unser Leben verändern wird (2014) 29 ff; 38 f; *Ohrtmann/Schwiering*, Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 2984.

optimalen Korrelationen zwischen den unterschiedlichen Daten identifizieren. Korrelationen sagen bei Big Data Analysen nur „was" (wahrscheinliche Zusammenhänge), aber nicht „warum" etwas so ist (kausale Relation).[990] Bei Big Data handelt es sich also um eine Technik der Zusammenführung und Aufbereitung von bruchstückhaften und teilweise widersprüchlichen (Sensor-)Daten in ein homogenes, für den Menschen verständliches Gesamtbild einer Situation. Das Ziel ist die automatische Extraktion von Informationen und Wissen aus rohen Daten und somit die Erzeugung abgeleiteter Information, die in vorhandenen rohen Datenmengen steckt, aber nicht auf den ersten menschlichen Blick erkennbar ist. Dies findet in drei Schritten statt:

- *monitor (beobachten, Daten sammeln)*: Daten über ein und dasselbe Objekt werden durch Beobachtung mit Hilfe von Sensoren gesammelt und gespeichert (das Beobachtungsobjekt ist bei der Hochfinanz ein Investmentprodukt; im zivilen Bereich ggf. der Bürger selbst; und im militärischen Bereich z.B. bei AWACS ein in der Luft befindliches unbekanntes Flugzeug). Die erfassten Daten werden dabei so gespeichert, dass sie leicht wiedergefunden und vollautomatisch analysiert werden können.
- *evaluate (Daten zu einer Lageanalyse aufbereiten)*: Die gesammelten riesigen heterogene Sensor- und Messdatenbestände werden mit sogenannten Sekundärdaten aus anderen Informationsquellen fusioniert. Dabei analysieren Algorithmen mit künstlicher Intelligenz diese umfangreichen heterogenen Rohdaten und stellen Korrelationen fest und können somit mögliche Absichten der Akteure identifizieren.
- *control (Fähigkeit Ereignisse zu lenken bzw. das Verhalten von Menschen zu beeinflussen)*: Auf Basis des aus der Datenanalyse entstehenden Lagebilds und einer daraus möglichen Wahrscheinlichkeitsprognose für die zukünftigen denkbaren und prozentuell wahrscheinlichen Handlungen des beobachteten Objekts, wird es im Ergebnis möglich, mit einer gewissen Wahrscheinlichkeit unbekannte Korrelationen sowie Absichten und Intentionen zu erkennen und darauf vorzeitig bzw. rechtzeitig reagieren zu können. Da künstliche Intelligenz naturgemäß nicht mit 100%iger Sicherheit richtig liegt (Wahrscheinlichkeitsprognose), ist eine statistische Komponente in Form der Bayes'schen Statistik eingebaut. Daraus wird es möglich aus vielen Vergangenheitsdaten auf die Zukunft zu schließen und es ergibt sich die Chance, möglichst großen Einfluss zu nehmen, wie sich die Zukunft entwickelt bzw. bei einem Individuum die Entscheidungsfindung zu beeinflussen.[991]

Mit Big Data Technologien können insbesondere **zwei Ziele** verfolgt werden:

Es geht auf dem *Makro-Level* darum, statistische Korrelationen zu erkennen und diese zur Erklärung denkbarer Phänomene einzusetzen. Diese Analysen zielen darauf ab Ereignisse vorherzusagen und zu beeinflussen. Es ist nicht das einzelne Individuum interessant, sondern seine soziale Rolle bzw. Funktion als Kunde, Patient, Wähler oder Beschäftigter. Damit lassen sich Fragen beantworten wie: Wo ist die beste Stelle für ein Werbeplakat? Wie

990 *Schönberger*, Big Data – Die Revolution, die unser Leben verändern wird (2014) 70 ff.

991 *Hofstetter*, Sie wissen alles. Wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen (2014) 14; 40; 44 ff; 58; 62; 64 f;71; 74; 79; 82; 91; 98 f; 118; *Hofstetter*, Das Ende der Demokratie. Wie künstliche Intelligenz die Politik übernimmt und uns entmündigt (2016) 26; 30; 38; 42;201; *Stiemerling*, "Künstliche Intelligenz" – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge, CR 12/2015, 762 ff.

breitet sich eine Infektionskrankheit aus? Auf diesen Ebenen ist es möglich mit anonymisierten Daten zu arbeiten und erheblichen Nutzen für die Gesellschaft zu erzeugen.[992]

Andererseits kann aber eine Zielsetzung auch darin bestehen, auf der *Mikro-Level Ebene* unbekannte Eigenschaften von bestimmten Personen besser und schneller zu erkennen und effektiv auszunutzen (Welcher Wähler ist noch unentschlossen und mit welchen Argumenten beeinflussbar? Wer hatte mit einer bestimmten Person in den letzten zwei Monaten Kontakt?). Es ist dabei die konkrete Person im Fokus der Analyse, wenn auch ihr konkreter Name ggf. gar nicht so interessant bzw. relevant ist, weil die Person bereits durch andere Merkmale ausreichend individualisiert wurde.[993]

5.4.2 Big Data im Militär

Seit über zwei Jahrzehnten findet im militärischen Bereich unter der Bezeichnung „Multi-Sensor-Datenfusion" bzw. „Datenfusion" etwas Vergleichbares statt, was man aktuell unter „Big Data" im zivilen Bereich versteht.[994]

Das fliegende Radarsystem AWACS („Airborne Early Warning and Control System") westlicher Streitkräfte ist nach *Hofstetter* ein über Jahrzehnte perfekt ausgereiftes „Big-Data System". Die AWACS-Systeme beobachten den Luftraum und müssen in der Lage sein, simultan mehrere hundert Luftobjekte gleichzeitig zu überwachen, schnell automatisch zu identifizieren und auch zu prognostizieren, was jedes erfasste Flugobjekt vorhaben könnte. Die Aufgabe ist es in kurzer Zeit die entscheidenden Beurteilungen und Schlüsse abzuleiten. Die dbzgl. automatischen Antworten entstehen dabei durch Fusion heterogener Datenquellen („Multi-Sensor-Datenfusion") und unterstützen maßgeblich die taktische menschliche AWACS Besatzung an Bord bei der Erstellung des Lagebildes und mit den zu treffenden Entscheidungen. Wichtigstes Element der AWACS ist ein sogenannter automatischer Identifizierer, welcher sich u.a. aus Regelverkettern und selbstlernenden neuronalen Netzen zusammensetzt. Ein System wie der im AWACS eingesetzte vollautomatische Identifizierer benötigt dabei riesige Mengen an unstruktierten und strukturierten Daten.[995] Die Vorgehensweise ist ähnlich wie in **Kapitel 5.4.1** bereits allgemein beschrieben:

- *„monitor" (beobachten)*: Die AWACS erhebt mittels eigenen Radars zunächst u.a. die Geschwindigkeit, die Radarrückstrahlfläche (Radarquerschnitt) sowie über die Laserabtastung, etc. weitere wichtige Daten zum noch unbekannten Flugobjekt. Zusätzlich kann die AWACS von anderen Quellen in Frage kommende strukturierte Daten abrufen (z.B. zivile Flugpläne, technische Daten aus Datenbanken über Flugzeuge weltweit wie bspw. Größe, Flügelspannweite, durchschnittliche Marschgeschwindigkeit und Flughöhe, Reichweite, etc.). Von anderen Stellen zu Boden oder in der Luft erhält die AWACS per Datenlink zusätzliche Sensordaten.

992 *Roßnagel,* ZD 2013, 562.
993 *Roßnagel,* ZD 2013, 562.
994 *irights.info* (23.10.2014), Interview mit Yvonne Hofstetter, was ist wirklich neu an „Big Data", abrufbar unter: https://irights.info/artikel/yvonne-hofstetter-was-ist-wirklich-neu-an-big-data/24147 (zuletzt abgerufen am 20.06.2019).
995 *Hofstetter*, Sie wissen alles. Wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen (2014) 14; 40; 44 ff; 58; 62; 64 f;71; 74; 79; 82.

- *„evaluate" (Daten zu einer Lageanalyse aufbereiten):* Die so gewonnenen heterogenen Daten sowohl in unstrukturierter Form (unterschiedlichste Sensordaten aller Art zu Boden oder aus der Luft) als auch in strukturierter Form aus Datenbanken (zivile Flugpläne, technische Details zu den Flugzeugtypen der Welt, etc.) werden fusioniert. Algorithmen analysieren diese Rohdaten und der automatische Indentifizierer der AWACs wägt daraus die relevanten Informationen ab (z.B. bewegt sich das Flugobjekt zu langsam für eine russische MIG 29; die Reisegeschwindigkeit liegt an der oberen Grenze von Verkehrsflugzeugen – die Wahrscheinlichkeit für ein Verkehrsflugzeug ist daher gering; ein automatisierter Abgleich der Flugspuren mit den zivilen Flugplänen ergeben ebenso, dass es sich um keine zivilen Flugzeuge handeln kann, etc.). Mit Hilfe der statistischen Komponente der Bayes'schen Statistik wird letztlich festgestellt, dass ein Flugobjekt mit 90%iger Wahrscheinlichkeit identifiziert werden kann. Die Meisterleistung der Datenfusion des AWACS Identifizierers besteht darin, diese unterschiedlichen und völlig heterogenen Daten (Text, Bilder, Zahlen, Spektralbereiche, Sensordaten) zu einer neuen Information – hier dem militärischen Lageüberblick – als maßgebliche Unterstützung für die militärische Besatzung und die Luftwaffen-Offiziere zusammenzuführen.
- *„control" (Fähigkeit Ereignisse zu lenken bzw. zu beeinflussen):* Auf Basis des mit Unterstützung der Datenfusionstechnik erhobenen fundierten Lagebilds können dann daraus die Handlungsalternativen der eigenen Luftstreitkräfte sicherer geplant werden (iSv. neue Information erzeugen und daraus Prognosen erstellen).[996]

5.4.3 Kommerzielles Big Data

Kommerzielle Datenanwendungen machen genau genommen eigentlich nicht viel anderes. Die in Smartphones und Tablets eingebaute Sensoren messen und zeichnen das menschliche Verhalten ihrer Nutzer auf und geben die Daten weiter, wo sich der Nutzer genau bewegt, wie schnell er sich bewegt, und je nach zusätzlichen Aktivitäten des Nutzers was er tut und sich fühlt. Die Menschen geben dabei weitgehend ihre Absichten preis, wenn sie online nach etwas suchen, Kurznachrichten schicken oder ihre Geoposition bestimmen. So verfügt bspw. jedes Smartphone über Kameras an der Vorder- und Rückseite, Beschleunigungsmesser, Mikrophon, Licht und Geopositionssensoren, Software-Beacons, die die Fähigkeiten haben, den exakten Standort des Nutzers auch innerhalb geschlossener Räume zu erkennen und weiter zu melden. Dabei entstehen riesige heterogene humane Messdaten. Diese Daten von den Nutzern werden mit sogenannten Sekundärdaten, den im Internet hinterlassenen elektronischen Spuren fusioniert (z.B. Online Einkaufsverhalten, Reisegebaren, Speicherung und Analyse der aktuell nicht geschützten OTT-Telekommunikation, etc., Chats in sozialen Netzwerken, das Heiz- und Lüftungsverhalten sowie Fernsehkonsum oder Bewegungsprofile via Google Maps). Aus den gewonnen Informationen über Vorlieben und Interessen sowie geographischen Daten wie Bewegungsprofilen lässt sich ein sehr detailliertes Lagebild über den einzelnen Menschen erstellen (bei Big Data Analysen auf *Mikro-Level Ebene*), mit der sich nun ergebenden Möglichkeit, präzise Prognosen für zukünftiges Verhalten sowie Interessen, etc. des beobachteten Individuums zu erstellen. Im

996 *Hofstetter*, Sie wissen alles. Wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen (2014) 14; 40; 44 ff; 58; 62; 64 f;71; 74; 79; 82.

Ergebnis besteht ein kommerzielles Interesse am Ende des gesamten Prozesses, die Absichten und Intentionen der beobachteten Kunden mit hoher Wahrscheinlichkeit zu erkennen. Eine zentrale Anwendung von Big Data Technologien liegt darin, dass durch die Erstellung von feinkörnigen Bevölkerungs- und Kundensegmenten mittels Big Data der „Zugang zum Kunden" stark verbessert werden kann, worauf Waren und Dienstleistungen individueller zugeschnitten werden können.[997]

Wie in den Analysen von *Christl*[998] und *Christl/Spiekermann*[999] festgestellt wird, lassen sich bereits aus rudimentären Metadaten über das Kommunikations- und Online-Verhalten umfangreiche Vorhersagen treffen. Aus reinen Metadaten von Mobiltelefonen lassen sich mit hoher Wahrscheinlichkeit erfolgreich die Charaktereigenschaften eines Mobiltelefonnutzers prognostizieren. Wie *Nokia Research* anhand des „Big-Five"-Modells nachweisen konnte, ist es möglich, allein aus reinen Mobiltelefon Metadaten die sogenannten „Big Five"-Charaktereigenschaften mit einer Genauigkeit von beachtlichen 75,9% Richtigkeit (bei ausschließlich Metadaten) erfolgreich auf einen Menschen anhand der vorliegenden Metadaten zu prognostizieren. Zieht man nun weitere umfangreichere Internet-Daten (Online Verhalten, Inhaltsdaten, etc.) hinzu, erhöht sich die Wahrscheinlichkeit der richtigen Prognose der Charaktereigenschaften einer Person exorbitant.[1000] Dabei wird zur Einschätzung des Individuums das sogenannte „Big Five" Modell der Persönlichkeitspsychologie herangezogen. Man unterscheidet in diesem psychologischen „Big-Five"-Modell folgende Charaktereigenschaften:

- *Neurotizismus / englisch: neuroticism* (Personen mit diesen Eigenschaften neigen dazu nervös, ängstlich, traurig, unsicher, verlegen zu sein, sich Sorgen um ihre Gesundheit machend, sie neigen zu unrealistischen Ideen und sind weniger in der Lage ihre Bedürfnisse zu kontrollieren und auf Stresssituationen angemessen zu reagieren);
- *Extraversion / englisch: extraversion* (Personen mit diesen Eigenschaften gelten als gesellig, aktiv, gesprächig, personenorientiert, herzlich, optimistisch und heiter und sie mögen Anregungen und Aufregungen);
- *Offenheit für Erfahrungen / englisch: openness* (Personen mit diesen Eigenschaften zeichnen sich durch eine hohe Wertschätzung für neue Erfahrungen aus, bevorzugen Abwechslung, sind wissbegierig, kreativ, phantasievoll und unabhängig in ihrem Urteil, verfolgen vielfältige kulturelle Interessen und interessieren sich für öffentliche Ereignisse);

997 *Schönberger*, Big Data – Die Revolution, die unser Leben verändern wird (2014) 184; *Hofstetter*, Das Ende der Demokratie. Wie künstliche Intelligenz die Politik übernimmt und uns entmündigt (2016) 26; 30; 38; 42;201 ff; *Richter* in Jandt/Steidle (Hrsg), Datenschutz im Internet (2018) 309 ff; *Weichert*, ZD 2013, 251; *Ohrtmann/Schwiering*, NJW 2014, 2984.

998 *Christl*, Kommerzielle Digitale Überwachung im Alltag. Studie im Auftrag der Bundesarbeitskammer (2014).

999 *Christl/Spiekermann*, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy (2016).

1000 *Christl/Spiekermann*, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy (2016) 16 ff; *Christl*, Kommerzielle Digitale Überwachung im Alltag. Studie im Auftrag der Bundesarbeitskammer (2014) 18 ff.

- *Verträglichkeit / englisch: agreeableness* (Personen mit diesen Eigenschaften gelten als altruistisch, mitfühlend, verständnisvoll und wohlwollend, sie neigen zum zwischenmenschlichem Vertrauen, zur Kooperativität, zur Nachgiebigkeit und sie verfolgen ein Harmoniebedürfnis),
- *Gewissenhaftigkeit / englisch: conscientiousness* (Personen mit diesen Eigenschaften zeichnen sich als ordentlich, zuverlässig, hart arbeitend, diszipliniert, pünktlich, penibel, ehrgeizig, systematisch aus. Sie grenzen sich damit deutlich von nachlässigen und gleichgültigen Personen ab).

Über 2.000 psychologische Studien mit Bezugnahme auf das „Big-Five"-Modell zwischen 1999 und 2006 haben die Reproduzierbarkeit und die Konsistenz des Modells über verschiedene Altersgruppen und Kulturen weltweit aufgezeigt.[1001]

5.4.4 Big Data in der Arbeitswelt

In der Arbeitswelt kann Big Data in zwei Formen zum Einsatz gelangen:

Mit Hilfe von Big Data Analysen wird für den Beschäftigten ein verbessertes Lagebild in seinem Beruf direkt am Arbeitsplatz erstellt (vgl. „AWACS Besatzung") und der Beschäftigte kann auf Basis von fundierten Datenanalysen seine Tätigkeit effizienter und auf Basis einer besseren Entscheidungsgrundlage gestalten (z.B. Big Data in der Medizin für Ärzte und medizinisches Personal). So zeigt *Schönberger*, dass mit Hilfe von Big Data es möglich wird, leichter Kreditkartenbetrüger zu identifizieren. Die Berücksichtigung sämtlicher Daten ermöglicht das Erkennen von Zusammenhängen und Einzelheiten, die in der Masse der Informationen verborgen bleiben. Beim Kreditkartenbetrug bzw. allgemein bei Fraud Detection wird auf Anomalien geachtet. Diese findet man besser über eine umfassende Datenanalyse als über Stichproben. Denn die interessanten Hinweise bspw. für Betrug findet man in den Ausreißern und diese kann man nur ausmachen, wenn man sie mit der Masse der normalen Transaktionen vergleicht.[1002]

Mit Hilfe von Big Data Analysen kann aber auch die über Sensoren und die IT-Nutzung erhobenen Daten für Effizienzanalysen über die eigenen Beschäftigten selbst verwendet werden. Bei Big-Data-Analysen in der Personalarbeit wird in der Regel auf Personal-, Leistungs- und Verhaltensdaten zurückgegriffen. Die klassischen Personal- (Name, Adresse, Alter, Geschlecht, Konfession, Familienstand, Dauer der Betriebszugehörigkeit, Qualifikationen et cetera) und Leistungsdaten (Beförderungen, Bewertungen durch Vorgesetzte, individuelle Produktivität et cetera) liegen einem Arbeitgeber in der Regel vor bzw. müssen zur Durchführung des Arbeitsverhältnis verarbeitet werden. Bei Verhaltensdaten (Wie oft steht ein Mitarbeiter von seinem Schreibtischstuhl auf? Wie schnell tippt er auf der Tastatur? Wie kommuniziert er mit seinen Kollegen? Welche Emotionen liegen in seiner Stimme,

1001 *Christl/Spiekermann*, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy (2016) 16 ff; *Christl*, Kommerzielle Digitale Überwachung im Alltag. Studie im Auftrag der Bundesarbeitskammer (2014) 18 ff.

1002 *Schönberger*, Big Data – Die Revolution, die unser Leben verändern wird (2014) 39; *Ohrtmann/Schwiering*, NJW 2014, 2984.

während er telefoniert?) ist dies meist nicht der Fall bzw. es liegen nur gewisse Verhaltensdaten z.B. im Rahmen der Protokollierung zu IT-Sicherheitszwecken vor.[1003] So weisen *Kamarinou/Millard/Singh* darauf hin, dass Unternehmen hinsichtlich der Entscheidung, welchen Beschäftigten man Zugang und Zugriff zu bestimmten internen Projekten, Daten und Ressourcen geben sollte, Big Data Machine Learning Techniken verwenden, um entsprechende Prognosen über deren sinnvolle Förderfähigkeit (z.B. Charaktereigenschaften) vorherzusagen und darauf aufbauend Mitarbeiter auszuwählen, anstatt diese Entscheidung einem ausgebildeten HR Mitarbeiter zu überlassen.[1004] Das Beratungsunternehmen Capgemini S.A. bspw. delegiert nach Medienberichten bereits die Identifikation von Experten und die Entscheidungen für die Heranziehung zu speziellen Projekten an „IBM Watson" und überlässt die Auswahl nicht mehr (allein) einem dafür speziell geschulten und ausgebildeten HR Mitarbeiter.[1005] Ähnliche Möglichkeiten zu „People Analytics" mit unternehmerischer Chance und gleichzeitigen Risiken für Betroffene stellen sich auch bei Verwendung dieser Technik im Bewerbungs- und Einstellungsprozess.[1006] Es können über alle erdenklichen Themen der Personalarbeit Big Data Analysen durchgeführt werden (Teamzusammensetzung, Beförderungsmaßnahmen, Stressbelastung, etc.).[1007] Weitere Zwecke sind die Nutzung sämtlicher Daten und Datenspuren bis auf Ebene der Protokolldateien eines Beschäftigten in einem Big Data System zur Mitarbeiterbewertung z.B. zur Ermittlung der Arbeitszufriedenheit oder der Kündigungswahrscheinlichkeit eines Mitarbeiters; oder z.B. zur unternehmensinternen Netzwerkanalyse, um so informelle Strukturen sichtbar zu machen, die es ermöglichen die Informationsbeziehungen von Beschäftigten zu beobachten und damit ihre soziale Stellung im Unternehmen – unabhängig von der formalen Stellung – zu analysieren. Durch eine solche Netzwerkanalyse wird ersichtlich, wer in der Belegschaft angesehen ist und einflussreich ist und wer eher peripher ist und wo sich dienstlich/private Gruppen und Clans im Unternehmen gebildet haben.[1008] Zudem ist es möglich über Big Data Analysen den eventuellen Karriereverlauf eines Mitarbeiters im Unternehmen (z.B. wann er den Arbeitsplatz wahrscheinlich wechseln wird) anhand vergleichender Daten vorherzusagen. Anschließend können Maßnahmen zur Bindung des Mitarbeiters an das Unternehmen ergriffen werden. Umgekehrt kann ein über Big Data Analysen „geschätzter" hypothetisch angenommener Abwanderungswille dazu führen, dass die Karriere

1003 *Niklas* in haufe.de (07.02.2018), Zulaessigkeit von Big Data Analysen, abrufbar unter: https://www.haufe.de/personal/arbeitsrecht/datenschutz-zulaessigkeit-von-big-data-analysen_76_441566.html (zuletzt abgerufen am 20.06.2019).

1004 *Kamarinou/Millard/Singh,* Machine Learning with Personal Data (2016) 11.

1005 *Mendonca* in ETtech (22.08.2016), How Capgemini is using IBM's Watson to assign employees to projects, abrufbar unter: http://tech.economictimes.indiatimes.com/news/corporate/how-capgemini-is-using-ibms-watson-to-assign-employees-to-projects/53803797 (zuletzt abgerufen am 20.06.2019).

1006 *Christl/Spiekermann*, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy (2016) 31.

1007 *Niklas* in haufe.de (07.02.2018), Zulaessigkeit von Big Data Analysen, abrufbar unter: https://www.haufe.de/personal/arbeitsrecht/datenschutz-zulaessigkeit-von-big-data-analysen_76_441566.html (zuletzt abgerufen am 20.06.2019).

1008 *Gola/Jaspars*, RDV 3/2018, 145 ff.

des Beschäftigten im Unternehmen nicht mehr gefördert wird bzw. einen negativen bzw. schlechteren Verlauf nimmt.[1009]

Auch für die relevante Beurteilung der Leistungsfähigkeit ergeben sich neue Analysemöglichkeiten. So lassen sich aus der Analyse des Rhythmus und der Dynamik des Tippens auf einer Tastatur die Emotionen erfolgreich prognostizieren (Wahrscheinlichkeit einer korrekten Prognose: 83% bei Zuversicht; 82% bei Unschlüssigkeit; 83% bei Nervosität; 77% bei Entspannung; 88% bei Trauer; 84% bei Müdigkeit).[1010]

Kroschwald weist daraufhin, dass die im Rahmen des Cloud Computing bei einem Cloud Anbieter gespeicherten Daten eine schier unerschöpfliche Quelle für Big Data Analysen sein können. Cloud Anbieter können externe Analysen auf die in ihren Cloud Diensten gespeicherten Daten durchführen und damit – unter Änderung des ursprünglichen Verarbeitungszwecks – weitere Datenverarbeitungen durchführen.[1011]

Kommt es im Rahmen des Einsatzes eines Digitalen Assistenten zu einem Rückgriff auf Big Data Technologien sind die entsprechenden datenschutzrechtlichen Grundsätze der DSGVO streng zu beachten (Rechtsgrundlage, Datenschutzgrundsätze, etc.). Der für Big Data Analysen in diesem Zusammenhang am relevanteste gesetzliche Erlaubnistatbestand ist Art 6 Abs 1 lit f DSGVO bzw. § 26 BDSG bzw., wenn es sich bei den Big Data Analysen um eine zweckkompatible Weiterverarbeitung handelt (Art 6 Abs 4 Hs 2 DSGVO), stützt sich die Weiterverarbeitung auf die bisherige Rechtsgrundlage des Primärzwecks (ErwGr 50 Satz 2 DSGVO).[1012] Im Zusammenhang mit Big Data steht im Zentrum der Diskussion der europarechtliche Grundsatz der Zweckbindung gemäß Art 5 Abs 1 lit b DSGVO und der Möglichkeit der Zweckvereinbarkeit nach einem Kompatibilitätstest gemäß Art 6 Abs 4 Hs 2 DSGVO. In der Praxis könnte dies bedeuten, dass Unternehmen umso weitgehender Big Data Analysen durchführen dürfen, je weiter die konkreten Zwecke – unter Berücksichtigung des Transparenzgrundsatzes – gefasst haben. Unklar ist jedoch bis zu welcher Detailtiefe über Big Data Analysen informiert werden muss, denn nur allgemein gehaltene Beschreibungen in Form von Oberbegriffen („Forschung", „interne Zwecke zur Produktverbesserung", etc.) werden nicht ausreichend sein.[1013]

Strittig ist, ob die ungeordnete Sammlung von Daten und deren Auswertung nach festgelegten Kriterien („Big Data") durch Art 89 DSGVO privilegiert wird oder doch als gewöhnliche Datenverarbeitung grundsätzlich dem Kompatibilitätstest des Art 6 Abs 4 Hs 2 DSGVO unterliegt und nur in Ausnahmefällen Art 89 DSGVO greift. Eine grundsätzliche

---

1009 *Gola,* Datenschutz am Arbeitsplatz[5] (2014) Rn 34.

1010 *Christl/Spiekermann*, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy (2016) 20; *Christl*, Kommerzielle Digitale Überwachung im Alltag. Studie im Auftrag der Bundesarbeitskammer (2014) 21; *Culik/Forte*, ABIDA-Dossier Oktober 2017, Big Data-Überwachung am Arbeitsplatz – Grenzen der Zulässigkeit durch aktuelle Gerichtsentscheidungen, abrufbar unter: http://www.abida.de/sites/default/files/Dossier_Ueberwachung.pdf (zuletzt abgerufen am 20.06.2019).

1011 *Kroschwald*, Informationelle Selbstbestimmung in der Cloud (2016) 231 ff.

1012 *Feiler/Fina,* Datenschutzrechtliche Schranken für Big Data, MR 2013, 303; *Weichert*, ZD 2013, 251; *Roßnagel,* ZD 2013, 562; *Ohrtmann/Schwiering*, NJW 2014, 2984; *Hackenberg* in Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019) Teil 16.7 Big Data Rn 19 ff.

1013 *Ohrtmann/Schwiering*, NJW 2014, 2984.

Privilegierung von Big Data gemäß Art 89 DSGVO wird u.a. mit dem Argument abgelehnt, dass die Statistik eine schon geordnete Anlegung der Datensammlung verlange, was bei Big Data nicht der Fall sei.[1014] Nach *Buchner* fallen Big Daten-Analysen ebenso nicht pauschal unter die privilegierte Statistik.[1015]

Geht man von der aktuell herrschenden Ansicht aus, dass Big Data nicht pauschal unter Statistik iSd. Art 89 DSGVO fällt, bedarf es in den meisten Fällen – mangels Vorliegens einer informierten Einwilligung bzw. einer qualifizierten Rechtsgrundlage im Unionsrecht oder Recht der Mitgliedstaaten iSd. Art 6 Abs 4 Hs 1 DSGVO – des Kompatibilitätstests gemäß Art 6 Abs 4 Hs 2 DSGVO, um zweckgebunden gespeicherte Daten für Big Data Analysen zusätzlich heranziehen zu können.[1016] Nach ErwGr 50 Satz 2 DSGVO ist bei Bestehen dieses Kompatibilitätstests keine neue Rechtsgrundlage mehr erforderlich. Dieses Verbleiben auf der bisherigen Rechtsgrundlage gemäß ErwGr 50 Satz 2 DSGVO nach erfolgreichem Kompatibilitätstest kann im Einzelfall zu starken Widersprüchen führen, denn einige Betroffenenrechte stellen bspw. nur auf eine bestimmte Rechtsgrundlage ab (z.B. Art 21 DSGVO). Bei einer zweckkompatiblen Weiterverarbeitung auf Basis der Rechtsgrundlage des ursprünglichen Zwecks muss ein Verantwortlicher seine Weiterverarbeitung gemäß ErwGr 50 Satz 2 DSGVO dann ggf. gar nicht auf die das Betroffenenrecht auslösende zutreffende Rechtsgrundlage stützen, oder umgekehrt der Verantwortliche muss auf einer Rechtsgrundlage verbleiben, die das Betroffenenrecht auch für den kompatiblen Zweck auslöst, obwohl bei einer theoretischen Neuerhebung – gestützt auf die an sich korrekte Rechtsgrundlage – das jeweilige Betroffenrecht gar nicht anwendbar wäre. *Schulz* spricht hier von Unstimmigkeiten, die sich infolge des gültigen ErwGr 50 Satz 2 DSGVO in bedenklicher Weise fortsetzen.[1017] Diese Widersprüche ließen sich nur mit einer Interpretation iSv. *Feiler/Forgó* lösen, wo gemäß ErwGr 50 Satz 2 DSGVO die Rechtsgrundlage des Primärzwecks solange auch für den Sekundärzweck weiterverwendet werden kann, wie der neue Zweck in der bisherigen Rechtsgrundlage Deckung findet. Eine wörtlicher Interpretation des ErwGr 50 Satz 2 DSGVO würde ansonsten zur Aushöhlung des Grundsatzes der Rechtmäßigkeit führen.[1018]

5.4.5 Kriterien Zweckkompatibilität gemäß Art 6 Abs 4 Hs 2 DSGVO

In Art 6 Abs 4 Hs 2 DSGVO werden die konkreten Kriterien angeführt, die dazu dienen die Zweckvereinbarkeit mit dem ursprünglichen Erhebungszweck der Verarbeitung zu prüfen. Der deutsche BMI Referent *Eickelpasch* äußert sich wie folgt dazu: *„Die Verordnung hat ja dann in Artikel 6 Abs. 4 die Kompatibilität, und das ist neu, wenn man so will. Nämlich anders als noch in der Richtlinie von 95, ein wenig erklärt. Es werden jetzt Kriterien in die Hand gegeben, ein nicht abschließender Katalog in Art. 6 Abs. 4 Buchstaben a bis e. Es betrifft also Fragen der Kompatibilität. Ganz schön ist, dass man da auch einbeziehen kann, ob man pseudonymisiert oder zum Beispiel verschlüsselt, dass also Sicherheitsmaßnahmen*

1014 *Wolff* in Schantz/Wolff (Hrsg), Das neue Datenschutzrecht (2017) Rn 412 ff.
1015 *Buchner*, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 3/2016, 155 (157).
1016 *Feiler/Fina,* MR 2013, 303; *Art 29 Datenschutzgruppe* WP 221 (2014) 3.
1017 ErläutRV 1613 BlgNR 20 GP 39; *Schulz* in Gola (Hrsg), DS-GVO^2 (2018) Art 6 Rn 210 ff.
1018 *Feiler/Forgó,* EU-DSGVO (2017) Art 6 Rn 15.

mit in die Betrachtung einbezogen werden. Dafür haben wir Sorge getragen. Das kann an der einen oder anderen Stelle ganz hilfreich werden."[1019]

Am Beispiel von Protokolldaten zu IT-Sicherheitszwecken, die nachträglich für die Zwecke der Leistungsbewertung, der unternehmensinternen Netzwerkanalysen zur Aufdeckung informeller Strukturen und/oder zur Zufriedensheits- bzw. Effizienzanalyse ausgewertet werden sollen (Big Data Analysen), wird der Kompatibilitätstest gemäß Art 6 Abs 4 Hs 2 DSGVO im Beschäftigtenverhältnis geprüft. Dabei ist folgendes zu beachten:

a) *jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung.*

Hier geht es um das Wesen der Verbindung zwischen dem Primärzweck und dem geplanten Sekundärzweck. Es geht also um Situationen, wo der Sekundärzweck mehr oder weniger im Primärzweck impliziert war oder sich als ein logischer Schritt der Verarbeitung des Primärzwecks darstellt, z.B. die Kontakt- und Bankdaten eines Kunden werden nach initialer Ersterhebung zum ersten Geschäftsabschluss für den Abschluss weiterer Geschäfte (Zweckänderung pro Kauf) weiterverwendet, ohne nicht jedes Mal beim Kunden neu erhoben zu werden. Ein Szenario, wo die Zweckkompatibilität nicht offensichtlich ist, aber dennoch eine starke Verbindung besteht ist bspw. die Weiterverarbeitung der Daten für Zwecke der Werbung als Sekundärzweck für die ursprünglich zum Primärzweck der Vertragserfüllung erhobenen Daten (vgl. ErwGr 47 letzter Satz DSGVO). Je weiter die Entfernung des Primärzwecks und des Sekundärzwecks ist, desto umfassender bedarf es der Analyse der Zweckkompatibilität.[1020]

Aus Beschäftigtendatenschutzsicht ist die Weiterverarbeitung von ursprünglich allein nur zu IT-Sicherheitszwecken erhoben personenbezogenen Daten zu nachträglichen Zwecken wie der Leistungsbewertung, der unternehmensinternen Netzwerkanalysen oder der Zufriedensheits- bzw. Effizienzanalyse der Beschäftigten – insbesondere wenn diese zusätzlichen Zwecke zum Zeitpunkt der Erhebung nicht intendiert und auch nicht an die Betroffenen kommuniziert waren – als kritisch mit der Zweckkompatibilität der DSGVO anzusehen. Es liegt nämlich hinsichtlich dieser neuen Weiterverarbeitungszwecke keine eindeutige Verbindung zum ursprünglichen Erhebungszweck vor, was eine Zweckinkompatibilität im Rahmen der Kompatibilitätsprüfung indiziert (mangelnde Verbindung der Zwecke miteinander). Ein solches Ergebnis (iSv. keine Verbindung zwischen Erhebungs- und Weiterverarbeitungszweck) ergibt sich (auch) aus einer historischen Interpretation: Der deutsche § 31 BDSG aF (gesetzliches Verbot)[1021] als auch der österreichische § 14 Abs 4 DSG 2000 aF hatten bisher schon eine Verwendung der Protokolldaten von IT-Systemen zur Sicherstellung der Datensicherheit zum nachträglichen zusätzlichen Zweck der Überwachung und Kontrolle der Beschäftigten ausdrücklich verboten.[1022] Die einzige Möglichkeit in Deutschland diese Protokolldaten von IT-Systemen trotzdem über § 31 BDSG aF hinaus nutzbar zu machen, war daher vor ihrer erstmaligen Erhebung diese zusätzlichen Zwecke (z.B. Leis-

1019 *Eickelpasch*, Sonderveröffentlichung zu RDV 06/2017, 7.
1020 *Art 29 Datenschutzgruppe*, WP 203 (2013) 23 f.
1021 *Eßer* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer BDSG [aF][4] (2014) § 31 BDSG [aF] Rn 9.
1022 *Knyrim*, Datenschutzrecht[3] (2015) 263.

tungskontrolle der Beschäftigten, Analysen) vorab sogleich mitzudefinieren inkl. einer Betriebsvereinbarung (§ 87 Abs 1 Nr 6 BetrVG) und Information an die Beschäftigten (§ 33 BDSG aF).[1023] In Österreich war eine eigene Datenanwendung, gestützt auf „überwiegend berechtigte Interessen" (§ 8 Abs 1 Z 4 DSG 2000 aF) inklusive Information der Betroffenen (§ 24 DSG 2000 aF) und einer Meldung an die Datenschutzbehörde (§§ 17 ff DSG 2000 aF) erforderlich, sowie die Mitbestimmung des Betriebsrats (§§ 96 Abs 1 Z 3; 96a ArbVG), bevor die IT-Protokolldaten auch für andere Zwecke als dem Zweck der Datensicherheit (§ 14 Abs 4 DSG 2000 aF) verwendet werden durften.[1024] Eine Weiterverarbeitung von ursprünglich rein zu IT-Sicherheitszwecken erhobenen Protokolldaten für eine Leistungsbewertung oder Charakteranalyse der Beschäftigten ist daher bereits auf der ersten Stufe der Kompatibilitätsprüfung des Art 6 Abs 1 Hs 2 lit a DSGVO grundsätzlich als inkompatibel einzustufen und eine solche Weitererarbeitung wäre daher trotz ggf. berechtigter Interessen aufgrund der mangelnden Verbindung zum ursprünglichen Erhebungszweck wegen Zweckinkompatibilität rechtswidrig.[1025] Dass der Kompatibilitätstest des Art 6 Abs 4 Hs 2 DSGVO grundsätzlich hier zum selben Ergebnis wie die bisherige Rechtslage § 31 BDSG aF in Deutschland bzw. § 14 Abs 4 DSG 2000 aF in Österreich führt, verwundert insofern nicht. Kontroll- und Überwachungsmaßnahmen sind wie bisher von ihrer Art, Umfang und Intensität vor Beginn und damit vor der erstmaligen Erhebung der Daten transparent jedem Betroffenen mitzuteilen.[1026]

In Deutschland schafft § 24 Abs 1 BDSG idF. DSAnpUG-EU seit 25. Mai 2018 als Rechtsvorschrift der Mitgliedstaaten iSd. Art 6 Abs 1 Hs 1 DSGVO – zum Schutz der Ziele des Art 23 Abs 1 lit d, lit i und lit d DSGVO – nur in zwei Fällen eine gewisse Flexibilität für Arbeitgeber einen nachträglichen Zweckwechsel ohne Kompatibilitätstest durchzuführen, nämlich für die Fälle von juristischen Auseinandersetzungen bzw. zur Strafverfolgung. Nachträgliche Zweckänderung zur Verfolgung von Straftaten bzw. zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche sind für Arbeitgeber ohne Zweckkompatibilitätstest gemäß § 24 BDSG möglich, nicht aber eine interessensbasierte nachträgliche Kontrolle oder Effizienzanalyse der Beschäftigten, insbesondere wenn beim Erhebungszeitpunkt nicht intendiert bzw. gegenüber Betroffene nicht von Anbeginn kommuniziert (Art 6 Abs 4 Hs 2 lit a – b DSGVO).

Österreich hat in den bisherigen vier Novellen[1027] zur Anpassung des österreichischen DSG an die DSGVO von einer solchen Möglichkeit wie Deutschland nicht Gebrauch gemacht. Österreichische Arbeitgeber sollten daher Analysen zu Kontroll- und Effizienzzwecken und auch eine potentielle nachträgliche Beweiserhebung für (Arbeits-)Gerichtsverfahren unbedingt als eigenständige Verarbeitung vorab transparent gegenüber betroffenen Beschäftigte

1023 *Gola/Klug/Körffer* in Gola/Schomerus (Hrsg), BDSG [aF][12] (2015) § 31 Rn 5; *Eßer* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer BDSG[aF][4] (2014) § 31 Rn 9;

1024 *Pollirer/Weiss/Knyrim*, DSG[2] (Stand 26.11.2015, rdb.at) § 14 Rn 15; *Knyrim*, Datenschutzrecht[3] (2015) 261 ff (263).

1025 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg) Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.71; *Art 29 Datenschutzgruppe*, WP 203 (2013) 22 ff.

1026 *Art 29 Datenschutzgruppe*, WP 203 (2013) 56 f; EGMR Urteil v. 05.09.2017, Az. 61496/08 („Bărbulescu").

1027 BGBl. I Nr. 120/2017; BGBl. I Nr. 23/2018; BGBl. I Nr. 24/2018; BGBl. I Nr. 14/2019.

bekannt geben (Art 5 Abs 1 lit a iVm. Art 13 u. Art 14 DSGVO), im Verarbeitungsverzeichnis dokumentierten (Art 30 DSGVO) und in einer Betriebsvereinbarung (§§ 96, 96a ArbVG) mit dem Betriebsrat die konkreten Modalitäten der Art und des Umfangs der Kontrollen bzw. Überwachung regeln, damit österreichische Arbeitgeber nicht in das Problem einer Zweckänderung mit letztlich mangelnder Kompatibilität kommen, wenn sie die Daten ihrer Beschäftigten eines Tages für andere Zwecke als die (IT-)Sicherheit ihrer Infrastruktur doch brauchen würden. Anders als bis 24. Mai 2018, wo ein Verstoß gegen die strikte Zweckbindung von Protokolldaten (§ 14 Abs 4 DSG 2000 aF) als Verstoß gegen die Anforderungen des § 14 DSG 2000 aF gemäß § 52 Abs 2 Z 5 DGS 2000 aF mit einer Höchststrafe von max. 10.000 € bestraft wurde, handelt sich bei einem Verstoß gegen die Zweckbindung (Art 5 Abs 1 lit b DSGVO) um einen Verstoß gegen Art 83 Abs 5 lit a DSGVO mit dem höchstmöglichen Bußgeld der DSGVO.[1028]

b) *der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen.*

Dieser Bewertungsfaktor der Kompatibilität fokussiert am spezifischen Kontext, in dem die personenbezogenen Daten erhoben wurden und in die damit verbundenen vernünftigen Erwartungen einer betroffenen Person („reasonable expectations of privacy") in eine zukünftige mögliche Weiterverarbeitung. Es geht also um die Sicht des Betroffenen: Was kann eine vernünftige Person in der Lage des Betroffenen im Kontext der Datenerhebung erwarten hinsichtlich einer möglichen Weiterverarbeitung? Je unerwarteter und überraschender eine solche Zweckänderung erfolgt, desto wahrscheinlicher ist eine Inkompatibilität der Weiterverarbeitung. Suggeriert der Verantwortliche beispielsweise den Betroffenen, dass die Daten besonders vertrauenswürdig und nur zu einem vorher eindeutig definierten Zweck verarbeitet werden würden, ist die Weiterverarbeitung zu einem anderen Zweck stets als inkompatibel einzuordnen. „Vernünftige Erwartungen" erstrecken sich zudem denkmöglich nur auf rechtmäßige Weiterverarbeitungsvorgänge.[1029]

Dabei ist auch das Machtverhältnis zwischen dem Verantwortlichen und dem Betroffenen zu berücksichtigen, insbesondere ob die Betroffenen per Gesetz verpflichtet waren ihre Daten dem Verantwortlichen bereitzustellen oder auf Basis eines Vertrages. Liegt der Grund in einem Vertragsverhältnis, ist die Art des Vertrages und das Kräfteverhältnis zwischen Verantwortlichem und Betroffenem zu analysieren (bspw. wie leicht es für den Betroffenen wäre, den Vertrag zu kündigen und einen alternativen Vertrag zu bekommen). Beruht der Grund der Verarbeitung in einer datenschutzrechtlichen Einwilligung, muss geprüft werden, wie weit die Einwilligung freiwillig war und wie bestimmt die Bedingungen der Einwilligung waren. War die Einwilligung nicht ausreichend freiwillig bzw. wurde dem Betroffenen nicht ausreichend eine freie Wahlmöglichkeit eingeräumt bzw. wenn die Bedingungen der Einwilligung zu unbestimmt waren, könnte eine Weiterverarbeitung als inkompatibel angesehen werden, wenn die problematische Einwilligung zum Primärzweck gerade noch zulässig war. Weiters ist zu berücksichtigen, ob aus dem Status des Verant-

1028 *Art 29 Datenschutzgruppe*, WP 203 (2013) 56 f; Art 83 Abs 5 lit a DSGVO.

1029 *Art 29 Datenschutzgruppe*, WP 203 (2013) 22 ff; *Buchner/Petri* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 6 Rn 188.

wortlichen, der Art der Verbindung oder dem bereitgestellten Service oder nach dem anwendbaren Recht bzw. vertraglichen Bedingungen wie bspw. Versprechungen oder Zusicherungen, die zum Zeitpunkt abgegeben wurden, sich eine vernünftige Erwartung des Betroffenen ergeben, die eine verstärkte Vertraulichkeit und strenge Zweckbindung erwarten lassen. Dabei muss auch auf die Transparenz der gesamten Verarbeitung geachtet werden, also welche Informationen dem Betroffenen am Beginn bzw. anschließend zur Verfügung gestellt wurden. Dies ist letztlich alles abzuwägen bei der Feststellung, ob eine Weiterverarbeitung vereinbar ist mit dem ursprünglichen Verarbeitungszweck.[1030]

Am Beispiel (siehe oben) der IT-Sicherheitsdaten im Beschäftigungsverhältnis ergibt sich auch wieder eine grundsätzliche Inkompatibilität, wenn Beschäftigtendaten, die ursprünglich zu reinen (IT-)Sicherheitszwecken erhoben wurden, später für die Zwecke der Leistungsbewertung, der unternehmensinternen Netzwerkanalysen zur Aufdeckung informeller Strukturen bzw. zur Zufriedensheits- bzw. Effizienzanalyse weiterarbeitet werden sollen. Bei Art 6 Abs 4 Hs 2 lit b DSGVO ergibt sich die Inkompatibilität dadurch, dass eine vernünftige Person in der Lage des betroffenen Beschäftigten im Kontext des ihr mitgeteilten Zwecks der Datenerhebung (IT-Sicherheitszwecke) nicht erwarten kann, dass die Daten auch gegen ihn oder sie zu solchen Zwecken verwendet werden (Treu und Glauben).[1031]

c) *die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Art 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art 10 verarbeitet werden.*

Hier wird geprüft, welche Art von personenbezogenen Daten von der Weiterverarbeitung erfasst sein sollen. Die Art der Daten spielt hier eine entscheidende Rolle, also ob sensitive Daten (Art 9 bzw. Art 10 DSGVO) oder ob Kommunikationsdaten, Standortdaten oder andere hochsensible Daten verarbeitet werden sollen. Darüberhinaus könnte auch abgestellt werden, ob es sich um besonders schutzwürdige Personengruppen handelt. Generell gilt hier der Grundsatz, je sensitiver die Informationen, desto enger ist der Spielraum einer kompatiblen Weiterverarbeitung.

Am Beispiel (siehe oben) der IT-Sicherheitsdaten im Beschäftigungsverhältnis ergibt sich bei einer nachträglichen Weiterverarbeitung von Kommunikationsdaten betrieblicher IT-Systeme (Metadaten, Protokolldaten), die ursprünglich ausschließlich zu IT-Sicherheitszwecken erhoben wurden, für die Zwecke der Leistungsbewertung, der unternehmensinternen Netzwerkanalysen zur Aufdeckung informeller Strukturen und zur Zufriedensheitsbzw. Effizienzanalyse ohne vorherige Information beim Beginn der Verarbeitung an die Betroffenen, ebenso eine grundsätzliche Zweckinkompatibilität. Aufgrund des engen Spielraums des Art 6 Abs 4 Hs 2 lit c DSGVO – begründet durch die hohe Sensibilität der Daten (IT-Protokolldaten) – ist keine Zweckkompatibilität herstellbar. Bereits die bisherigen § 31 BDSG aF für Deutschland bzw. § 14 Abs 4 DSG 2000 aF für Österreich kamen zu selben

1030 *Art 29 Datenschutzgruppe*, WP 203 (2013) 24 f.

1031 *Goricnik/Grünanger* in Grünanger/Goricnik (Hrsg) Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) Rn 2.71; *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 6 Rn 56 f.

Ergebnis. Als einzige Lösung bietet sich an, diese zusätzlichen Zwecke bereits bei der Erhebung mitzuberücksichtigen und Betroffene darüber ausreichend zu informieren oder die Einwilligung nach Art 6 Abs 4 Hs 1 DSGVO einzuholen.[1032]

d) *die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen.*

Hier werden die voraussichtlichen Auswirkungen einer geplanten Weiterverarbeitung geprüft. Sowohl positive als auch negative Auswirkungen sind dabei gleichberechtigt zu berücksichtigen. Im Rahmen dieser Folgenabschätzung sind auch potentielle zukünftige Entscheidungen und Handlungen von Dritten mit zu berücksichtigen bis hin zur Gefahr von Diskriminierungen und Ausgrenzung der Betroffenen. Auch müssen potentielle emotionalen Auswirkungen in die Kompatibilitätsprüfung miteinbezogen werden wie bspw. Angst, Irritation, Bedrängnis und Schmerz, die daraus resultieren, wenn ein Betroffener die Kontrolle über sensible personenbezogene Informationen verliert bzw. realisiert, dass diese kompromittiert wurden. Ebenso ist wichtig im Rahmen der weiteren Verarbeitung zu prüfen, wie die Daten weiterverarbeitet werden sollen, also ob sie durch einen anderen Verantwortlichen in einem anderen Kontext verarbeitet werden sollen mit unbekannten Konsequenzen, bzw. ob die Daten einer größeren Zahl von Menschen bekannt gemacht werden sollen, oder ob eine große Menge personenbezogener Daten mit anderen Daten verarbeitet, kombiniert bzw. abgeglichen werden sollen (Profiling). Solche Weiterverarbeitungen sind grundsätzlich zum Zeitpunkt der Erhebung für Betroffene nicht vorhersehbar.

Generell gilt auch hier der Grundsatz, je negativer oder ungewisser die möglichen Auswirkungen einer Verarbeitung sind, desto eher ist eine Weiterverarbeitung als nicht vereinbar mit dem ursprünglichen Zweck der Datenerhebung anzusehen bzw. desto enger ist der Spielraum einer kompatiblen Weiterverarbeitung. Ein wichtiges Kriterium ist insbesondere, ob die Weiterverarbeitung ausschließlich bei dem ursprünglichen Verantwortlichen erfolgt, oder ob ein Dritter infolge der Weiterverarbeitung Kenntnis von den Daten erlangt.[1033]

Hinsichtlich der Weiterverarbeitung von ursprünglich zu IT-Sicherheitszwecken erhobenen Beschäftigtendaten (siehe oben) stellen sich hier ebenso Probleme. Eine Zweckänderung der Daten für die Zwecke der Leistungsbewertung, der unternehmensinternen Netzwerkanalysen zur Aufdeckung informeller Strukturen und/oder zur Zufriedensheits- bzw. Effizienzanalyse kann massive Folgen für Betroffene haben, die eine solche Weiterverarbeitung nicht vorhersehen konnten, weil sie zum Zeitpunkt der Erhebung nicht über diesen zusätzlichen Zweck der Weiterverarbeitung informiert wurden. Die mit der Weiterverarbeitung verbundenen Risiken beinhalten für Betroffene: finanzielle Verluste, erhebliche wirtschaftliche oder gesellschaftliche Nachteile (Arbeitsplatzverlust) und Rufschädigung inklusive

1032 *Art 29 Datenschutzgruppe*, WP 203 (2013) 25 f; *Buchner/Petri* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 6 Rn 189; *Eßer* in Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer BDSG [aF][4] (2014) § 31 Rn 9; *Gola/Klug/Körffer* in Gola/Schomerus (Hrsg), BDSG [aF][12] (2015) § 31 Rn 5; *Pollirer/Weiss/Knyrim*, DSG[2] (2014) § 14 Rn 15; *Knyrim*, Datenschutzrecht[3] (2015) 261 ff (263).

1033 *Art 29 Datenschutzgruppe*, WP 203 (2013) 25 f; *Buchner/Petri* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 6 Rn 190.

fortgesetzter Beobachtung durch Dritte, etc. Folglich ergibt sich auch auf dieser Stufe eine Inkompatibilität mit dem ursprünglichen Verarbeitungszweck der IT-Sicherheit.[1034]

e) *das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.*

Geeignete Garantien können problematische Aspekte in Rahmen der Kompatibilitätsprüfung kompensieren. Dazu gehören Verschlüsselung, Pseudonymisierung, gesteigerte Transparenz mit der Möglichkeit des Betroffenen zu widersprechen. Neben den klassischen Zielen der IT-Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) spielen die spezifischen Datenschutzziele (Transparenz, Nicht-Verkettbarkeit, Intervenierbarkeit, Datenminimierung) ebenso eine bedeutende Rolle. Maßnahmen der Nicht-Verkettbarkeit spielt dabei mA eine ganz besonders entscheidende Rolle.[1035]

Hinsichtlich der Weiterverarbeitung von ursprünglich zu IT-Sicherheitszwecken zur Verwendung für die Zwecke der Leistungsbewertung, der unternehmensinternen Netzwerkanalysen zur Aufdeckung informeller Strukturen und zur Effizienzsteigerung könnten ausreichende Garantien in diesem Kontext entgegen der klaren negativen Ergebnisse in den Punkten a) – d) diese möglicherweise kompensieren, wenn durch die pseudonyme Nutzung für den einzelnen Betroffenen die Risiken weitgehend so minimiert werden bzw. es klar nur um allgemeine Analysen auf höherer Ebene geht (z.B. „*Makro-Level*“[1036]). *Eickelpasch* sieht durch die Einbeziehung von konkreten technischen und organisatorischen Schutzmaßnahmen in die Kompatibilitätsbetrachtung eine hilfreiche Möglichkeit, doch noch Zweckkompatibilität einer Verarbeitung herzustellen.[1037] Allerdings wird dies von *Gola/Jaspars* hinsichtlich IT-Sicherheitsprotokolldaten klar und eindeutig verneint.[1038] Nach *Schulz* – mit Verweis auf die BfDI – kann genau dieser Punkt der „geeigneten Garantien“ bei Big Data-Anwendungen die praktische Relevanz haben, denn es zeige, dass auch das Zusammenspiel verschiedener Kompatibilitätsaspekte letztlich eine Weiterverarbeitung legitimieren könne.[1039]

5.4.6 Ergebnis Big Data in der Arbeitswelt

Für Big Data Analysen zur Lagebildaufbereitung für Beschäftigte im Rahmen ihrer beruflichen Tätigkeit über einen Digitalen Assistenten (z.B. proaktive Informations- und Handlungsvorschläge aus Datenanalysen) bedarf es vor Analysebeginn zum neuen Zweck des Zweckkompatibilitätstestes gemäß Art 6 Abs 4 Hs 2 DSGVO, nämlich ob die zweckgebunden gespeicherten Daten zu diesem neuen Zweck zweckkompatible verarbeitet (analysiert) werden dürfen. Gemäß ErwGr 50 Satz 2 DSGVO ist dann keine neue Rechtsgrundlage mehr erforderlich, die Weiterverarbeitung stützt sich auf die bisherige Rechtsgrundlage.

Nachträgliche Big Data Analysen über die Beschäftigten des Unternehmens selbst, sind aufgrund des Grundsatzes von Treu und Glauben hingegen schwerer zu legitimieren, da für

1034 *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 6 Rn 59.
1035 *Art 29 Datenschutzgruppe*, WP 203 (2013) 26 f.
1036 *Roßnagel,* ZD 2013, 562.
1037 *Eickelpasch*, Sonderveröffentlichung zu RDV 06/2017, 7.
1038 *Gola/Jaspars*, RDV 3/2018, 145 ff.
1039 *Schulz* in Gola (Hrsg), DS-GVO[2] (2018) Art 6 Rn 209.

den neuen Verwendungszweck noch ein innerer Zusammenhang zum Beschäftigtenverhältnis bestehen muss.[1040] *Gola/Jaspars* stellen klar, dass die Nutzung sämtlicher Daten und Datenspuren bis auf Ebene der Protokolldateien eines Beschäftigten in einem Big Data System zur Mitarbeiterbewertung jedenfalls unzulässig ist. Auch die Bewertung der Kommunikation der Beschäftigten in sozialen Netzwerken zur Ermittlung der Arbeitszufriedenheit oder der Kündigungswahrscheinlichkeit mittels Big Data Systemen sei nach *Gola/Jaspars* datenschutzrechtlich nicht zulässig, weil sie zweckinkompatibel mit dem Zweck der Durchführung des Beschäftigtenverhältnisses sind. Gleiches gelte für die Ermittlung der sozialen Graphen der Beschäftigten in Auswertung der betrieblichen elektronischen Kommunikationswege. Denn auch unternehmensinterne Netzwerkanalysen können informelle Strukturen sichtbar machen und ermöglichen es die Informationsbeziehungen von Beschäftigten zu beobachten und damit ihre soziale Stellung im Unternehmen – unabhängig von der formalen Stellung – zu analysieren. Durch eine solche Netzwerkanalyse wird ersichtlich, wer in der Belegschaft angesehen und einflussreich ist und wer eher peripher ist und wo sich dienstlich/private Gruppen und Clans im Unternehmen gebildet haben.[1041] Zudem ist es möglich über Big Data Analysen den eventuellen Karriereverlauf eines Mitarbeiters im Unternehmen (z.B. wann er den Arbeitsplatz wahrscheinlich wechseln wird) anhand vergleichender Daten vorherzusagen. Anschließend können Maßnahmen zur Bindung des Mitarbeiters an das Unternehmen ergriffen werden. Umgekehrt kann ein über Big Data Analysen „geschätzter" hypothetisch angenommener Abwanderungswille dazu führen, dass die Karriere des Beschäftigten im Unternehmen nicht mehr gefördert wird bzw. einen negativen Verlauf nimmt. Solche Big Data Analysen über Beschäftigte lassen sich schwer mit dem Grundsatz der Zweckbindung und Zweckvereinbarkeit in Einklang bringen und sind im Anwendungsbereich der DSGVO als unzulässig anzusehen.[1042]

Letztlich bedeutet dies, dass der Einsatz von Big Data Technologien von Beginn an – soweit wie objektiv möglich – bereits mit enstsprechender Angabe sämtlicher (wahrscheinlich) intendierter Zwecke als eigene Verarbeitungstätigkeiten im Verzeichnis der Verarbeitungstätigkeiten dokumentiert werden sollte inkl. Information der Betroffenen darüber (Treu und Glauben), um nicht später in die Problematik einer mangelnden Zweckkompatibilität zu kommen. Das heißt für eine geplante Verarbeitung iZh mit Big Data Analysen sollten von Beginn gleich mehrere intendierte Zwecke angegeben werden.

1040 *Datenschutzkonferenz*, Kurzpapier Nr. 14 – Beschäftigtendatenschutz (2018) 3.
1041 *Gola/Jaspars*, RDV 3/2018, 145 ff.
1042 *Gola,* Datenschutz am Arbeitsplatz[5] (2014) Rn 34.

5.5 Enterprise Search Suchmaschine

5.5.1 Überblick

Eine Suchmaschine wird definiert als ein Programm zur Recherche von Dokumenten und sonstigen Daten, die an einem Computer oder Computernetzwerk gespeichert sind. Konkreter handelt sich dabei um Computerprogramme, die einen definierten Datenbestand in Datenbanken schnell und systematisch nach dem Vorhandensein bestimmter Informationen durchsuchen und das Ergebnis einem Anfragenden sogleich anzeigen.

Man kann aufgrund der zu durchsuchenden Informationsquellen (des Suchraums) folgende zwei Arten von Suchmaschinen unterschieden:

- öffentliche Internet-Suchmaschinen (z.B. Google Search).
- unternehmensinterne Suchmaschinen (Enterprise Search).

Beide Arten von Suchmaschinen zeichnen sich an der Benutzeroberfläche („Front-end") durch folgende Gemeinsamkeiten aus: „Ein-Feld-Ansatz", sämtliche Suchbegriffe werden in ein einziges Feld eingegeben, es werden die Suchergebnisse innerhalb kürzester Zeit geliefert, die Darstellung der Ergebnisse erfolgt in Listenform.[1043]

- *öffentliche Internet-Suchmaschinen*

Der von einer Internetsuchmaschine (z.B. Google Search) zu durchsuchende Suchraum besteht vorwiegend aus WWW Internetseiten im HTML Format und dort verlinkten Standardformaten wie PDF, Microsoft Word oder Excel. Der Zugriff auf die Daten erfolgt über das HTTP-Protokoll. Über das Internet zugängliche nicht-öffentliche Datenbanken werden von einer öffentlichen Internet-Suchmaschinen in den meisten Fällen nicht indexiert, daher beschränkt sich der Suchraum einer öffentlichen Internetsuchmaschine auf unstrukturiert vorliegende Daten. Internetsuchmaschinen untersuchen nur den öffentlich-zugänglichen Teil des Internets, Fragen über Zugriffsberechtigungen und eine dbzgl. Berücksichtigung von Rechte und Rollen einzelner Nutzer stellen sich insofern nicht.[1044]

- *unternehmensinterne Suchmaschine (Enterprise Search)*

Unternehmensinterne Suchmaschinen müssen mit einem ganz anderen viel heterogeneren Suchraum umgehen als öffentliche Internetsuchmaschinen. Die Daten in einem Unternehmen liegen auf verschiedenen Speicherorten, auf die mit unterschiedlichen Protokollen zugegriffen werden muss. Zudem wird in Unternehmen häufig mit speziellen Datenformaten gearbeitet, die ebenfalls durchsucht werden müssen. Auch kann bei unternehmensinternen Suchmaschinen auf strukturiert vorliegende Daten zurückgegriffen werden (z.B. CRM-Datenbank). Daher müssen unternehmensinterne Suchmaschinen in der Lage sein, sowohl strukturierte als auch unstrukturierte Daten zu indexieren. Zudem müssen die Rollen und

1043 *Egermann* in Kilian/Heusen (Hrsg), Computerrecht (34. Ergänzungslieferung 2018) Suchmaschinen Rn 1 ff; *Elixmann*, Datenschutz und Suchmaschinen (2012) 39 ff; *Lewandowski*, Whitepaper Enterprise Search (2010), abrufbar unter: https://searchstudies.org/wp-content/uploads/2019/04/Whitepaper-Enterprise-Search-Was-die-Nutzer-erwarten-und-warum-Social-Media-so-entscheidend-ist.pdf (zuletzt abgerufen am 20.06.2019).

1044 *Egermann* in Kilian/Heusen (Hrsg), Computerrecht (34. Ergänzungslieferung 2018) Suchmaschinen Rn 1 ff; *Karg* in Jandt/Steidle (Hrsg), Datenschutz im Internet (2018) 263 ff.

Berechtigungen verschiedener Quellsysteme erfasst werden und den indexierten Daten zugeordnet werden. Ein Nutzer darf bei unternehmensinternen Suchmaschinen nur die Daten angezeigt bekommen, die er auch im jeweiligen Quellsystem einsehen könnte. Alle anderen Daten müssen ausgeblendet werden bzw. er darf darauf nicht zugreifen dürfen. Das erfordert im Ergebnis ein System der Nutzerauthentifizierung. Während Internet-Suchmaschinen auf Basis verschiedener Daten und Ranking-Algorithmen ein Ranking von Suchergebnissen vornehmen können, liegen diese für ein Ranking erforderlichen Daten (z.B. Wichtigkeit einer Website anhand der auf sie verweisenden Links und entsprechendes Ranking im Suchergebnis) innerhalb eines Unternehmens nicht vor, weil es bspw. nur äußerst wenige miteinander verlinkte HTML-Dateien gibt (daher gibt die Linkpopularität kaum Aufschluss über die Wichtigkeit einer gefundenen Informationsquelle). Bei unternehmensinternen Suchmaschinen müssen daher andere Ranking Algorithmen eingesetzt werden.[1045]

Bei den gängigen unternehmensinternen Suchmaschinen kann man darüberhinaus hinsichtlich der Art und Weise der Suche zwischen *indexbasierten Suchmaschinen* und *Metasuchmaschinen* unterscheiden.

- *indexbasierte Suchmaschine*

Die Funktionsweise einer indexbasierten Suchmaschine wird in drei Bereiche gegliedert:

- Die entsprechenden elektronischen Dokumente müssen in den Computernetzwerken und Unternehmensdatenbanken gefunden werden. Bei Internetsuchmaschinen erfolgt dies bspw. über Crawler (Spider), welche die Weiten des WWW nach neuen Inhalten durchsuchen und herunterladen. Um eine schnelle Suche sicherzustellen, müssen Suchmaschinen im Vorfeld alle für Suchanfragen relevante Inhalte (z.B. im Internet sämtliche Websites von Suchanfragen) erfassen und vollautomatisch ohne inhaltliche Prüfung in einem Datenbank-Index abspeichern.
- Die Vielzahl der ermittelten Daten wird dabei vor der Speicherung in den Datenbank-Index durch eine spezielle Indexierung-Software (Indexer) analysiert, ausgewertet, zugeordnet und strukturiert (Information Retrieval Systeme zur Aufbereitung der Daten – „Wiederfinden von Informationen“) und anschließend an die Datenbank der Suchmaschine übermittelt, wo die herunter geladene Seite verkürzt in den Index aufgenommen wird. Diese automatische Lokalisierung, Konvertierung und Indexierung der gefundenen Informationen erfolgt völlig unabhängig von den einzelnen Suchanfragen eines Nutzers. Die Suchmaschinenergebnisse des Nutzers werden nämlich nicht in Echtzeit aus dem Internet gewonnen, sondern aus der Datenbank der Suchmaschine erzeugt. Je nach dem Grad der Übereinstimmung werden die Ergebnisse der Suchanfrage sortiert, man bezeichnet ein solches hierarchisierendes, nach Plausibilität abgestuftes Verfahren als „Ranking“ (Auswertung der Indexdaten und anschließende Darstellung anhand der

1045 *Stocker,* Enterprise Search: Potenziale und Fallstricke (2015) 2 ff, abrufbar unter: https://www.researchgate.net/publication/274388399_Enterprise_Search_Potenziale_und_Fallstricke (zuletzt abgerufen am 20.06.2019); *Lewandowski*, Whitepaper Enterprise Search (2010), abrufbar unter: https://searchstudies.org/wp-content/uploads/2019/04/Whitepaper-Enterprise-Search-Was-die-Nutzer-erwarten-und-warum-Social-Media-so-entscheidend-ist.pdf (zuletzt abgerufen am 20.06.2019); *Wiegand*, Einführung einer Enterprise Search Lösung und Erweiterung dieser um Aspekte einer Search Based Application (2012), Diplomarbeit Otto von Guericke Universität Magdeburg Fakultät für Informatik, Betreuer Prof. Dr. rer. Pol. Habil. Hans-Knud Arndt, 26 ff.

Relevanzkriterien in der Trefferanzeige der Suchmaschine). Das Ranking erfolgt semantisch an Hand objektiver Wertungskriterien mit Hilfe sogenannter „Ranking-Algorithmen".

- Letztlich müssen die individuellen Suchanfragen der Nutzer beantwortet werden. Dies erfolgt über ein Abfragemodul, das auf die Suchanfrage des Nutzers die Trefferliste generiert. Die Trefferliste zeigt bspw. bei Internetsuchmaschinen die Adresse oder einen kurzen Textauszug aus einem Dokument (Snippet) an. Zudem vermittelt die Suchmaschine den Zugang durch eine Verlinkung auf die Quelle.[1046]

Für indexbasierte Suchmaschinen in einem Unternehmen stellen sich konkret zwei datenschutzrechtlich relevante Sachverhalte dar:[1047]

I. Die Verarbeitung der erhobenen und im Suchindex gespeicherten Daten aus den mit Crawlern durchsuchten Datenbanken, Computernetzwerken und Quellen und

II. die Verarbeitung der Daten über ihre Nutzer (Protokolldateien) inklusive der Möglichkeit Profile zu erstellen.[1048]

Die technische Umsetzung sieht bei einer *Client-Server indexbasierten Suchmaschine* wie folgt aus: Es werden Suchanfragen über einen Client-Rechner (Benutzerschnittstelle z.B. via Intranet-Seite) an einen zentralen Server gestellt. Der Suchserver hält den Suchindex vor, bearbeitet die Suchanfrage und ermittelt dem Nutzer das Suchergebnis. Damit übernimmt der Server sowohl die Erstellung des Suchindexes als auch die Bearbeitung von Suchanfragen (Berechnung der Rangfolge der einzelnen Suchergebnisse). Der Server kann mit Hilfe entsprechender Schnittstellen grundsätzlich auf alle im Unternehmensnetzwerk verfügbaren Datenquellen zugreifen. Zur Berücksichtigung von Zugriffsberechtigungen müssen diese während der Indexierung mitausgelesen werden und der Nutzer muss sich vor Suchanfragen vor dem Server identifizieren (Abgleich der zwischen den am Suchserver angemeldeten Nutzer und deren quellenspezifischen Zugriffsrechten z.B. dadurch, dass die Nutzer sich am Suchserver mit denselben Zugangsdaten anmelden, die sie auch für den Zugriff auf das Quellsystem verwenden oder ein Mapping von am Suchserver hinterlegten Informationen mit den Berechtigungsdaten der Nutzer zur Nutzung des Quellsystems).[1049]

1046 *Karg* in Jandt/Steidle (Hrsg), Datenschutz im Internet (2018) 263 ff; *Elixmann*, Datenschutz und Suchmaschinen (2012) 39 ff; *Egermann* in Kilian/Heussen (Hrsg) Computerrecht (34. Ergänzungslieferung 2018), Suchmaschinen Rn 1 ff; *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 53 ff; EuGH GA v. 25.06.2013, C-131/12 („Google Spain SL u.a.") Rn 32 ff; Rn 46; EuGH Urteil v. 13.05.2014, C-131/12 ("Google Spain SL u.a.") Rn 27 f; *Herrmann*, Das Recht der Suchmaschinen – Ausgewählte Rechtsprobleme der Suchmaschine Google (2010), Dissertation Universität Wien, Betreuer ao. Univ.-Prof. Dr. Wolfgang Zankl, 32 ff.

1047 EuGH GA v. 25.06.2013, C-131/12 ("Google Spain SL u.a.") Rn 70.

1048 *Art 29 Datenschutzgruppe*, WP 148 (2008) 5 f; *Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (IWGDPT)*, Resolution on Privacy Protection and Search Engines (2006) 1 f; *Weichert*, Datenschutz bei Suchmaschinen, in D. Lewandowski (Hrsg) Handbuch Internetsuchmaschinen (2009) 286.

1049 *Wiegand*, Einführung einer Enterprise Search Lösung und Erweiterung dieser um Aspekte einer Search Based Application (2012), Diplomarbeit Otto von Guericke Universität Magdeburg Fakultät für Informatik, Betreuer Prof. Dr. rer. Pol. Habil. Hans-Knud Arndt, 47 f.

- *Metasuchmaschine*

Die Funktionsweise einer Metasuchmaschine (sekundäre Suchmaschinen) ist anders. Metasuchmaschinen besitzen selbst keinen Suchindex, sondern sie bauen auf bestehende Suchmöglichkeiten über andere Suchmaschinen auf. Technisch betrachtet, leiten Metasuchmaschinen eine Suchanfrage an mehrere andere primäre Suchmaschinen der Quellsysteme weiter und tragen die Treffer der einzelnen primären Suchmaschinen der Quellsysteme auf einer eigenen Trefferliste zusammen. Daher ist bei Metasuchmaschinen – mangels eigenem Index – grundsätzlich nur die Verarbeitung der Nutzerdaten inkl. Profiling aus Datenschutzgesichtspunkten relevant.[1050]

5.5.2 Verarbeitung personenbezogener Daten im Suchindex der Suchmaschine[1051]

Dieses Thema betrifft grundsätzlich nur indexbasierte Suchmaschinen (Enterprise Search). Um eine schnelle Suche sicherzustellen, müssen indexbasierte Suchmaschinen im Vorfeld alle für Suchanfragen relevante Inhalte erfassen und vollautomatisch (defacto ohne inhaltliche Prüfung) in einem Datenbank-Index abspeichern. Unternehmensinterne Suchmaschinen sollen dabei strukturierte und unstrukturierte Daten in unterschiedlichen Formaten und an verschiedenen Speicherorten mit einer zentralen Suchfunktion abfragen können.[1052] Am Digitalen Arbeitsplatz von heute stößt man auf verschiedene angebundene Systeme, Fileserver, Datenbanken, webbasiertes Intranet und Social Collaboration Komponenten.[1053] All diese Systeme müssen von einer internen Suchmaschine durchsuchbar und die relevanten Ergebnisse müssen für die suchenden Mitarbeiter anschaulich angezeigt werden können. Die Mitarbeiter übermitteln dabei der internen Suchmaschine die Begriffe und die interne Suchmaschine sucht diese nach Übereinstimmungen in ihrem Index, der aus allen zu durchsuchenden Daten erstellt wurde. Der Suchindex besteht grundsätzlich aus dem Volltext und sollte nicht beschränkt sein auf reine Metadaten. „Relevant" bedeutet für die Suchmaschine ganz allgemein, ob eine Übereinstimmung der Begriffe vorliegt. Ein Nutzer benötigt jedoch mehr Präzision, nämlich eine Eingrenzung der Suchergebnisse, die seinen Vorstellungen und Suchbedürfnissen entspricht. Allgemeine Kriterien wie Trefferanzahl und –dichte, Erstellungsdatum und Ursprung des Suchergebnisses helfen dabei, aber um optimale Ergeb-

1050 *Elixmann*, Datenschutz und Suchmaschinen (2012) 45; *Egermann* in Kilian/Heussen (Hrsg) Computerrecht (34. Ergänzungslieferung 2018), Suchmaschinen Rn 1 ff; *Herrmann*, Das Recht der Suchmaschinen – Ausgewählte Rechtsprobleme der Suchmaschine Google (2010), Dissertation Universität Wien, Betreuer ao. Univ.-Prof. Dr. Wolfgang Zankl, 31; *Wiegand*, Einführung einer Enterprise Search Lösung und Erweiterung dieser um Aspekte einer Search Based Application (2012), Diplomarbeit Otto von Guericke Universität Magdeburg Fakultät für Informatik, Betreuer Prof. Dr. rer. Pol. Habil. Hans-Knud Arndt, 53.

1051 EuGH GA v. 25.06.2013, C-131/12 ("Google Spain SL u.a.") Rn 70.

1052 *Schonschek*, Interne Suchmaschinen: So geht's datenschutzkonform, abrufbar unter: https://www.datenschutz-praxis.de/fachartikel/wie-sich-interne-suchmaschinen-datenschutzkonform-einsetzen-lassen/ (zuletzt abgerufen am 20.06.2019); *Art 29 Datenschutzgruppe*, WP 148 (2008) 17 ff.

1053 *Stocker,* Enterprise Search: Potenziale und Fallstricke (2015) 2 ff, abrufbar unter: https://www.researchgate.net/publication/274388399_Enterprise_Search_Potenziale_und_Fallstricke (zuletzt abgerufen am 20.06.2019); *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 81.

nisse zu liefern, muss jede Suchmaschine speziell konfiguriert werden, nach den Ansprüchen und Bedürfnissen ihres Einsatzgebietes – also unternehmensspezifisch. Das beginnt am Anfang bei der Frage welche Teile und Datenfelder von Inhalten indexiert werden sollen.[1054]

Werden in die unternehmensinterne Suchmaschine Datenbanken, Systeme und Collaboration Tools mit personenbezogenen Daten einbezogen, bestehen Datenschutz-Risiken:

- ohne entsprechende technische und organisatorische Maßnahmen beziehen interne Suchmaschinen personenbezogene Daten in die Abfrage-Ergebnisse mit ein, auf die nicht jeder Nutzer Zugriff haben darf.
- die Suchmaschine fragt unter Umständen Speicherbereiche ab, die nicht für den Nutzer-Zugriff des Suchanfragestellenden vorgesehen sind.
- der Suchindex enthält in komprimierter Form alle Daten des Unternehmens, die indexiert wurden (Risiko von unbefugten Zugriffen auf den Suchindex).
- interne Suchmaschinen können Schnappschüsse (Snapshots) der durchsuchten Dokumente anlegen für schnelle Ergebnis-Präsentation. Die Snapshots liegen im Suchmaschinen-Cache. Dieser Suchmaschinen-Cache bleibt auch nach Löschung der Ursprungsdatei weiter durchsuchbar, womit Daten ggf. nicht gelöscht werden.[1055]

Die Datenschutzrechtliche Prüfung beinhaltet:

Rechtmäßigkeit, Treu und Glauben und Transparenz

Die Rechtmäßigkeit einer Verarbeitung wird grundsätzlich durch einen datenschutzrechtlichen Erlaubnistatbestand sichergestellt. Ein Suchindex einer Enterprise Search greift aber lediglich zweckändernd auf bereits vorliegende zweckgebundene personenbezogene Daten zusätzlich zur Erstellung eines Suchindexes zu (Weiterverarbeitung). Gemäß ErwGr 50 Satz 2 DSGVO ist bei zweckkompatibler Verarbeitung (zweckgebundene Daten werden für den Zweck der „Suchfunktionalität“ in einem zusätzlichen Suchindex weiterverarbeitet) dann kein neuer Erlaubnistatbestand erforderlich. Im Rahmen der Zweckkompatibilität stützt sich die zweckkompatible Verarbeitung grundsätzlich weiter auf den bisherigen Erlaubnistatbestand (z.B. Art 6 Abs 1 lit f DSGVO bzw. § 26 BDSG) der Verarbeitung des Primärzwecks.[1056]

Wichtigster Punkt für die Rechtmäßigkeit ist, dass eine Enterprise Search sicherstellen muss, dass nur derjenige Daten überhaupt suchen, sie finden und darauf zugreifen darf, der dazu auch wirklich befugt ist (entsprechend Rollen- und Rechtekonzepte der Quellsysteme). Dazu bedarf es gut geregelter Zugriffsrechte im Unternehmen. Bei bestehenden und gut funktionierenden Zugriffsrechten im Unternehmen hält sich eine unternehmensinterne Suchmaschine (Enterprise Search) nur noch an diese Zugriffsrechte, die es im Unternehmen ohnehin schon gibt. Dies geschieht wie folgt:

1054 *Arbeitsplatz 4.0.,* Suchmaschine fürs Intranet gesucht? Das gibts zu beachten…, abrufbar unter: https://www.arbeitsplatz40.de/intranet-suche/ (zuletzt abgerufen am 20.06.2019).

1055 *Schonschek*, Interne Suchmaschinen: So geht’s datenschutzkonform, abrufbar unter: https://www.datenschutz-praxis.de/fachartikel/wie-sich-interne-suchmaschinen-datenschutzkonform-einsetzen-lassen/ (zuletzt abgerufen am 20.06.2019).

1056 *Schulz* in Gola (Hrsg), DS-GVO^2 (2018) Art 6 Rn 210 ff; *Feiler/Forgó,* EU-DSGVO (2017) Art 6 Rn 15.

- Jeder Mitarbeiter meldet sich an seinem Rechner mit Namen und Passwort an.
- Damit authentifiziert sich der Mitarbeiter im Firmennetz.
- Im Benutzerkonto des Mitarbeiters ist hinterlegt, wer der Mitarbeiter ist und was er darf. Diese hinterlegten Daten sind quasi wie ein „virtueller Ausweis".
- Diese hinterlegten Zugriffsrechte des Mitarbeiters im Benutzerkonto („virtueller Ausweis") nutzt zugleich auch die Enterprise Search. Nachdem die Suchmaschine die Identität des Mitarbeiters festgestellt hat, weiß die Enterprise Search sofort, wo (in welchen Datenquellen) sich der Mitarbeiter umsehen darf und wo nicht.
- Benutzt der Mitarbeiter die Enterprise Search, werden nur die indexierten Datenquellen durchsucht und dem Mitarbeiter nur Dokumente daraus als Suchvorschläge angezeigt, auf die er auch ohne Enterprise Search Zugriffsrechte hätte. Es ist äußerst wichtig, dass eine Enterprise Search nur bestimmte Daten für eine genau definierte Nutzergruppe zugänglich machen darf, denn es geht nicht nur darum, dass ein Mitarbeiter gesperrte Dokumente nicht lesen darf, sondern dass ein Mitarbeiter überhaupt nicht nach für ihn gesperrten Dokumenten suchen darf.[1057]

Im Idealfall muss sich der Mitarbeiter nur einmal bei der Anmeldung an seinen Computer authentifizieren („Single Sign-on").[1058]

Die Grundsätze von Treu und Glauben und Transparenz werden durch eine jederzeit abrufbare und leicht auffindbar Datenschutzerklärung auf der Startseite der internen Suchmaschine mit den Inhalten gemäß Art 13 und Art 14 DSGVO sichergestellt.[1059]

Darüberhinaus können die Anforderungen an Treu und Glauben (Fairness) und Transparenz zusätzlich durch ein Kommunikationskonzept umgesetzt werden. Dabei werden die Nutzer vorab intensiv über die Funktionalität der internen Suchmaschine aufgeklärt. Es erfolgt dabei auch eine Datenschutzaufklärung der Mitarbeiter als Betroffene, dass weiterhin nur jeder das sehen kann, wofür er eine Berechtigung auch hat, insbesondere dann, wenn alle Mitarbeiter zukünftig eine korrekt Datenablage sicherstellen und keine Dokumente entgegen ihrer unternehmensinternen Klassifizierung in falschen Ablagen und Systemen ablegen.[1060]

Zudem erfolgt eine Klarstellung, dass durch Enterprise Search keine Überwachung von Beschäftigten möglich wird, denn E-Mail-Postfächer, etc. werden nicht im Suchindex für die Enterprise Search indexiert.[1061]

Zweckbindung und Zweckvereinbarkeit

Im Rahmen der Implementierung einer Suchmaschine und der Erstellung eines Suchindexes für die Funktionsfähigkeit der internen Suchmaschine wird auf zweckgebundene Daten zu einem neuen Zweck der „Suchfunktionalität" zugegriffen (Art 5 Abs 1 lit b iVm. Art 6

1057 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 42 ff; 105 ff.
1058 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 43.
1059 *Art 29 Datenschutzgruppe*, WP 148 (2008) 25 ff.
1060 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 123 ff.
1061 *Schütt*, Der Weg zum Digitalen Unternehmen[2] (2015) 57.

Abs 4 Hs 2 DSGVO). Mangels Einwilligung bzw. einer qualifizierten datenschutzrechtlichen Erlaubnisnorm im Unionsrecht oder im Recht der Mitgliedstaaten (Art 6 Abs 1 Hs 1 DSGVO) zum Betrieb einer internen Suchmaschine im Unternehmen, bedarf es für die Verarbeitungstätigkeit „Suchindex" des Kompatibilitätstests. Folgende Prüfschritte sind zu berücksichtigen (Art 6 Abs 4 Hs 2 lit a – lit e DSGVO):

- *jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung.*

Zu prüfen ist, ob eine Verbindung zwischen dem Primärzweck und dem geplanten Sekundärzweck „unternehmensinterne Suchmaschinenfunktion" besteht. Es ist also zu fragen, ob der Sekundärzweck mehr oder weniger im Primärzweck impliziert war oder sich als ein logischer Schritt der Verarbeitung des Primärzwecks darstellt. Je weiter die Entfernung des Primärzwecks und des Sekundärzwecks ist, desto umfassender bedarf es der Analyse der Zweckkompatibilität.[1062]

In diesem Fall ist mA der Sekundärzweck „Suchfunktionalität" im Primärzweck impliziert, da heute jedermann im Rahmen einer Datenverarbeitung auch eine entsprechende Suchfunktionalität annimmt und erwartet. Voraussetzung für die Annahme ist aber, dass sich an den Benutzer- und Zugriffsrechten der zu findenden Daten durch die Aufnahme im Suchindex der internen Suchmaschine – mit Ausnahme der Suchmaschinen Administratoren – nichts ändert. Die Mitarbeiter dürfen über die interne Suchmaschine und damit über den Suchindex ausschließlich nur dieselben Daten finden, wie wenn sie manuell mit ihren Berechtigungen die bestehenden Verzeichnisse und Quellsysteme durchkämmt hätten.

- *den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen.*

Hier wird auf den spezifischen Kontext, in dem die personenbezogenen Daten erhoben wurden und in die damit verbundenen vernünftigen Erwartungen einer betroffenen Person („reasonable expectation of privacy"), in eine zukünftige mögliche Weiterverarbeitung abgestellt. Es geht also um die Sicht des Betroffenen – was kann eine vernünftige Person in der Lage des Betroffenen im Kontext der Datenerhebung erwarten hinsichtlich einer möglichen Weiterverarbeitung? Je unerwarteter und überraschender eine solche Zweckänderung erfolgt, desto wahrscheinlicher ist eine Inkompatibilität der Weiterverarbeitung.[1063]

Eine „reasonable expectation of privacy" ist gegeben, zugleich erwarten Mitarbeiter in der heutigen Zeit funktionierende unternehmensinterne Suchfunktionen, um ihre Arbeit effizient gestalten zu können. Werden die Benutzer- und Zugriffsrechte durch die Enterprise Search nicht verletzt und rechtswidrig erweitert, wird mA auch die „reasonable expectation of privacy" der betroffenen Beschäftigten nicht verletzt.

1062 *Art 29 Datenschutzgruppe*, WP 203 (2013) 23 f.

1063 *Art 29 Datenschutzgruppe*, WP 203 (2013) 22 ff; *Buchner/Petri* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 6 Rn 188.

- *die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden.*

Hier wird geprüft, welche Art von personenbezogenen Daten von der Weiterverarbeitung erfasst sein sollen. Die Art der Daten spielt hier eine entscheidende Rolle, also ob sensitive Daten (Art 9 bzw. Art 10 DSGVO) oder ob Kommunikationsdaten, Standortdaten oder andere hochsensible Daten verarbeitet werden sollen.[1064]

Im Rahmen der Einführung einer Enterprise Search Lösung ist anhand des Verzeichnisses der Verarbeitungstätigkeiten (Art 30 Abs 1 lit c DSGVO) zu prüfen, ob bei den zu indexierenden Systemen, Datenbanken und Collaborations Tools auch besondere Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO) bzw. personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Art 10 DSGVO) enthalten sind und damit auch im Suchindex verarbeitet werden würden. Im Regelfall wird das bei einer unternehmensinternen Suchmaschine nicht der Fall sein, denn solche Daten sollten nicht im Suchindex einer Enterprise Search enthalten sein, weil schlicht unternehmensinterne Anwendungsfälle (Ausnahme z.B. bei Ärzten und medizinischem Personal, etc.) hinsichtlich solcher sensitiver Daten fehlen.

Auch Kommunikationsdaten (eMails, individuelle Chats) werden grundsätzlich nicht durch den Suchmaschinenindex erfasst, da sich in den wenigsten Fällen ein berechtigtes Interesse bzw. eine Erforderlichkeit für das Beschäftigtenverhältnis an der allgemeinen Verfügbarkeit und Auffindbarkeit von individueller eMail-Kommunikation (inkl. privaten Inhalten) begründen lässt (Ausnahmen ggf. rein dienstlich genützte Gruppenpostfacher, die ohnehin einem größeren Nutzer/Betroffenenkreis zur Verfügung stehen sollen). Demgemäß werden grundsätzlich keine solchen Daten durch den Suchindex erfasst.[1065]

In einem Suchindex werden aber folgende unternehmensöffentliche Kommunikationsdaten erfasst, an deren Verfügbarkeit durch Suchfunktion ein berechtigtes Interesse des Unternehmens besteht ohne, dass die schutzwürdigen Betroffeneninteressen überwiegen: Enterprise Social Media, Blogs, Wikis, Collaboration Tools. Wird in diesen Anwendungen – umfassend durch unternehmensinterne Nutzungsbedingungen sichergestellt – nur fachlich bzw. dienstlich kommuniziert, wird ein erhebliches betriebliches Wissen generiert und elektronisch verfügbar gemacht. Bei Sicherstellung der rein dienstlichen bzw. fachlichen Kommunikation, können die dortigen Inhalte auch nach Aussscheiden des „postenden" Mitarbeiters aufgrund berechtigter Interessen weitergespeichert werden, weil keine privaten Daten vorliegen und damit kein überwiegend berechtigtes Betroffeneninteresse besteht.[1066]

1064 *Art 29 Datenschutzgruppe*, WP 203 (2013) 25 f; *Buchner/Petri* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 6 Rn 189.

1065 *Schütt*, Der Weg zum Digitalen Unternehmen[2] (2015) 57.

1066 *Schütt*, Der Weg zum Digitalen Unternehmen[2] (2015) 57.

- *die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen.*

Es sind die voraussichtlichen Auswirkungen der geplanten Weiterverarbeitung zu prüfen:[1067] Grundsätzlich liegen die Daten im Unternehmen bereits vor, sie werden im Rahmen der Suchindexerstellung lediglich dupliziert, insofern liegt ein ähnliches Risiko vor wie bei Back Ups, vorausgesetzt die Zugriffs- und Benutzerrechte werden durch die Enterprise Search nicht erweitert. Es entsteht folglich ein gewisses erhöhtes Risiko aufgrund der doppelten Datenhaltung; dieses Risiko ist mA nicht höher wie im Rahmen der ohnehin erforderlichen mehrfachen Back Up Sicherung.

- *das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.*

Geeignete Garantien können problematische Aspekte in Rahmen der Kompatibilitätsprüfung kompensieren. Dazu gehören Verschlüsselung, Pseudonymisierung, gesteigerte Transparenz, etc. Neben den klassischen Zielen der IT-Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) spielen die spezifischen Datenschutzziele (Transparenz, Nicht-Verkettbarkeit, Intervenierbarkeit) ebenso eine bedeutende Rolle. Hervorzuheben ist insbesondere die Maßnahme der Nicht-Verkettbarkeit.[1068] Ein Suchindex einer unternehmensinternen Suchmaschine sollte auf jeden Fall nur verschlüsselt gespeichert werden, als wichtige Maßnahme iSd. Art 32 DSGVO.[1069] Als Ergebnis zeigt sich mA die Zweckkompatibilität der Erstellung eines Suchmaschinenindex aus zweckgebundenen personenbezogenen Daten im Unternehmen zum Betrieb einer Enterprise Search.

Datenminimierung

Der Grundsatz der Datenminimierung beim Suchindex wird durch entsprechende technische und organisatorische Maßnahmen sichergestellt.

Maßnahmen zur Datenminimierung in einem Suchindex sind:

- Es muss konkret und transparent festgelegt werden, welche Datenbestände mit Bezeichnung des Quellsystems / der Anwendung indexiert werden und für welche Fachbereiche diese Indices überhaupt erforderlich sind. Nicht ratsam ist es, einfach das nächstbeste Programm über den gesamten Datenbestand zu schicken, mit der abstrakten Mission, einfach alles für die unternehmensinterne Suchmaschine zu indexieren.
- Es muss vor der Indexierung der Daten ein „Finderkonzept" erstellt werden, das heißt es muss festgelegt werden, welche Daten von wem wo gefunden werden dürfen, welche Daten auf welche Indizes (falls mehrere angelegt) indexiert werden.

1067 *Art 29 Datenschutzgruppe*, WP 203 (2013) 25 f; *Buchner/Petri* in Kühling/Buchner, DS-GVO BDSG[2] (2018) Art 6 Rn 190; *Heberlein* in Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 6 Rn 59.

1068 *Art 29 Datenschutzgruppe*, WP 203 (2013) 26 f; *Schulz* in Gola (Hrsg), DS-GVO[2] (2018) Art 6 Rn 209.

1069 *Schonschek*, Interne Suchmaschinen: So geht's datenschutzkonform, abrufbar unter: https://www.datenschutz-praxis.de/fachartikel/wie-sich-interne-suchmaschinen-datenschutzkonform-einsetzen-lassen/ (zuletzt abgerufen am 20.06.2019).

- Es hat durch Einsicht in das Verzeichnis der Verarbeitungstätigkeiten eine Dokumentation zu erfolgen, welche Art von Daten indexiert werden (Art 30 Abs 1 lit c DSGVO).[1070]
- Es ist festzulegen, wem die Daten zugänglich gemacht werden sollen. Dies geschieht durch eine automatische Übernahme der bereits existierenden und funktionierenden Strukturen und Rechtesysteme der individuellen Zugriffsrechte eines jeden Mitarbeiters auf die bestehenden Systeme (dbzgl. Dokumentation erforderlich, dass dies durch die Suchmaschine nicht verändert werden kann). Das bestehende Berechtigungssystem muss ebenso für die Suchmaschine gelten bzw. übernommen/integriert werden.[1071]
- Es hat zudem eine Unterscheidung zu erfolgen zwischen Suchindex-Berechtigung (wer hat Zugriff auf den Index als Ganzen) und Datenquellen-Berechtigungen (welcher Mitarbeiter hat Zugriffsrechte in welchen Systemen – bleiben entsprechend dem bisherigen Zugriffs- und Berechtigungskonzept) inkl. Dokumentation.[1072]
- Es ist darzulegen wie viele Suchindizes angelegt werden sollen, denn kleinere Indices sind leichter aktualisierbar als große Indices.[1073]
- Ein wesentliches Element des Grundsatzes der Datenminimierung ist die Filterung: Durch den Einsatz eines Indexfilters können sensible Dokumente, die bei der Suche gar nicht zur Verfügung stehen sollen (z.B. falsch abgelegte „geheime“ oder „vertrauliche“ Dokumente), herausgefiltert werden. Dies kann entweder durch die Anpassung der Indexierungsfilter geschehen oder durch die Vergabe entsprechender Berechtigungen an den zu indexierenden Datenbestand.[1074] Mit Hilfe einer Black-List Filterung besteht die Möglichkeit, Dokumente ganz aus der Suche auszublenden, das heißt es können sensible Dokumente anhand eines Such-Ausdrucks aus dem Index ausgeblendet werden. Die auf diese Art ausgeblendeten Daten sind dann für keinen Nutzer mehr sichtbar. Mit Hilfe von Black-List Filterung kann die Sichtbarkeit von Dokumenten in der Suchmaschine reduziert werden ohne, dass der Zugriff auf die Dokumente in den Datenquellen dadurch beeinflusst wird.[1075]
- Mit Hilfe einer effektiven Filterung können letztlich sensible falsch abgelegte Dokumente (= entgegen ihrer unternehmensinternen Klassifizierung abgelegt) vorab im Rahmen der Indexierung entsprechend identifiziert und herausgefiltert werden, ohne dass ein Nicht-Berechtigter über die Falschablage eines Kollegen und die dann mögliche leichtere Auffindbarkeit über Enterprise Search auf die falsch abgelegten Daten stößt.

Datenrichtigkeit

Die Datenrichtigkeit wird durch eine regelmäßige Aktualisierung des Suchindex sichergestellt.

1070 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 130 ff.

1071 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 42 ff; 105 ff;

1072 *Daoud*, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016) 4 ff.

1073 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 130 ff.

1074 *Daoud*, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016) 5.

1075 *Daoud*, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016) 5.

Speicherbegrenzung

Im Rahmen der regelmäßigen Aktualisierung des Suchindexes sind in den Quellsystemen gelöschte Daten auch im Suchindex zu löschen, da der Zweck der Speicherung im Suchindex mit der Löschung der Daten im Quellsystem erreicht ist und keine Erforderlichkeit für eine weitere Speicherung im Suchindex mehr besteht.

Integrität und Vertraulichkeit

Zur Sicherstellung des Grundsatzes der Integrität und Vertraulichkeit muss besonders auf die Benutzerrechte geachtet werden. Liegen funktionierende Benutzerrechte im Unternehmen vor, muss nicht viel geändert werden (siehe oben). Das Rechtesystem muss klar gewährleisten welcher Mitarbeiter welche Zugriffsrechte auf Systeme hat. Insbesondere ist wichtig, dass ein Mitarbeiter Informationen und Dateien, auf die er keine Zugriffsrechte hat, nicht nur nicht finden darf, er soll danach gar nicht suchen dürfen. Denn bereits im Rahmen der internen Suche kann ein Mitarbeiter durch die Voransicht auf ein für ihn gesperrtes Dokument relevante Informationen erhalten, die für ihn nicht relevant sind, auch wenn der Mitarbeiter das eigentliche Dokument gar nicht öffnen kann.[1076]

Da mittlerweile Home-Office oder mobiles Arbeiten Standard ist, ist der Zugriff auf die Suchmaschine und unternehmensinterne Daten und Systeme nur über ein Virtual Private Network (VPN) zu ermöglichen. Die VPN-Technik stellt sicher, dass niemand unterwegs auf die Firmendaten zugreifen kann.[1077]

Als weitere Maßnahmen zur Sicherstellung der Integrität und Vertraulichkeit erfolgt eine regelmäßige Sensibilisierung der Mitarbeiter in ihrer Rolle als Nutzer auf korrekte Datenablage je unternehmensinterner Klassifizierung und ihrer Benutzerrechte, denn eine Falschablage hat nach Etablierung der Enterprise Search viel gravierendere Auswirkungen, denn sobald die Indexierung erfolgt ist, sind falsch abgelegte Daten für jeden Nutzer mit gleichen Benutzerrechten viel leichter auffindbar als bisher, womit falsch abgelegte Daten oder in Worddokumenten abgespeicherte (z.B. in Unterordnern versteckte) Passwörter für jeden mit der gleichen Nutzerberechtigung sofort sichtbar werden können. Vor Kick-off einer Enterprise Search Lösung ist eine zeitliche Frist festzulegen, damit Mitarbeiter vor dem Start der Indexierung die bisherigen Datenbestände auch rechtskonform aufräumen können.

Die Datensicherheits- und IT-Sicherheitsmaßnahmen sind für den Suchindex genauso in der gleichen Intensität vorzunehmen wie für die Daten im Quellsystem selbst:

- Suchmaschine liefert erst nach lokaler Anmeldung am Netzwerk Suchergebnisse, d.h. die Suchmaschine braucht die Rechte ihres Anwenders, um zu suchen. Ohne Anmeldung sind auch Suchergebnisse nicht zugänglich.[1078]

1076 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 42 ff; 105 ff; *Daoud*, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016) 4 ff.

1077 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 114.

1078 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 42 ff; 105 ff.

- Suchindex muss vor unbefugten Zugriff ausreichend geschützt sein – Kenntnisnahme sowohl der Daten selbst als auch des Suchindexes nur durch autorisierte Benutzer;
- Suchindex u. Daten selbst dürfen nicht unbemerkt verändert werden können;
- Suchmaschinen Cache muss ebenso gelöscht werden, dbzgl. Umgang mit Snapshots regeln, dass diese nicht existieren obwohl Ursprungsdatei bereits gelöscht;
- Indexverschlüsselung und nur verschlüsselte Übertragung;
- Audit Logging.[1079]

Kein Datenabfluss an den externen Anbieter, der ggf. die Softwarelösung anbietet. Der Index muss im Unternehmen bleiben, ausgenommen es liegt Cloud Computing vor und die Quellsysteme wurden ohnehin bereits in die Cloud transferiert.[1080]

5.5.3 Die Verarbeitung der Daten über ihre Nutzer (Protokolldateien)[1081]

Dieses Thema betrifft sowohl indexbasierte Suchmaschinen als auch Metasuchmaschinen.[1082] Es werden Protokolldaten der Suchmaschinennutzung erhoben.[1083] (Internet-)Suchmaschinen protokollieren u.a. bspw. zumindest folgende Daten der Nutzer:

- IP Adresse des anfragenden Rechners,
- Cookie-Kennung des von der Suchmaschine bei einer vorherigen Sitzung gesetzten (falls vorhanden),
- Flashcookie (falls vorhanden),
- Datum und Uhrzeit der Anfrage,
- Inhalt der Suchanfrage,
- Browserversion des Nutzers,
- Sprachversion des Browsers,
- Benutzerspezifische Einstellungen in erweiterten Dienstumgebungen,
- Betriebssystemversion,
- Desktopauflösung,
- Website von der der Nutzer auf die Suchseite gekommen ist (Referrer),
- Welchen Links aus der Trefferliste der Nutzer gefolgt ist.[1084]

1079 *Daoud*, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016) 6.

1080 *Lange*, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009) 81 f.

1081 EuGH GA v. 25.06.2013, C-131/12 ("Google Spain SL u.a.") Rn 70.

1082 *Art 29 Datenschutzgruppe*, WP 148 (2008) 5 f; *Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (IWGDPT)*, Resolution on Privacy Protection and Search Engines (2006) 1 f; *Weichert* in D. Lewandowski (Hrsg) Handbuch Internetsuchmaschinen (2009) 286.

1083 *Art 29 Datenschutzgruppe*, WP 148 (2008) 17 ff.

1084 *Feldmann* in Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019) Teil XI. Kapitel 4. Rn 4; *Elixmann*, Datenschutz und Suchmaschinen (2012) 47; *Art 29 Datenschutzgruppe*, WP 148 (2008) 31; *Knyrim,* Suchmaschinen andersrum: Datenschutzrechtliche Implikationen von Suchmaschinen und Web-Analyse-Tools in Österreichische Juristenkommission (Hrsg), Alles unter Kontrolle? (2009) 119; *Egermann* in Kilian/Heusen (Hrsg), Computerrecht (34. Ergänzungslieferung 2018) Suchmaschinen Rn 24.

Rechtmäßigkeit, Treu und Glauben und Transparenz

Es liegt eine Neuerhebung von personenbezogenen Daten vor, die einer Prüfung bedarf:

Art 6 Abs 1 lit f DSGVO (EU, Österreich)[1085]	**§ 26 Abs 1 Satz 1 BDSG (Deutschland)[1086]**
Liegen berechtigte Interessen vor? Effizienzsteigerung der Arbeitsleistung durch bessere Suchergebnisse am Arbeitsplatz. Aufgrund einer funktionierenden internen Suchmaschine werden auch Doppelarbeiten vermieden. *Ist die Verarbeitung zur Verfolgung des berechtigten Zweckes erforderlich?* Ohne die Verarbeitungstätigkeit ist der effiziente Einsatz der unternehmensinternen Suchmaschine nicht möglich. Weniger stark in die Privatssphäre eingreifende Mittel sind nicht möglich. *Abwägung der Interessen, also ob die Grundrechte und Grundfreiheiten oder Interessen des Betroffenen die berechtigten Interessen des Verantwortlichen überwiegen.* Im Rahmen dieser Abwägung überwiegen aufgrund der hohen wirtschaftlichen Effizienzsteigerung grundsätzlich die berechtigten Interessen des Arbeitgebers. Zudem bestehen neben den entgegengesetzten Datenschutzinteressen der Arbeitnehmer auch mit dem Arbeitgeber gleichlaufende Interesse an der Verfügbarkeit einer effektiven internen Suchmaschine um bessere Arbeitsergebnisse zu erzielen. *Herstellung eines letztendlichen Gleichgewichts der Interessen durch Berücksichtigung zusätzlicher Schutzmaßnahmen (Einsatz von Technologien und Maßnahmen zur Stärkung der Privatssphäre).* Es werden entsprechende technische und organisatorische Maßnahmen eingeleitet, welche die Datenschutzrisiken für die Arbeitnehmer abfangen. Für die Datensicherheit erfolgt zur Sicherstellung des Art 32 DSGVO im erforderlichen Ausmaß eine personenbezogene Protokollierung. Diese IT-Sicherheitsprotokolldaten werden ausschließlich für die Zwecke der Integrität und Vertraulichkeit (Art 5 Abs 1 lit f DSGVO) verwendet. Es erfolgt (grundsätzlich) keine personenbezogene Protokollierung zur erforderlichen Suchmaschinenoptimierung, sondern es werden für diesen Zweck alle Daten vorher vollständig anonymisiert.	*Berechtigte Zwecke (Ziele) auf Seiten des Arbeitgebers im Zusammenhang mit der Durchführung des Beschäftigtenverhältnisses?* Effizienzsteigerung der Arbeitsleistung durch bessere Suchergebnisse am Arbeitsplatz. Aufgrund einer funktionierenden internen Suchmaschine werden auch Doppelarbeiten vermieden. *Geeignetheit (Erheblichkeit)* Die Einführung einer unternehmensinternen Suchmaschine ist geeignet, den angestrebten Zweck zu erreichen und fördert diese Zweckerrereichung. *Erforderlichkeit im engeren Sinne* Es geht hier darum, ob Maßnahmen gleicher Eignung bestehen, anstatt der geplanten. Das ist nicht der Fall. Für den erfolgreichen Einsatz der unternehmensinternen Suchmaschine ist die Verarbeitung auch im engeren Sinn erforderlich. *Angemessenheit (Verhältnismäßigkeit im engeren Sinn)* Hier erfolgt eine Abwägung der widerstreitenden Interessen: Im Rahmen dieser Abwägung überwiegen aufgrund der hohen wirtschaftlichen Effizienzsteigerung grundsätzlich die berechtigten Interessen des Arbeitgebers. Zudem bestehen neben den entgegengesetzten Datenschutzinteressen der Arbeitnehmer auch mit dem Arbeitgeber gleichlaufende Interesse an der Verfügbarkeit einer effektiven internen Suchmaschine, um bessere Arbeitsergebnisse zu erzielen. Es werden entsprechende technische und organisatorische Maßnahmen eingeleitet, welche die Datenschutzrisiken für die Arbeitnehmer abfangen. Für die Datensicherheit erfolgt zur Sicherstellung des Art 32 DSGVO im erforderlichen Ausmaß eine personenbezogene Protokollierung. Diese IT-Sicherheitsprotokolldaten werden ausschließlich für die Zwecke der Integrität und Vertraulichkeit (Art 5 Abs 1 lit f DSGVO) verwendet. Es erfolgt (grundsätzlich) keine personenbezogene Protokollierung zur erforderlichen Suchmaschinenoptimierung, sondern es werden für diesen Zweck alle Daten vorher vollständig anonymisiert.

1085 *Art 29 Datenschutzgruppe*, WP 217 (2014) 70 ff.
1086 *Oberthür* in Kramer (Hrsg), IT-Arbeitsrecht (2017) Kapitel B Rn 427 f.

Die Interessensabwägung (Art 6 Abs 1 lit f DSGVO) bzw. die Erforderlichkeitsprüfung (§ 26 Abs 1 BDSG) hinsichtlich der Verarbeitung der Protokolldaten ergibt mA dann ein positives Ergebnis, wenn entsprechende technische und organisatorische Maßnahmen eingeleitet werden, um die Betroffenenrisiken zu reduzieren.[1087]

Allgemein gilt, dass eine unternehmensinterne Suchmaschine grundsätzlich keine personenbezogenen Daten erheben sollte, die nicht unbedingt aus den Gründen der Datensicherheit gemäß Art 32 DSGVO erforderlich sind, weil für die Zwecke der Suchmaschinenoptimierung (bessere Suchergebnisse) anonyme Daten in der Regel völlig ausreichen:[1088]

Die beiden Grundsätze von Treu und Glauben und Transparenz werden durch eine jederzeit abrufbare Datenschutzerklärung am der Enterprise Search Startseite im Intranet des Unternehmens, welche die Anforderungen der Art 12 ff DSGVO erfüllt, sichergestellt.[1089]

Bei den Protokolldaten handelt es sich – siehe oben – um neu erhobene Daten und nicht wie beim Suchmaschinenindex um eine zweckändernde Datenverarbeitung.

Zweckbindung

Die Protokolldaten werden insbesondere für folgende Zwecke im Rahmen einer unternehmensinternen Suchmaschine erhoben:

- *Systemsicherheit (Art 32 DSGVO):* Die Server-Protokolle tragen zur Sicherheit der Suchmaschine bei, da man durch die Server-Protokolldaten wiederkehrende Muster erkennen kann und so Sicherheitsbedrohungen analysieren kann. Die Zweckbindung dieser personenbezogenen Protokolldaten beschränkt sich klar auf die Sicherstellung der Integrität und Vertraulichkeit gemäß Art 5 Abs 1 lit f iVm. Art 32 DSGVO.
- *Verbesserung des Dienstes:* Mit Hilfe der Server-Protokolle wird es möglich, das Dienstleistungsangebot und die Qualität der Suchmaschine zu verbessern. Die Auswertung der Server-Protokolle wird als wichtiges Instrument gesehen, die Qualität der Suchvorgänge und die Suchergebnisse zu verbessern.[1090]

Datenminimierung

Es werden nur solche Daten protokolliert, die für die genannten Zwecke erforderlich sind:

- *Systemsicherheit (Art 32 DSGVO):* Nach Ansicht der *Art 29 Datenschutzgruppe* unterliegen die personenbezogenen Protokolldaten für die Datensicherheit einer strengen

1087 EuGH Urteil v. 13. Mai 2014 C-131/12 (Google Spain) Rn 73; *Art 29 Datenschutzgruppe*, WP 148 (2008) 19; *Karg* in Jandt/Steidle (Hrsg), Datenschutz im Internet (2018) 263 ff; *Arbeitsplatz 4.0.,* Suchmaschine fürs Intranet gesucht? Das gibts zu beachten…, abrufbar unter: https://www.arbeitsplatz40.de/intranet-suche/ (zuletzt abgerufen am 20.06.2019).

1088 *Art 29 Datenschutzgruppe*, WP 148 (2008) 20; *Daoud*, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016) 6.

1089 *Art 29 Datenschutzgruppe*, WP 148 (2008) 25 ff.

1090 *Art 29 Datenschutzgruppe*, WP 148 (2008) 17 ff; *Elixmann*, Datenschutz und Suchmaschinen (2012) 49 ff; *Herrmann*, Das Recht der Suchmaschinen – Ausgewählte Rechtsprobleme der Suchmaschine Google (2010), Dissertation Universität Wien, Betreuer ao. Univ.-Prof. Dr. Wolfgang Zankl, 108 ff.

Zweckbindung (Art 5 Abs 1 lit f DSGVO – Sicherstellung der Integrität und Vertraulichkeit) und dürfen nicht für andere Zwecke verarbeitet werden (klare Datentrennung durch Nicht-Verkettbarkeit). Die Verarbeitung der dazu erforderlichen personenbezogenen Daten werden als berechtigtes Interesse angesehen.[1091]

- *Verbesserung des Dienstes:* Die Speicherung der Benutzeranfragen in den Server-Protokollen kann ein Instrument zur Verbesserung des Dienstes darstellen, denn die Daten ermöglichen die Analyse der Arten der Suchanfragen und die Verfeinerung der der Suchergebnisse durch die Auswertung der vom Benutzer weiterverfolgten Suchergebnisse. Für diesen Vorgang ist aber in der Regel keine Identifizierung des Benutzers erforderlich. Um die Aktionen eines einzelnen Benutzers zu korrelieren (z.B. um zu ermitteln, ob die Vorschläge der Suchmaschine hilfreich sind), ist lediglich eine Abgrenzung der Aktionen eines Benutzers bei einer bestimmten Suchanfrage von denen eines anderen Benutzers notwendig. Demgemäß sind soweit wie möglich nur anonyme bzw. anonymisierte Daten für die Zwecke der Diensteverbesserung zu speichern und zu verarbeiten.[1092] Die Erhebung zusätzlicher personenbezogener Daten über die Benutzer ist insbesondere hinsichtlich von Zwecken der Systemverbesserung nicht notwendig – es reichen dazu in der Regel anonyme Daten aus – und ist damit grundsätzlich unzulässig.[1093]

Somit hat eine vollständige Anonymisierung der Suchmaschinen-Protokolle zu erfolgen. Personenbezogenen Suchmaschinen-Protokolldaten, die aus Gründen der Systemsicherheit (Art 32 DSGVO) unbedingt personenbezogen gespeichert werden müssen, sollten pseudonymisiert und getrennt (Nicht-Verkettbarkeit) ausschließlich für die Zwecke der Datensicherheit gespeichert werden (Art 25 iVm. Art 32 DSGVO).[1094]

Etwaige Nutzerprofile – z.B. iZh mit dem Betrieb des Digitalen Assistenten – sollten wenn möglich in Hashwerten gespeichert werden.[1095]

Datenrichtigkeit

Die Datenrichtigkeit wird durch regelmäßige Aktualisierung der Protokolldaten (und ggf. der pseudonymen Nutzerprofile) sichergestellt.

Speicherbegrenzung

Protokolldaten der Suchmaschinennutzung sollten nicht länger als 6 Monate gespeichert werden. Werden Protokolldaten länger gespeichert, bedarf es einer umfassenden Begründung.[1096]

1091 *Art 29 Datenschutzgruppe*, WP 148 (2008) 20.
1092 *Art 29 Datenschutzgruppe*, WP 148 (2008) 20.
1093 *Art 29 Datenschutzgruppe*, WP 148 (2008) 29.
1094 *Art 29 Datenschutzgruppe*, WP 148 (2008) 20.
1095 *Art 29 Datenschutzgruppe*, WP 148 (2008) 20; *Daoud*, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016) 6.
1096 *Art 29 Datenschutzgruppe,* WP 148 (2008) 21 ff.

Integrität und Vertraulichkeit

Die Suchmaschinen-Protokolldaten werden grundsätzlich anonymisiert und nur soweit zur Sicherstellung der Anforderungen an die Datensicherheit gemäß Art 32 DSGVO pseudonymisiert gespeichert.[1097] Etwaige Nutzerprofile werden – soweit möglich – verschlüsselt in Hashwerten gespeichert.[1098]

5.5.4 Ergebnis Enterprise Search

Letztlich zeigt sich, dass eine Enterprise Search Lösung datenschutzkonform im Unternehmen implementiert werden kann, wenn gewisse Maßnahmen zum Datenschutz getroffen werden.

5.6 Gesamtergebnis

Der Einsatz eines Digitalen Assistenten inklusive Big Data Technologien und Enterprise Search ist unter folgenden Bedingungen mA datenschutzkonform möglich:

Cloud Computing

- Sicherstellung der Transparenz über sämtliche (denkmögliche) Empfänger der Daten (Auftragsverarbeiter, Subauftragsverarbeiter sowie auch staatliche Zugriffsrechte auf den Cloud Anbieter);[1099]
- Sicherstellung der Nicht-Verkettbarkeit durch technische und organisatorische Maßnahmen. Die beim Cloud Anbieter gespeicherten Daten dürfen nicht durch diesen (rechtswidrig) für eigene Zwecke verarbeitet werden können. Eine solche Möglichkeit darf gar nicht technisch möglich sein (z.B. ausreichende Verschlüsselung);
- Verschlüsselung nach Stand der Technik inkl. Schlüssel grundsätzlich beim Cloud Anwender und nicht beim Cloud Anbieter; ggf. Ausnahmen von diesem strengen Grundsatz bei personenbezogenen Daten, die gemäß interner Datenklassifizierung als grundsätzlich wenig risikobehaftet einzustufen werden;
- Auswahl der Cloud Serverstandorte und Heranziehung von Subdienstleistern nicht nur nach reinen Kostengesichtspunkten, sondern auch aus dem Blickwinkel des darauf anwendbaren Rechtssystems (Staatliche Grundrechte vorhanden? Grundrechte am Serverstandort nur als reine Staatsbürgerrechte oder als Menschenrechte ausgestaltet? Umfassende gesetzliche Zugriffs- und Übermittlungspflichten für Privatunternehmen an staatliche Dienste, Sicherheits- und Strafverfolgungsbehörden mit entsprechenden Rechtschutzmechanismen und nachträglicher Transparenz für Betroffene vorhanden? Ein aufwändiges Telekommunikationsüberwachungsprogramm in Betrieb?);
- Der Einsatz von Cloud Computing außerhalb Europas bringt einerseits zwar große Kostenvorteile, erhöht aber gleichzeitig die Datenschutzrisiken (vgl. **Kapitel 6.2**). Innerhalb Europas besteht zumindest über Art 8 EMRK ein ausjudizierter rechtlicher Schutz vor staatlichen Zugriffen in allen Politikbereichen (inkl. nationale Sicherheit) auf ursprünglich zu privaten und wirtschaftlichen Zwecken verarbeiteten Daten. Durch die Art 7 und

1097 *Art 29 Datenschutzgruppe,* WP 148 (2008) 20.
1098 *Daoud*, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016) 6.
1099 Art 28 Abs 3 lit a DSGVO.

Art 8 EU-GRC und Art 6 Abs 1 lit c iVm. Abs 2 und Abs 3 DSGVO sowie die Datenschutzrichtlinie (EU) 2016/680 für Polizei und Strafjustiz existieren zudem auch über die Europäische Union unionsrechtliche Anforderungen für staatliche Verarbeitungen auch z.B. zu strafrechtlichen Zwecken oder zur Abwehr von Gefahren für die öffentliche Sicherheit (im EU-Recht aber klar ausgenommen: „nationale Sicherheit"). Beim Cloud Computing außerhalb Europas ergeben sich zusammengefasst folgende Risiken:

- *Fehlende Vertraulichkeit und Einbußen bei der Datenhoheit:* Daten können grundsätzlich nur unverschlüsselt verarbeitet werden, dies führt zum Problem, dass die Cloud als reine ausgelagerte Festplatte nicht die Wettbewerbs- und Größenvorteile der Cloud als gleichzeitige Rechenmaschine bietet. Wird die Cloud auch als Rechenmaschine eingesetzt und dazu ein Anbieter z.B. aus den USA ausgewählt, kann jeder US Cloud Anbieter nach US Recht (FISA Abschnitt 702) unmittelbar angewiesen werden, geheim den Schlüssel bzw. die unverschlüsselten Daten selbst, flankiert durch sogenannte „Gag Orders"[1100], an die entsprechenden US Dienste auszuhändigen. Der US Cloud Provider hat nach *Bowden* dabei kein Wahlrecht. Es ist seine gesetzliche Pflicht aus dem amerikanischen Recht, die mit hohen Sanktionen für die CEOs bei Nichtbefolgung untermauert ist. Verschlüsselung ist daher nach *Bowden* in dieser Konstellation, wo die Cloud nicht nur als verschlüsselte externe Festplatte, sondern auch als Rechenmaschine („Compute Engine") dienen soll, z.B. mit einem US Cloud Anbieter hinsichtlich der Abwehr eines Zugriffs von US Behörden völlig zwecklos, da der US Cloud Anbieter die bei ihm hinterlegten Schlüssel geheim ex lege sofort herausgeben müsse. Der europäische Cloud Nutzer und die Betroffenen erfahren davon nichts (Normenkollision zwischen US-Recht und EU-Datenschutzrecht). Deshalb schützt – etwas verallgemeinert – eine noch so starke Verschlüsselung einer als Rechenmaschine genutzten Non-EU-Drittstaats-Cloud nur vor Angriffen von externen Hackern oder anderen Staaten, nicht aber vor einem Zugriff des Staates des Cloud Anbieters, welcher sich auf ein gültiges nationales Gesetz für einen Datenzugriff berufen kann (siehe **Kapitel 6.2**). Es könnten Ersuchen von drittstaatlichen Strafverfolgungsbehörden direkt an den Cloud Provider als Auftragsverarbeiter im Drittstaat gerichtet werden. Damit besteht das Risiko einer Datenherausgabe an drittstaatliche Strafverfolgungsbehörden ohne Einhaltung der europäischen Datenschutzvorschriften bzw. der Nicht-Respektierung völkerrechtlicher Abkommen zum zwischenstaatlichen Datenaustausch mit der EU und den EU-Mitgliedstaaten.[1101] Zur Sicherstellung der Vertraulichkeit und Datenhoheit sind Clouds innerhalb des Europäischen Rechtssystems sinnvoller. Die Wahrscheinlichkeit ist deutlich höher, dass ein europäischer Cloud Anbieter, der sich bspw. einer Anordnung durch eine Drittstaatsbehörde bzw. einen Drittstaatsdienst ausgesetzt sieht, erheblichen Widerstand leisten wird, als ein Non-EU-Cloud Anbieter, wo für CEOs unmittelbare und horrende Sanktionen bei Nichtbefolgung direkt in ihrem eigenen Heimatstaat drohen (siehe **Kapitel 6.2**).[1102]

1100 *Barnitzke*, Rechtliche Rahmenbedingungen der Cloud Computing (2014) 282.

1101 *Art 29 Datenschutzgruppe*, WP 196 (2012) 6 ff.

1102 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 41 f.

- *Fehlende Isolierung:* Es besteht das Risiko, dass Informationen verschiedener Cloud-Anwender rechtswidrig miteinander verbunden werden könnten. Dies würde geschehen, wenn der Cloud Anbieter seine physische Kontrolle über die Daten aller Anwender zur rechtswidrigen Verknüpfung all dieser Daten nutzt, um daraus einen persönlichen Mehrwert oder einen Mehrwert für interessierte Dritte zu generieren.
- *Mangelnde Transparenz:* Es könnte eine Kettenverarbeitung zahlreicher Auftragsverarbeiter stattfinden ohne Wissen des Verantwortlichen bzw. Cloud Nutzers, mit dem Risiko, dass personenbezogene Daten in Drittländer übermittelt werden, mit der sofortigen Gefahr des unmittelbaren Zugriffs durch Behörden aus dem Drittstaat, ohne Wissen und Möglichkeit der Risikoabschätzung des Cloud Nutzers und Verantwortlichen.[1103]

Enterprise Search

- Die Erstellung eines Suchindex der Enterprise Search ist – bei Sicherstellung diverser erforderlicher datenschutzfreundlicher Maßnahmen – als zweckkompatible Verarbeitungstätigkeit (Art 6 Abs 4 Hs 2 iVm. ErwGr 50 Satz 2 DSGVO) anzusehen. Wichtigste Maßnahme ist, dass die Enterprise Search die Rechte und das Rollenkonzept der Datenquellsysteme übernehmen kann und umfassend respektiert, womit Nutzer über die Enterprise Search nur solche Informationen überhaupt suchen dürfen, die sie auch bei einer normalen Suche in Quellsystemen ohne Enterprise Search suchen könnten, denn bereits Suchergebnisse mit Dokumenten mit Hinweis der mangelnden Zugriffsrechte sind bereits zuviel Information für unbefugte Nutzer.
- Zur Sicherstellung der Datensicherheit (Art 32 DSGVO) kann es erforderlich sein personenbezogene Protokolldaten für die Enterprise Search für die Zwecke der Integrität und Vertraulichkeit (Art 5 Abs 1 lit f DSGVO) zu speichern. Durch eine tatsächliche Datentrennung (Nicht-Verkettbarkeit) ist zu gewährleisten, dass diese Protokolldaten auch tatsächlich ausschließlich für diese Zwecke verarbeitet werden. Ist dies nachweisbar der Fall, greift für diese Protokolldaten in Deutschland auch die Ausnahme von der Auskunftspflicht an Betroffene gemäß § 34 Abs 1 Nr 2 lit b BDSG.
- Daten für die Suchmaschinenoptimierung müssen im Regelfall nicht in personenbezogener Form gespeichert werden, es reichen anonymisierte Daten.
- Eine Enterprise Search Suchmaschine darf nur auf solche Enterprise Social Collaboration Tools zugreifen, bei welchen im Rahmen von Nutzungsbedingungen eindeutig klargestellt wurde, dass nur eine dienstliche Nutzung im Rahmen von Projektarbeiten erfolgt (Wikis, Enterprise Social Media, Bloqs, etc.). Eine Indexierung der eMail-Postfächer insbesondere bei erlaubter Privatnutzung ist ausgeschlossen und grundsätzlich nicht erlaubt (ggf. ausgenommen Gruppenpostfächer mit rein dienstlicher Nutzung).

Digitaler Assistent

- Für die Sprachsteuerung und damit verbundene Erstellung von Audiodateien ist eine straf- (§ 201 dStGB bzw. § 120 öStGB) und ausdrückliche datenschutzrechtliche Einwilligung (Art 9 Abs 2 lit a DSGVO) erforderlich. Es handelt sich bei den Sprachbefehlen (digitale Sprache) um besondere Arten personenbezogener Daten, weil aus Gründen

1103 *Art 29 Datenschutzgruppe*, WP 196 (2012) 6 ff.

der Datensicherheit (Art 32 DSGVO) über die gesprochene Stimme auch gleichzeitig eine korrekte Authentifizierung des Sprechenden zu erfolgen hat, damit keine Unbefugten Zugang zu den Informationen des Digitalen Assistenten allein über Sprachbefehle erhalten (ErwGr 51 Satz 3, Art 9 Abs 1 DSGVO). Der Nutzer hat jederzeit die Möglichkeit die Audiodateien seiner Sprachbefehle zu löschen. Entsprechend der betrieblichen Löschfristen weiter gespeichert – wie die übliche elektronische Kommunikation des Betriebes – können die transkribierten Texte (digiale Texte) der sprachlichen Anfragen (z.B. über Sprachsteuerung transkribiertes eMail) an den Digitalen Assistenten, wie wenn sie direkt von der Tastatur gekommen wären.[1104]

- Freiwilligkeit der Einwilligung hinsichtlich der Sprachsteuerung (Audiodateien bzw. digitale Sprache) besteht, da der Nutzer die Sprachsteuerung des Digitalen Assistenten nicht benutzen muss, sondern auch per Tastatur mit dem Digitalen Assistenten kommunizieren kann ohne tatsächliche Nachteile (ausgenommen die geringere Usability) zu erleiden (Art 7 Abs 4; ErwGr 155 DSGVO).
- Profiling (Art 4 Nr 4 DSGVO) ist für den Betrieb des Digitalen Assistenten erforderlich und stellt aber zugleich einen erheblichen Eingriff in das Persönlichkeitsrecht der Arbeitnehmer dar. Es werden effektive eingriffslindernde Maßnahmen gesetzt z.B. individuelle Abschaltbarkeit des Digitalen Assistenten durch die Nutzer; Profiling erfolgt nicht über ein umfassendes Profil, sondern es werden im Rahmen des Profilings ausschließlich nur Teilaspekte des beruflichen Wirkens des Betroffenen verarbeitet; das Level der Detailliertheit des Profils wird ausschließlich an den Erfordernissen für den Betrieb des Digitalen Assistenten orientiert und wird so wenig eingriffintensiv wie möglich ausgestaltet; es erfolgt eine Pseudonymisierung und weitere im konkreten Einzelfall mögliche Maßnahmen im Zusammenhang mit Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen; es erfolgt eine starke Verschlüsselung der pseudonymen Nutzerprofile in der Cloud. So wird es mA möglich, ein Gleichgewicht herzustellen, womit die schutzwürdigen Interessen der Betroffenen nicht mehr überwiegen und die Verarbeitung auf Art 6 Abs 1 lit f DSGVO bzw. § 26 Abs 1 Satz 1 BDSG gestützt werden kann.[1105]
- Es werden konkrete Speicherfristen für die unterschiedlichen Metadaten und Inhaltsdaten des Digitalen Assistenten definiert und das von einem Nutzer erstellte Profil wird nach Beendigung der Tätigkeit iZh. mit dem Digitalen Assistenten bzw. beim Arbeitgeber sofort (kein denkbares berechtigtes Interesse beim Arbeitgeber) gelöscht.

Big Data

- Klare Definition zu welchen Zwecken Big Data im Beschäftigtenverhältnis eingesetzt wird (z.B. Verbot von „People Analytics" der Beschäftigten durch Big Data Vorhersagen z.B. über den wahrscheinlichen Karrierelauf, die wahrscheinliche Zufriedenheit oder die wahrscheinlichen charakterliche Geeignetheit, bzw. betriebliche Netzwerkanalysen um den Einfluss des Mitarbeiters in einem Umfeld zu beobachten).

1104 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten" (2019) 24; 35 ff.

1105 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 14; *Kroschwald*, Informationelle Selbstbestimmung in der Cloud (2016) 219 ff.

- Zwecktrennung (Nicht-Verkettbarkeit) durch logische Separierung, durch zweckdienliche Daten, durch Anonymisierung / Aggregierung vor der Verkettung;[1106]
- Lückenlose Dokumentation des Big Data Verfahrens (Transparenz);[1107]
- Sicherstellung der Intervenierbarkeit – Betroffenen muss die Ausübung ihrer Betroffenenrechte wirksam möglich ist. Dies gilt auch bei Pseudonymen;[1108]
- Verwertungsregeln, die diskriminierende Suchkriterien und die Verwertung unzulässiger Auswertungen in rechtlichen Verfahren verbieten;[1109]
- Anwendung von effektiven Pseudonymisierungs-, Anonymisierungs und Verschlüsselungstechniken.[1110]

5.7 Vorschlag für Maßnahmen für einen effektiven Beschäftigtendatenschutz durch Betriebsvereinbarungen

Die DSGVO ermöglicht es Kollektiv- und Betriebsvereinbarungen als eigenständige Rechtsgrundlage für Datenverarbeitungen auszugestalten, wenn das nationale Recht dies vorsieht (vgl. § 26 Abs 4 BDSG). Dies versetzt Unternehmen in die Lage, gemeinsam mit dem Betriebsrat, datenschutzrechtliche Fragen im konkreten Einzelfall und auch hinsichtlich spezieller Risiken durch neue Technologien in betrieblichen Spezialregelungen zu lösen und damit den Einsatz neuer Technologien leichter zu ermöglichen und gleichzeitig die damit verbundenen Risiken effektiv in Abstimmung mit dem Betriebsrat einzudämmen. Die Möglichkeit, die die DSGVO iZh. mit dem nationalen kollektiven Arbeitsrecht bietet, soll hier am Beispiel Deutschland und Österreich geprüft werden, sowie welche Inhalte hierzu in einer Betriebsvereinbarung berücksichtigt werden könnten:

5.7.1 Deutschland – Betriebsvereinbarung als Rechtsgrundlage iSd. DSGVO?

§ 26 Abs 4 BDSG bestimmt in Ausführung des ErwGr 155 iVm. Art 88 DSGVO, dass die Verarbeitung personenbezogener Beschäftigtendaten aufgrund von Kollektivvereinbarungen inkl. Betriebsvereinbarungen zulässig sein kann, was die konkrete Ausgestaltung eines auf die betrieblichen Bedürfnisse ausgestalteten Beschäftigtendatenschutz in Deutschland ermöglicht.[1111] Zudem ist ohnehin bei Anwendbarkeit des § 87 Abs 1 Nr 6 BetrVG (Leistungs- und Verhaltenskontrolle objektiv möglich) eine Betriebsvereinbarung abzuschließen.[1112]

1106 *Weichert*, ZD 2013, 251.
1107 *Weichert*, ZD 2013, 251.
1108 *Weichert*, ZD 2013, 251.
1109 *Roßnagel,* ZD 2013, 562; *Europäisches Parlament*, Entschließung vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatssphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)) Erwägungen M und N.
1110 *Europäisches Parlament*, Entschließung vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatssphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)) Erwägung I und Erwägung 11.
1111 BT-Drs 18/11325, 98 f.
1112 *Ricard/Maschmann* in Ricardi (Hrsg), Betriebsverfassungsgesetz[16] (2018) § 87 Rn 488; 508; 511.

Der Begriff der „Kollektivvereinbarung“ iSd. Art 88 DSGVO wird in § 26 Abs 1 Satz 1 BDSG konkretisiert. Darunter fallen Tarifverträge (§ 4 TVG), Betriebsvereinbarungen (§ 77 BetrVG), Dienstvereinbarungen (§ 73 BPersVG) und auch Sozialpläne, die gemäß § 112 Abs 1 Satz 3 BetrVG mit Betriebsvereinbarungen gleichgestellt sind. Gemäß § 26 Abs 4 Satz BDSG müssen die Parteien beim Abschluss von solchen „Kollektivvereinbarungen“ (§ 26 Abs 1 Satz 1 BDSG) die Vorgaben des Art 88 Abs 2 DSGVO beachten.[1113] Das heißt, es müssen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen vorgesehen werden – insbesondere im Hinblick:

- auf die Transparenz der Verarbeitung,
- der Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und
- auf Überwachungssysteme am Arbeitsplatz.

Nur unter diesen Voraussetzungen können sie als eigenständige Rechtsgrundlage herangezogen werden.[1114] Unklar ist, ob durch die DSGVO (Vollharmonisierung) die bisherige Rechtsprechung des BAG seit 1986 obsolet wird, welche Betriebsvereinbarungen auch zuungunsten für Beschäftigte und damit sogar unter das gesetzliche Niveau des alten BDSG für zulässig erachtet.[1115] Das BAG sprach aus*: „Die Verarbeitung von personenbezogenen Daten der Arbeitnehmer ist datenschutzrechtlich schon dann zulässig, wenn sie durch eine Betriebsvereinbarung oder durch einen Spruch der Einigungsstelle erlaubt wird. Betriebsvereinbarung oder Spruch der Einigungsstelle können auch zuungunsten der Arbeitnehmer von den Vorschriften des Bundesdatenschutzgesetzes abweichen. Sie müssen sich im Rahmen der Regelungskompetenz der Betriebspartner halten und den Grundsätzen über den Persönlichkeitsschutz des Arbeitnehmers im Arbeitsverhältnis Rechnung tragen.*[1116] (…) *[Betriebsvereinbarungen und Tarifverträge] sind nicht darauf beschränkt, nur unbestimmte Rechtsbegriffe des Bundesdatenschutzgesetzes unter Berücksichtigung der betrieblichen Besonderheiten näher zu konkretisieren oder den Datenschutz der Arbeitnehmer zu verstärken. Der Datenschutz nach dem Bundesdatenschutzgesetz ist gegenüber den genannten anderen Rechtsvorschriften nicht unabdingbarer Mindeststandard, der durch Tarifverträge oder Betriebsvereinbarungen nur zugunsten der Arbeitnehmer verbessert werden könnte.“*[1117] Die DSGVO erlaubt grundsätzlich seit 25. Mai 2018 keine Abweichungen mehr „nach oben oder unten“.[1118] Für *Forst* trägt dieses Argument jedoch nicht im Rahmen des Art 88 DSGVO. Art 88 DSGVO will seiner Ansicht genau diesen Spielraum „nach oben oder unten“ auf nationaler Ebene beim Beschäftigtendatenschutz schaffen – in den Grenzen der Vorgaben des Art 88 Abs 2 DSGVO und der Grundrechte der EU-GRC.[1119] Insofern würde es § 26 Abs 4 BDSG ermöglichen, die bisherige deutsche Praxis 1:1 fortzusetzen,

1113 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), DSGVO BDSG[6] (2018) § 26 BDSG Rn 88 ff.
1114 *Art 29 Datenschutzgruppe,* WP 249 (2017) 10.
1115 *Thüsing/Granetzny* in Thüsing (Hrsg), Beschäftigtendatenschutz und Compliance[2] (2014) § 4 Rn 5 ff.
1116 BAG, NJW 1987, 674.
1117 BAG, Beschluss v. 27.05.1986, Az. 1 ABR 48/84 (Düsseldorf).
1118 *von Lewinski* in Eßer/Kramer/v. Lewinski (Hrsg), DSGVO BDSG[6] (2018) Art 2 Rn 2.
1119 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), DSGVO BDSG[6] (2018) Art 88 Rn 17 ff.

dass die Betriebsparteien durch Betriebsvereinbarungen im Rahmen der BAG Judikatur[1120] diverse Datenschutz- und IT-Themen für den Betrieb umfassend individualisiert regeln können, womit Betriebsvereinbarungen ein wesentliches Gestaltungsinstrument bei der Regelung des betrieblichen Datenschutzes in Deutschland bleiben. Solange die Anforderungen des Art 88 Abs 2 DSGVO darin berücksichtigt werden, könnte auch das Datenschutzniveau im Unternehmen durch Betriebsvereinbarungen sogar gesenkt werden.[1121]

Meiner Ansicht ist die Auslegung des Art 88 DSGVO durch *Forst* zutreffend, denn das Ziel von Öffnungsklauseln ist es, mehr Flexibilität für EU-Mitgliedstaaten zu schaffen. Folglich gilt die Rechtsprechung des BAG aus dem Jahr 1986 zum BDSG aF auch weiter für neue Betriebsvereinbarungen gemäß § 26 Abs 4 BDSG nF iVm. Art 88 Abs 2 DSGVO.[1122]

5.7.2 Österreich – Betriebsvereinbarung als Rechtsgrundlage iSd. DSGVO?

Art 88 DSGVO sieht vor, dass Kollektivvereinbarungen (ErwGr 155: „*einschließlich Betriebsvereinbarungen*“) spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen können. Kollektivverträge (§ 2 Abs 1 ArbVG) sind in Österreich Vereinbarungen, die zwischen kollektivvertragsfähigen Körperschaften der Arbeitgeber einerseits und der Arbeitnehmer andererseits schriftlich abgeschlossen werden. Damit könnten – im Falle einer nationalen Umsetzung des Art 88 DSGVO („*Mitgliedstaaten können* […] *vorsehen*“) – grundsätzlich auch Fragen des Beschäftigtendatenschutzes direkt über Kollektivverträge (Betriebsvereinbarungen) geregelt werden. Dies ist aber in Österreich nach hA so nicht möglich: Kollektivverträge können in Österreich nämlich nicht beliebige Gegenstände regeln (Nichtigkeit), sondern nur jene Gegenstände in der taxativen Aufzählung des § 2 Abs 2 ArbVG sowie gemäß § 2 Abs 2 Z 7 ArbVG auch jene Gegenstände, deren Regelung durch ein anderes „Gesetz“ dem Kollektivvertrag übertragen worden ist (z.B. AZG, KJBG, etc).[1123] Art 88 Abs 1 DSGVO selbst ist kein „Gesetz“ iSd. § 2 Abs 2 Z 7 ArbVG, weil Art 88 Abs 1 DSGVO lediglich eine Öffnungsklausel für die EU-Mitgliedstaaten ist, eine solche Möglichkeit im nationalem Recht „vorzusehen“. Der österreichische Gesetzgeber hat von dieser Möglichkeit des Art 88 Abs 1 DSGVO nicht Gebrauch gemacht und kein „Gesetz“ iSd. § 2 Abs 2 Z 7 ArbVG geschaffen (vgl. Deutschland: § 26 Abs 1 Satz 1 u. Abs 4 BDSG).[1124] Das an die DSGVO angepasste österreichische DSG[1125] idgF. BGBl. I Nr. 14/2019 enthält keine Bestimmung iSd. § 2 Abs 2 Z 7 ArbVG

1120 BAG, Beschluss v. 27.05.1986, Az. 1 ABR 48/84 (Düsseldorf).

1121 *Forst* in Eßer/Kramer/v. Lewinski (Hrsg), DSGVO BDSG[6] (2018) Art 88 Rn 17 ff; *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017), C. III. Rn 154 ff; BAG, Beschluss v. 27.05.1986, Az. 1 ABR 48/84.

1122 BAG, Beschluss v. 27.05.1986, Az. 1 ABR 48/84 (Düsseldorf); BAG, NJW 1987, 674.

1123 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 2 ArbVG Rn 16 f; *Strasser* in Strasser/Jabornegg/Resch (Hrsg), ArbGV (Stand 1.10.2002, rdb.at) § 2 Rn 14.

1124 *Gerhartl*, Datenschutz im Arbeitsrecht – Betrachtungen im Kontext der neuen Rechtslage, ASok 2018, 223 (227); *Gerhartl*, Datenverarbeitung im Arbeitsverhältnis, ecolex 2018, 496 (498 f); *Grünanger*, Auswirkungen der DSGVO auf den Arbeitnehmer-Datenschutz in Österreich, ZAS 2017/55, 284 (285 f).

1125 Datenschutz-Anpassungsgesetz 2018 BGBl. I Nr. 120/2017; Datenschutz-Deregulierungs-Gesetz 2018 BGBl. I Nr. 24/2018.

und Art 88 DSGVO.[1126] Zu beachten ist, dass § 11 DSG (aF) idF. BGBl. I Nr. 120/2017 für kurze Zeit eine solche Bestimmung enthielt, die das ArbVG, soweit dort die Verarbeitung personenbezogener Daten geregelt wird (u.a. §§ 89, 91, 96, 96a und 97 ArbVG), als Vorschrift im Sinne des Art. 88 DSGVO betrachtete (dies wurde jedoch kurz vor dem 25. Mai 2018 mit BGBl. I Nr. 24/2018 wieder aufgehoben).[1127] Trotz (bzw. „entgegen") des Gesetzesbeschlusses BGBl. I Nr. 24/2018 vom 15. Mai 2018 notifizierte das Bundesministerium für Arbeit, Soziales, Gesundheit und Kosumentenschutz am 27. Juni 2018 gemäß Art 88 Abs 3 DSGVO das österreichische ArbVG, soweit es die Verarbeitung personenbezogener Daten im Beschäftigungskontext betrifft, als spezifische österreichische Rechtsvorschrift iSd. Art 88 DSGVO bei der EU-Kommission in Brüssel.[1128] Durch die Novellierung des § 11 DSG (aF) idF. BGBl. I Nr. 120/2017 kurz vor Anwendbarkeit der DSGVO ab 25. Mai 2018 durch BGBl. I Nr. 24/2018 mit 15. Mai 2018 hatte aber der österreichische Gesetzgeber kurz zuvor eindeutig politisch klar gestellt, dass er das ArbVG nicht als Rechtsvorschrift iSd. Art 88 DSGVO betrachtet, denn es wurde die Bezugnahme auf das ArbVG in § 11 DSG (aF) idF. BGBl. I Nr. 120/2017 als Rechtsvorschrift iSd. Art 88 DSGVO völlig gestrichen. Stattdessen wurde § 11 DSG idF. BGBl. I Nr. 24/2018 neu formuliert und regelt nun eine gänzlich neue Thematik, nämlich die Verwarnpflicht für die Datenschutzbehörde. Folglich stellt sich die Frage, ob die nachfolgende Notifizierung des ArbVG als Rechtsvorschrift iSd. Art 88 DSGVO bei der EU-Kommission – „entgegen" dem Gesetzesbeschluss BGBl. I Nr. 24/2018 vom 15. Mai 2018 – durch das Bundesministerium für Arbeit, Soziales, Gesundheit und Kosumentenschutz mit 27. Juni 2018 an der rechtlichen Qualität des ArbVG iZh. mit Art 88 DSGVO etwas ändert? Meiner Ansicht gilt für die nationale Rechtsanwendung weiter alleine der in BGBl. I Nr. 24/2018 vom 15. Mai 2018 kundgemachte unzweifelhafte Wille des (damaligen) österreichischen Gesetzgebers, dass das ArbVG mit 25. Mai 2018 keine Rechtsvorschrift iSd. Art 88 DSGVO werden sollte. Die Notifizierung des ArbVG durch das Bundesministerium für Arbeit, Soziales, Gesundheit und Kosumentenschutz bei der EU-Kommission mit 27. Juni 2018 kann daran mA insofern nichts ändern. Folglich ist das ArbVG aktuell als keine Rechtsvorschrift iSd. Art 88 DSGVO zu betrachten (vgl. BGBl. I Nr. 24/2018). Datenschutzrecht und Betriebsverfassungsrecht stehen in Österreich schlicht nebeneinander.[1129] Eine andere Meinung vertritt *Goricnik*, der direkt in § 2 Abs 2 Z 2 ArbVG eine Möglichkeit zum Abschluss von „Beschäftigtendatenschutz-Kollektivverträgen" iSd. Art 88 Abs 1 DSGVO sieht.[1130] Allerdings ist diese Ansicht *Goricniks*

1126 *Körber-Risak*, DSGVO und Betriebsverfassungsrecht, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 56.

1127 ErläutAB 1761 BlgNr 25. GP 7 f (zu § 11 DSG idF. BGBl. I Nr. 120/2017); AA-10 26. GP 2; 4 (zu § 11 DSG idF. BGBl. I Nr. 24/2018); vgl. auch OGH 23.05.2019, 6 Ob A1/18t.

1128 *Bundesministerium für Arbeit, Soziales, Gesundheit und Kosumentenschutz*, Mitteilung v. 27.06.2018 von Rechtsvorschriften der Republik Österreich zu Art. 88 Abs. 3 Datenschutz-Grundverordnung, GZ: BMASGK-462.501/0012-VII/B/8/2018, abrufbar unter: https://ec.europa.eu/info/sites/info/files/at_notification_art_88.3_complement_publish.pdf (zuletzt abgerufen am 04.07.2019).

1129 *Brodil*, Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 11; *Brodil*, ecolex 2018, 486 (489); *Körber-Risak,* DSGVO und Betriebsverfassungsrecht, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 60.

1130 *Goricnik*, Kollektivvereinbarungen als Erlaubnistatbestände für Datenverarbeitungen im Beschäftigungskontext, DRdA 2018, 10 (13 f.).

mit Hinweis auf die Kommentarliteratur und Judikatur zu bezweifeln, da Kollektivverträge gestützt auf § 2 Abs 2 Z 2 ArbVG nur jene Inhalte erfassen, die nach der Verkehrsauffassung der am jeweiligen Kollektivvertrag beteiligten Kreise typischerweise im Arbeitsvertrag enthalten sind (iSv. typische und regelmäßig wiederkehrende Inhalte von Arbeitsverträgen). Datenschutz wird im Regelfall kein in Arbeitsverträgen verhandelbares Thema sein. *Reissner* weist ausdrücklich daraufhin, dass Regelungen über die Privatsphäre kein typischer Inhalt eines Arbeitsvertrages sind.[1131]

Vergleichbares gilt hinsichtlich Betriebsvereinbarungen. Auch Betriebsvereinbarungen können in Österreich genauso wie Kollektivverträge nicht über beliebige Gegenstände abgeschlossen werden, sondern nur über jene Gegenstände, deren Regelung durch Gesetz oder durch Kollektivvertrag der Betriebsvereinbarung vorbehalten worden ist (§ 29 ArbVG). Solche gesetzlichen Delegationsnormen finden sich bspw. im ArbVG, AZG, ARG, EFZG, etc.[1132] Eine gesetzliche Regelung, die Fragen des Beschäftigtendatenschutzes iSd. Art 88 Abs 1 DSGVO einer Betriebsvereinbarung vorbehalten würde, existiert nach hA nicht und wurde vom österreichischen Gesetzgeber bisher auch nicht geschaffen.[1133] *Körber-Risak* führt aus: *„Betriebsvereinbarungen können daher weiterhin nur auf Basis der einschlägigen Tatbestände des ArbVG geschlossen werden. Hätte der Gesetzgeber eine direkte Kompetenz der Betriebsvereinbarungen intendiert, hatte er zB einen neuen Betriebsvereinbarungstatbetand »Datenschutzbetriebsvereinbarung iSd Art 88 DSGVO« schaffen können.“*[1134] Eine andere Meinung vertritt ebenfalls *Goricnik*, der in den § 96a ArbVG bzw. § 97 Abs 1 Z 6 ArbGV für Betriebsräte trotzdem Möglichkeiten zur Anwendung des Art 88 Abs 1 DSGVO sieht: Entweder der Betriebsrat schließe wie bisher eine „schlichte Datenschutz-BV“ ab, auf deren Basis der Arbeitgeber unter Berücksichtigung der allgemeinen Anforderungen der DSGVO die Beschäftigtenverarbeitung durchführt (Zwei-Ebenen Prüfung – DSGVO u. betriebliche Mitbestimmung[1135]). Andererseits könne der Betriebsrat aber nun im Rahmen des § 96a ArbVG auch eine komplette „europarechtlich qualifizierte BV“ mit dem Arbeitgeber verhandeln bzw. im Rahmen des § 97 Abs 1 Z 6 ArbVG zumindest einzelne „europarechtlich qualifizierte“ BV-Bestimmungen in eine BV hineinverhandeln, die dann eigene Erlaubnistatbestände iSd. Art 88 Abs 1 DSGVO wären.[1136] Diese Ansicht *Goricniks* ist mA ebenso zu bezweifeln: Wie *Brodil* zeigt, wird – mit dem Blick auf die Gesetzgebungshistorie zu § 11 DSG idF. BGBl. I Nr. 24/2018[1137] – die Öffnungsklausel des

1131 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 2 ArbVG Rn 48; *Strasser* in Strasser/Jabornegg/Resch (Hrsg), ArbGV (Stand 1.10.2002, rdb.at) § 2 Rn 30.

1132 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 29 ArbVG Rn 4; 13 ff; *Strasser* in Strasser/Jabornegg/Resch (Hrsg), ArbGV (Stand 1.10.2002, rdb.at) § 29 Rn 10 ff.

1133 *Gerhartl*, ASok 2018, 223 (227); *Gerhartl*, ecolex 2018, 496 (498 f); *Grünanger*, ZAS 2017/55, 284 (285 f).

1134 *Körber-Risak,* DSGVO und Betriebsverfassungsrecht, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 59 f.

1135 *Körber-Risak*, DSGVO und Betriebsverfassungsrecht, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 63 f.

1136 *Goricnik*, DRdA 2018, 10 (12 ff.); *Goricnik,* Adaption und Neu-Abschluss von Betriebsvereinbarungen zum Datenschutz im Lichte der DS-GVO, in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 152 ff.

1137 BGBl. I Nr. 120/2017; ErläutRV 1664 BlgNR 25. GP 13 (zu § 29); ErläutAB 1761 BlgNr 25. GP 7 f (zu § 11); BGBl. I Nr. 24/2018; IA 189/A 26. GP 2; 7 f (zu § 11); AA-10 26. GP 2; 4 (zu § 11).

Art 88 DSGVO von Österreich mangels bisheriger (bzw. wieder aufgehobener) gesetzgeberischer Aktivitäten überhaupt gar nicht wahrgenommen. Österreich verzichtet aktuell völlig auf spezifische datenschutzrechtliche Vorschriften im arbeitsrechtlichen Bereich iSd. Art 88 DSGVO.[1138] Damit sind auch die §§ 96, 96a ArbVG – trotz Notfizierung durch das Bundesministerium für Arbeit, Soziales, Gesundheit und Kosumentenschutz bei der EU-Kommission[1139] – keine datenschutzrechtlichen Normen iSd. Art 88 DSGVO, sondern es besteht in Österreich ein schlichtes Nebeneinander von Datenschutzrecht und Arbeitsrecht, insbesondere beim Betriebsverfassungsrecht.[1140]

Im Ergebnis ist mA daher der Meinung *Brodils* und *Körber-Risaks* bzgl. der Nichtumsetzung des Art 88 DSGVO in Östereich zu folgen, womit sich aktuell aus dem österreichischen ArbVG keine Möglichkeiten ergeben, Art 88 DSGVO im Beschäftigtenverhältnis fruchtbar zu machen: Dies zeigt bzgl. Kollektivverträge die Auslegung des § 2 Abs 2 Z 2 ArbVG (Regelungen über die Privatsphäre sind kein typischer Inhalt eines Arbeitsvertrages[1141]) und bzgl. Betriebsvereinbarungen gemäß §§ 29, 96, 96a ArbVG die historische Entwicklung des finalen § 11 DSG idF. BGBl. I Nr. 24/2018[1142].[1143]

Deutschland notifizierte gemäß BT-Drs. 19/5155, S. 96 ff im Zusammenhang mit dem Beschäftigtendatenschutz nicht-öffentlicher Stellen nur § 26 BDSG als Rechtsvorschrift iSd. Art 88 Abs 3 DSGVO, nicht notifiziert wurden die im Zusammenhang mit dem Datenschutz relevanten Bestimmungen des BetrVG (z.B. § 87 BetrVG), mit vergleichbaren Regelungsinhalt wie die österreichischen §§ 96, 96a ArbVG.[1144]

5.7.3 Vorschlag für Inhalte einer Betriebsvereinbarung iZh Digitalen Assistenten

Folgende inhaltliche Themen und Maßnahmen können bzw. sollten im Rahmen einer Betriebsvereinbarung zum Datenschutz iZh. mit Enterprise Search und Digitalen Assistenten – zumindest in Deutschland gemäß § 26 Abs 4 BDSG bzw. § 87 Abs 1 Nr 6 BetrVG /

1138 *Brodil,* Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 11; *Brodil*, ecolex 2018, 486 (489).

1139 *Bundesministerium für Arbeit, Soziales, Gesundheit und Kosumentenschutz*, Mitteilung v. 27.06.2018 von Rechtsvorschriften der Republik Österreich zu Art. 88 Abs. 3 Datenschutz-Grundverordnung, GZ: BMASGK-462.501/0012-VII/B/8/2018, abrufbar unter: https://ec.europa.eu/info/sites/info/files/at_notification_art_88.3_complement_publish.pdf (zuletzt abgerufen am 04.07.2019).

1140 *Körber-Risak*, DSGVO und Betriebsverfassungsrecht, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 60.

1141 *Reissner* in Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at) § 2 ArbVG Rn 48.

1142 BGBl. I Nr. 120/2017; ErläutRV 1664 BlgNR 25. GP 13 (zu § 29); ErläutAB 1761 BlgNr 25. GP 7 f (zu § 11); BGBl. I Nr. 24/2018; IA 189/A 26. GP 2; 7 f (zu § 11); AA-10 26. GP 2; 4 (zu § 11).

1143 *Brodil*, Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 11; *Brodil*, ecolex 2018, 486 (489); *Körber-Risak,* DSGVO und Betriebsverfassungsrecht, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 60.

1144 BT-Drs. 19/5155, 96 ff; sowie auf der Homepage der EU-Kommission abrufbar unter: https://ec.europa.eu/info/sites/info/files/de_notification_articles_49.5_51.4_83.9_84.2_85.3_88.3_90.2_publish.pdf (zuletzt abgerufen am 04.07.2019).

eingeschränkt in Österreich gemäß § 96 Abs 1 Z 3; § 96a Abs 1 Z 1, § 97 Abs 1 Z 6 ArbVG – berücksichtigt werden:

- Örtlicher, sachlicher und persönlicher Anwendungsbereich der Betriebsvereinbarung;[1145]
- Definition welches IT-System konkret eingeführt werden soll. Nach *Feiler/Horn* sollte man jedoch nicht auf ein bestimmtes IT-System abstellen, sondern auf die dazu verarbeiteten Datenkategorien und Verarbeitungszwecke (z.B. Betriebsvereinbarung „Digitaler Assistent", der eine Reihe von verschiedenen IT-Systemen und Applikationen umfassen kann);[1146]
- Beschreibung der für die private Nutzung zugelassenen Kommunikationsmittel und welche ausschließlich mit dienstlichen Inhalten verwendet werden dürfen:[1147]
  - *E-Mail:* Privatnutzung erlaubt; keine Indexierung in der Enterprise Search Suche;
  - *Enterprise Social Network:* ausschließlich betriebliche Nutzung; Verbot der Privatnutzung, weil die dort „geposteten" Inhalte und Themen durch die Enterprise Search im Suchindex indiziert werden und damit – je Zugriffsrechte und Rolle – für einen größeren Benutzerkreis auffindbar sein sollen;
  - *Enterprise Wiki:* ausschließlich betriebliche Nutzung; Verbot der Privatnutzung um für Enterprise Search nutzen zu können;
  - *Betriebliche Blogs:* ausschließlich betriebliche Nutzung, Verbot der Privatnutzung um für Enterprise Search nutzen zu können;
  - *diverse Collaboration Tools:* ausschließlich betriebliche Nutzung erlaubt; Verbot der Privatnutzung um für Enterprise Search nutzen zu können;
  - *sonstige Laufwerke und Datenquellsysteme des Unternehmens*: ausschließlich betriebliche Nutzung erlaubt; Verpflichtung zur korrekten Datenablage gemäß Datenklassifizierung um für Enterprise Search nutzen zu können; Verbot der Privatnutzung in Form von Speicherung privater Daten auf Laufwerke und Quellsysteme.
- Liste der Datenkategorien inkl. der protokollierten Verbindungsdaten;
- Liste der Verarbeitungzwecke;
- Liste der konkreten Datenempfänger;
- Liste der Zugriffsberechtigten, also den Kreis der in gespeicherte Daten einsichtsberechtigten Personen.[1148]
- Beschreibung welche Risiken durch die Datenverarbeitung Digitaler Assistent in der Cloud bestehen und welche Maßnahmen konkret erforderlich und umzusetzen sind, um die identifizierten Risiken und Anforderungen auf ein akzeptables Maß zu reduzieren (vgl. im Detail **Kapitel 5.6** und **Kapitel 6**):[1149]

1145 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017) C.III Rn 183 ff; *Fritsch/Haslinger* in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 158 ff;

1146 *Fritsch/Haslinger*, Checkliste Betriebsvereinbarung – das Prüfschema, in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 158 ff; *Feiler/Horn*, Umsetzung der DSGVO in der Praxis (2018) 127.

1147 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017) C.III Rn 183 ff.

1148 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017) C.III Rn 189; *Feiler/Horn*, Umsetzung der DSGVO in der Praxis (2018) 127 ff.

1149 *Fritsch/Haslinger* in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 158 ff.

  - starke Verschlüsselungsmaßnahmen sowohl in der Cloud (Schlüssel beim Cloud Anwender und nicht beim Cloud Anbieter) als auch am Transportweg und ausdrückliche Verpflichtung des Arbeitgebers zur IT-Security am Stand der Technik zur Sicherstellung des Datenschutzes und der Vertraulichkeit der Beschäftigtendaten und -kommunikation sowie auch gleichzeitig der Betriebs- und Geschäftsgeheimnisse vor (DSGVO-widrigen) externen Zugriffen (vgl. **Kapitel 6)**;
  - grundsätzliche Pseudonymisierung der Daten bzw. sogar Anonymisierung soweit möglich;
  - Nicht-Verkettbarkeit durch getrennte Datenspeicherung insbesondere der zweckgebundenen Daten zur Datensicherheit (Art 32 DSGVO);
  - Profiling iZh mit dem Digitalen Assistenten ausschließlich nur hinsichtlich bestimmter Teilaspekte des beruflichen Wirkens des Betroffenen soweit tatsächlich konkret für die Funktionsfähigkeit des Digitalen Assistenten erforderlich;
  - Cloud Computing von Beschäftigtendaten aufgrund der Risiken von Drittstaatszugriffen (vgl. **Kapitel 6)** und kommerziellen Datenmissbrauchsrisiken (z.B. Big Data Analysen zu fremden Zwecken des Cloud Anbieters) grundsätzlich im europäischen Rechtsrahmen EU-GRC und EMRK; ggf. Ausnahmen von diesem strengen Grundsatz bei personenbezogenen Daten, die gemäß interner Datenklassifizierung als grundsätzlich wenig risikobehaftet einzustufen sind.

- Benennung klarer Speicher- und Löschfristen inkl. Löschpflichten je benannter Datenkategorie.[1150]
- Beschreibung der Kontrollmöglichkeiten durch den Arbeitgeber, insbesondere wann in ausschließlich betriebliche Kommunikation (Enterprise Social Networks, Wikis, Bloqs, Laufwerke, etc.) sowie auch in E-Mail Accounts mit erlaubter privater Nutzung eingesehen werden darf (z.B. beim auch privat genutzten eMail Account nur bei dokumentiertem strafrechtlicher Verdacht bzw. schwerem Pflichtverstoß im Arbeitsverhältnis) gemäß § 26 Abs 1 BDSG bzw. Art 6 Abs 1 lit f DSGVO.[1151]
- Ausdrückliches Verbot der Einsichtnahme durch den Arbeitgeber oder sonstige Dritte in das sensible Nutzerprofil des Digitalen Assistenten über Teilaspekte des beruflichen Wirkens des Beschäftigten mangels irgendeines denkmöglichen berechtigten Interesses bzw. Erforderlichkeit daran, abseits der technisch erforderlichen Verarbeitung zum Betrieb des Digitalen Assistenten. Sofortige Löschung des Profils, wenn keine Erforderlichkeit für diese Verarbeitung zum Zweck Digitaler Assistent mehr besteht (Beschäftigter nutzt den Digitalen Assistenten nicht mehr, da er/sie aus dem Unternehmen ausgeschieden ist, etc.).[1152]
- Klares gerichtliches, außergerichtliches und behördliches Beweisverwertungsverbot im Falle unzulässiger Beweismittelbeschaffung durch den Arbeitgeber (z.B. rechtswidrige Einsicht in das Nutzungsprofil des Digitalen Assistenten über den Beschäftigten durch den Arbeitgeber). Es müssen hier beide denkbaren Fälle unzulässiger Datenverarbeitung geregelt werden:

1150 *Fritsch/Haslinger* in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 158 ff.

1151 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017) C.III Rn 183 ff;

1152 *Steidle*, Multimedia-Assistenten im Betrieb (2005) 299 ff.

- Beweismittelverbot eines von Anbeginn unzulässigen Verarbeitungsvorgangs durch den Arbeitgeber (z.B. rechtswidrige heimliche Mitarbeiterüberwachung, z.B. entgegen DSGVO bzw. ohne BV gemäß § 87 Abs 1 Nr 6 dBetrVG bzw. § 96 Abs 1 Z 3; § 96a Abs 1 Z 1 öArbVG); Dazu empfiehlt *Goricnik* folgende Klausel: *„Eine Verarbeitung von personenbezogenen Daten, die unter Zuhilfenahme des gegenständlichen Systems, aber entgegen den einschlägigen Bestimmungen dieser Betriebsvereinbarung verarbeitet wurden, ist untersagt und damit rechtswidrig und es wird zur diesbezüglichen Bewehrung aus Gründen rechtlicher Vorsicht beschäftigtendatenschutzrechtlich ein entsprechendes außergerichtliches, gerichtliches und behördliches Beweismittel- und verwertungsverbot, das sich an Jedermann (dh. insb. Arbeitgeber, Behörden und Gerichte) richtet, vereinbart, soferne von einem solchen Beweismittel- und -verwertungsverbot nicht sowieso schon eo ipso (europa-)rechtlich auszugehen ist.“*[1153]
- Beweismittelverbot einer grundsätzlich zulässigen Datenverarbeitung, die später einem unzulässigem Zweck zugeführt wird (z.B. Weiterverarbeitung von personenbezogenen Daten zur Gewährleistung der Datensicherheit gemäß Art 32 DSGVO werden trotz getroffener Maßnahmen der Nicht-Verkettbarkeit und trotz damit verbundener getrennter Datenspeicherung durch den Arbeitgeber der nachträglichen Leistungs- und Verhaltenskontrolle zugeführt; rechtwidrige Auswertung des Nutzerprofils des Digitalen Assistenten für Big Data „People Analytics; etc.). Dazu empfiehlt *Goricnik* folgende Klausel: *„Eine Verarbeitung von personenbezogenen Daten, die unter Zuhilfenahme des gegenständlichen Systems und gemäß der gegenständlichen Betriebsvereinbarung erlaubter Weise verarbeitet wurden, zur Leistungs- und Verhaltenskontrolle oder zur wie auch immer gearteten Beurteilung von Arbeitnehmerinnen und Arbeitnehmern ist untersagt und damit rechtswidrig und es wird zur diesbezüglichen Bewehrung aus Gründen rechtlicher Vorsicht beschäftigtendatenschutzrechtlich ein entsprechendes außergerichtliches, gerichtliches und behördliches Beweismittel- und verwertungsverbot, das sich an Jedermann (dh. insb. Arbeitgeber, Behörden und Gerichte) richtet, vereinbart, soferne von einem solchen Beweismittel- und –verwertungsverbot nicht sowieso schon eo ipso (europa-)rechtlich auszugehen ist.“*[1154]

- Vereinbarung konkreter Kontroll- und Mitwirkungsrechte durch den Betriebsrat iZh. mit dem neuen System.[1155]
- Unterrichtungspflichten und –modalitäten gegenüber dem Betriebsrat und der Belegschaft.[1156]
- Es bietet sich auch die Möglichkeit in die Betriebsvereinbarung auch den Inhalt der Datenschutzmitteilung (Art 12 ff DSGVO) aufzunehmen, da mit dem Abschluss und Aushang der Betriebsvereinbarung im Betrieb (vgl. § 77 Abs. 2 Satz 3 dBetrVG bzw. § 30 Abs 1 öArbVG) keine seperate Datenschutzinformation mehr erforderlich wäre.

1153 *Goricnik*, Bringt die DS-GVO neue Möglichkeiten hinsichtlich Beweismittel- und -verwertungsverboten im Beschäftigungsverhältnis? DRdA-infas 2018, 125 (127 f).

1154 *Goricnik*, DRdA-infas 2018, 125 (128.).

1155 *Fritsch/Haslinger* in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 158 ff.

1156 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017) C.III Rn 189.

Der Nachteil wäre aber, dass bei Änderungen der Verarbeitungstätigkeit (Zwecke, Datenkategorien, Empfänger, etc.) die Betriebsvereinbarung angepasst werden müsste.[1157]

- Vereinbarung einer regelmäßigen Evaluierung des Betriebes eines Digitalen Assistenten.[1158]
- Kündigungsfristen; Nachwirken der Betriebsvereinbarung (Beweismittelverbot).[1159]

1157 *Feiler/Horn*, Umsetzung der DSGVO in der Praxis (2018) 127 ff.

1158 *Fritsch/Haslinger* in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 158 ff.

1159 *Raif* in Kramer (Hrsg), IT-Arbeitsrecht (2017) C.III Rn 189.

6 Exkurs – Datenschutzrisiken durch Auslandsaufklärung

6.1 Technische Grundlagen Computer und Computer-Netzwerke

Das Internet ist ein weltweites Netzwerk aus Rechnern und Übertragungswegen der unterschiedlichen Hersteller. Der Vorläufer des heutigen Internets hieß „ARPAnet" und entstand im Jahr 1969, als die US Regierung ein Netzwerk in Auftrag gab, welches darauf ausgerichtet sein sollte, einen atomaren Krieg zu überleben.[1160] Aus Gründen der Ausfallsicherheit sollte ein dezentraler Verbund von Computern eine Datenübertragung auch dann ermöglichen, wenn einzelne Hauptrechner (EDV-Kommandozentralen) des US Militärs durch einen direkten sowjetischen Angriff ausgefallen wären. Durch eine dezentrale Vernetzung konnte sichergestellt werden, dass trotz einer möglichen Vernichtung von US Kommandozentralen im Rahmen eines sowjetischen Überraschungsangriffs, die Kommandodaten für Vergeltungsschläge an die US-Raketensilos jedenfalls übermittelt worden wären. Zu Beginn bestand das „ARPAnet" aus vier Rechner, im Jahr 1971 waren bereits dreizehn Rechner ein Teil des Netzwerks und im April 1972 waren dreiundzwanzig Rechner an das Netz angeschlossen. Später schlossen sich amerikanische Universitäten und Forschungseinrichtungen der Industrie dem Netzverbund an, um Hard- und Softwareressourcen gemeinsam nutzen zu können. Denn die Computer von Militär, Waffenindustrie und Universitäten mit verteidigungsrelevanter Forschung sollten selbst noch miteinander kommunizieren können, auch wenn Teile des Netzwerks kriegsbedingt nicht mehr funktionieren sollten. Parallel zum militärischen APRAnet entstanden auch unabhängige zivile Netzwerke wie das „Usenet", die nicht miteinander kompatible Protokolle verwendeten. Dieses Problem der Verbindung von unterschiedlichen existierenden Netzwerken miteinander wurde letztlich in den Jahren 1974 bzw. 1978 von Vint Cerf, Bob Kahn und Jon Postel mit dem Verbindungsprotokoll TCP (Transmission Control Protocol) und mit dem Übertragungsprotokoll IP (Internet Protocol) gelöst. Bei den TCP/IP Protokollen handelt es sich um die noch heute dem Internet zugrundeliegenden Datenprotokolle. Der Zugang zum ARPAnet" war bis Anfang der 1990er Jahre allein auf die militärische Nutzung, Forschung und Lehre beschränkt, die kommerzielle Nutzung war entsprechend verboten. Im Jahr 1992 rückte das Internet jedoch ins politische Rampenlicht der Wahlkampfkampagne zur „National Information Infrastructure" bzw. zu „information superhighways" von US Präsidentschaftskandidaten Bill Clinton. Letztlich wurde es auch für kommerzielle Zwecke freigegeben.[1161] Das Internet basiert auf der Idee eines Meta-Netzwerkes, es handelt sich also um ein Netzwerk von Netzwerken, welches einen weltumspannenden Zusammenschluss von Computern ermöglicht und vorhandene Netzwerktechniken verwendet, um Rechnernetze miteinander zu verbinden. Das Internet besteht aus einer speziellen Netzarchitektur mit all-

1160 *Gridl,* Datenschutz in globalen Telekommunikationssystemen (1999) 62.

1161 z.B. der vom damaligen US Senator Al Gore eingebrachte *High Performance Computing Act of 1991*, abrufbar unter: https://www.congress.gov/bill/102nd-congress/senate-bill/00272 (zuletzt abgerufen am 04.07.2019).

C. Jaksch, *Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes*,
AutoUni – Schriftenreihe 143, https://doi.org/10.1007/978-3-658-29450-2_6

gemein anerkannten Netzprotokollen (TCP/IP), deren weltweite Anerkennung und Verwendung die Verbindung unterschiedlicher Rechner und Datennetze ermöglicht. Voraussetzung ist also, dass schon nutzbare Anschlüsse vorhanden sind, um lokale Netze einzugliedern. Mit dem Vorhandensein der Hardware bedarf es lediglich der Software, um der vorhandenen Hardware die Sprache des Internets (das Internetwork Protocol IP) zu vermitteln. Ein Nutzer merkt nicht, dass seine Netzwerkverbindung über diverse unterschiedliche Netzwerke mit verschiedenen Eigenschaften geleitet wird und was letztlich an großem Aufwand betrieben wird, um die Unterschiede zwischen diesen Netzen für Software und Anwender zu verwischen. Jedes der an das Internet angebundenen Netzwerke hat seine ganz besondere Eigenheit bspw. besondere Formen der Adressierung, unterschiedliche Größen der maximalen Datenpakete oder eine andere Art den Weg eines Datenpakets durch das Netz festzulegen. Durch das Internetwork Protocol (IP) werden diese Schwierigkeiten für den Nutzer gelöst. Der Senderechner setzt seine Daten in einzelnen Paketen in das Netz ab und die Daten suchen sich ihren Weg über das Netz zum Ziel, denn die Datenpakete sind mit einem Steuerungsteil verbunden, der u.a. auch die Sender- und Zieladresse enthält. Dadurch können die mit der Zieladresse versehenen Datenpakete individuell über die Weiterleitungseinheiten (Router) auf ihren Weg zum Zielrechner weitergereicht werden. Am Zielrechner angekommen, werden sie wieder in die richtige Reihenfolge zusammengesetzt, denn das TCP/IP Protokoll prüft nach, ob alle Datenpakete tatsächlich angekommen sind und fordert ggf. eine Neuübertragung an. Durch entsprechende organisatorische Maßnahmen muss auch die Eindeutigkeit und Einmaligkeit einer Zieladresse sichergestellt werden.[1162]

1162 *Köhntopp* in Rost (Hrsg), Die Netz-Revolution: Auf den Weg in die Weltgesellschaft (1996) 21 ff; *Sieber* in Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019) Teil 1 Technische Grundlagen Rn 1 ff; Rn 42; *Sonntag,* Informationstechnologie: Grundlagen, in Jahnel/Mader/Staudegger (Hrsg) IT-Recht[3] (2012) 29 f; *Mazzucato*, Das Kapital des Staates – Eine andere Geschichte von Innovation und Wachstum (2014) 134 f; *Grimm* in Roßnagel/Banzhaf/Grimm (Hrsg), Datenschutz im Electronic Commerce (2003) 24 ff; *Schaar*, Datenschutz im Internet (2002) Rn 10; *Art 29 Datenschutzgruppe*, WP 37 (2000) 4; *Jaburek/Blaha*, Die technische Umsetzung der eMail in IT-LAW.AT (Hrsg), e-Mail – elektronische Post im Recht (2003) 1 ff.

6.2 Drittstaatliche Abhörprogramme als große Datenschutz- und Vertraulichkeitsrisiken für auf Cloud Computing gestützte Verarbeitungen

„Jeder belauscht jeden. Der ganze Unterschied ist das unterschiedliche Budget der einzelnen Länder."[1163]

6.2.1 Überblick

Globale staatliche Telekommunikationsüberwachungsprogramme verschiedener Staaten schaffen große Risiken für den Datenschutz und die Gewährleistung der Vertraulichkeit elektronischer Kommunikation. Die Darstellung der Datenschutzrisiken beschränkt sich auf die folgenden Staaten, da diese Staaten nach seriösen Quellen über äußerst große Überwachungsprogramme verfügen:

- UKUSA-Vertragsstaaten
- Russland
- Frankreich
- Deutschland
- China

6.2.2 UKUSA-Vertragsstaaten

Ein weltweit sehr umfangreiches Kommunikationsüberwachungsprogramm wird nach zwei Analysen des *Europäischen Parlaments* (2001, 2014) seit Mitte des 20. Jhdt von den fünf angelsächsischen Ländern USA, Großbritannien, Kanada, Australien und Neuseeland gemäß UKUSA-Abkommen 1948 („Five Eyes") betrieben. Zusätzlich beteiligt sind daran – nach unterschiedlicher bündnistreuer Verbundenheit zu den „Five Eyes" – die diversen westlichen (NATO-) Staaten:

- **„5-Eyes"** (= UKUSA-Vertragsstaaten: USA, UK, Kanada, Neuseeland, Australien);
- **„9-Eyes"** (=UKUSA-Staaten + Dänemark, Frankreich, Norwegen und Niederlande);
- **„14-Eyes"** (= sämtliche „9-Eyes"-Staaten + Bundesrepublik Deutschland, Belgien, Italien, Spanien und auch Schweden als Nicht-NATO-Mitglied).[1164]

1163 *Eric Denécé*, Forschungsdirektor am Zentrum für Geheimdienstforschung, zitiert in: *Weber-Lamberdière* in focus.de (07.07.2013), Die langen Ohren Frankreichs: Wie uns die Grande Nation groß ausspioniert, abrufbar unter: https://www.focus.de/politik/ausland/tid-32242/spezialgebiet-wirtschaftsspionage-die-langen-ohren-frankreichs-wie-uns-die-grande-nation-gross-ausspioniert_aid_1036856.html (zuletzt abgerufen am 20.06.2019).

1164 *Europäisches Parlament,* Entschließung vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres (2013/2188(INI)) Empfehlung 21; *Europäisches Parlament*, Bericht vom 14. Februar 2014 über das Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres (2013/2188(INI)) Empfehlung 22; *Europäisches Parlament,* Entschließung vom 05. September 2001 zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem

(Verfassungsrechtliche) Rechtsgrundlagen US Intelligence Community

Grundsätzlich erfolgt in den USA – nach aktuellem Kenntnisstand der Fachliteratur – eine Überwachung des über die USA laufenden Telekommunikationsverkehrs („Auslandsaufklärung im Inland"). Zudem ist das von den UKUSA-Staaten („Five-Eyes") gemeinsam betriebene nachrichtendienstliche Abhörsystem mit weltweiten Abhörstationen auf den Territorien der „Five Eyes"-Staaten nach einer Analyse des *Europäischen Parlaments* in der Lage sämtliche (bereits Stand Juni 2001[1165]) über geostationäre Fernmeldesatelliten geleitete Kommunikation (Telefonate, E-Mails, Faxe, etc.) abzufangen und abzuhören (z.B. Programm ECHELON) sowie in einem beschränkteren Umfang auch die außerhalb der USA stattfindende kabel- und funkgebundene Kommunikation mitzuschneiden (z.B. Programme UPSTREAM und BLARNEY).[1166] Diese Überwachung stützt sich dabei nach *Wischmeyer* auf zwei unterschiedliche Rechtsgrundlagen, nämlich auf die gesetzliche Grundlage des Foreign Intelligence Surveillance Act (FISA) für Abhörmaßnahmen von Kommunikation gemäß der Legaldefinition der „electronic surveillance" (*„the acquisition* (…) *of the contents of any wire communication* ***to*** *or* ***from*** *a person in the United Sates* (…) *if such acquisition occurs in the United States"*[1167]) und auf die Grundlage der nicht-gesetzlichen presidentiellen Executive Order 12333 bzgl. der reinen *„*foreign to foreign communication*"*. Aufgrund der eingeschränkten Legaldefinition der „electronic surveillance" in FISA („*communication to or from a person in the United Sates"*) regelt nach *Wischmeyer* FISA Überwachungsmaßnahmen, die auch direkt auf US Staatsgebiet stattfinden, selbst nur teilweise. Denn soweit sich der US Kongress zu einem Thema noch nicht (gesetzlich) geäußert hat, kann nach hM in den USA der US Präsident handeln (Art 2 US Verfassung). Da die *„*foreign to foreign communication*"* (auch auf US Territorium) in der gesetzlichen Legaldefinition der „electronic surveillance" gemäß 50 U.S. Code § 1801 FISA nicht enthalten ist, finden sich die Regelungen zur Überwachung der *„*foreign to foreign communication*"* in der tlw. geheimen presidentiellen Executive Order 12333, begründet mit einer sogenannten „Transit Authority" des US Präsidenten. Die Menge der auf Basis dieser „Transit Authority" des US Präsidenten (ohne Richtervorbehalt) von den USA abgefangenen „foreign-to-foreign"-Kommunikationsdaten, übersteige nach *Wischmeyer* dabei die Menge der auf

---

Echelon) (2001/2098(INI)) Erwägung A; *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 62 ff.

1165 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 36.

1166 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 33 ff; *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 17; *Snowden*, Permanent Record[2] (2019), 284 f; *Greenwald*, Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen (2014) 137 ff; 151 ff; *Wischmeyer,* Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen der nachrichtendienstlichen Tätigkeiten in den USA (2017) 51 ff.

1167 50 U.S. Code § 1801 (Definitions); *Wischmeyer*, Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeit in den USA (2017) 57 ff (58).

Basis des gesetzlichen FISA-Rahmens abgefangenen Daten um ein Vielfaches.[1168] *Bowden* schreibt zusammenfassend: „*In einer Reihe aufschlussreicher Interviews betonte der ehemalige NSA-Direktor, General Hayden, dass* (…) *die USA hinsichtlich des ungehinderten Zugriffs auf den ausländischen Kommunikationsverkehr, der über das US-Hoheitsgebiet geleitet wird, oder Auslandsdaten, die dort gespeichert werden, einen »Heimvorteil« hätten.*“[1169] Für die auf den gesetzlichen FISA-Rahmen (z.B. 50 U.S. Code § 1801) gestützte Überwachung der elektronische Kommunikation („*communication **to** or **from** a person in the United Sates“*) gilt ein Richervorbehalt zum Schutz von US Staatsbürgern (4th Amendment US Verfassung). Zu beachten ist dabei, dass der FISC (Foreign Intelligence Surveillance Court) als zuständiges Gericht z.B. bei Überwachungen im Rahmen von FISA 50 U.S. Code § 1881a. („Procedures for targeting certain persons outside the United States other than United States persons“) nicht über die Überwachung konkret von den Behörden bezeichneter (verdächtiger) Individuen entscheidet, wie in Europa üblich, sondern der FISC „zertifiziert“ in regelmäßigen Abständen ganz allgemein verschiedene von den NSA vorab entworfene Überwachungssysteme. Die konkrete Auswahl eines jeden einzelnen Selektors zur Überwachung wird dabei nach *Wischmeyer* aber nicht richterlich überprüft, sondern unterliegt den rein NSA-internen Aufsichtsmaßnahmen.[1170] Eine auf FISA gestützte und gerichtlich zertifizierte nachrichtendienstliche Überwachung auch der Kommunikation von US Staatsbürgern ist nach *Greenwald* dann erlaubt, wenn es sich um den Kontakt zu einem unter Beobachtung stehenden Ausländer handelt.[1171] Bei auf die presidentielle Executive Order 12333 gestützten Überwachungen bedarf es mangels Anwendbarkeit des gesetzlichen FISA-Rahmens allein gestützt auf die „Transit Authority“ des US Präsidenten keiner gerichtlichen FISC-Zertifizierungen, es genüge für die Genehmigung dieser Programme die Zustimmung des US Justizministers (Attorney General). Allerdings muss auch für auf die Executive Order 12333 gestützten Überwachungsprogramme der verfassungsrechtliche Schutz der US Staatsbürger sichergestellt werden, denn auch bei z.B. direkt im Ausland gesammelten Informationen müssen die verfassungsrechtlichen Anforderungen zum Schutz von US-Staatsbürgern gemäß 4th Amendment der US Verfassung gewahrt bleiben. *Wischmeyer* geht jedoch davon aus, dass der Schutzstandard bei auf Executive Order 12333 gestützten Überwachungen geringer ist als bei Überwachungen im gesetzlichen FISA-Rahmen.[1172] Zur Überwachung der Kommunikation von Ausländern (Nicht-US-Staatsbürger) und zum Schutz der Kommunikation von US-Staatsbürgern (4th Amendment US Verfassung), die keinen Kontakt zu einem unter Beobachtung stehenden Ausländer (Nicht-US-Staatsbürger) haben, wird operativ ein Filterungsverfahren eingesetzt, welches in seiner

1168 *Wischmeyer*, Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeit in den USA (2017) 57 ff.

1169 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 25 ff.

1170 *Wischmeyer*, Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeit in den USA (2017) 32 ff; 51 ff.

1171 *Greenwald*, Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen (2014) 185.

1172 *Wischmeyer*, Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeit in den USA (2017) 60 ff (62 f).

konkreten Umsetzung in der Fachliteratur umstritten ist. Nach *Bowden* erfolge die Herausfilterung der Kommunikation der US-Staatsbürger iSd. 4th Amendment direkt bei der NSA über eine Datenbank mit Telefonnummern und Internetidentifikatoren. *Bowden* beschreibt dies am Beispiel von Telekommunikationsüberwachungen: „*Ergab die Abfrage* [NSA geführtes Verzeichnis von mutmaßlich amerikanischen Telefonunmmern], *dass die Nummer wahrscheinlich nicht die eines Amerikaners war, konnte der Inhalt des Gesprächs gemäß Abschnitt 702 des FISA-Gesetzes ohne weitere Genehmigung abgehört werden. Handelte sich dagegen wahrscheinlich um die Nummer eines Amerikaners, wäre (gemäß einem anderen Abschnitt von FISA) für das Abhören eine weitere spezifische richterliche Anordnung erforderlich gewesen* (…)."[1173] Nach *Wischmeyer* würden die US Telekom Provider eine Deep Packet Inspection durchführen und nur iSd. 4th Amendment gefilterte Daten an die NSA weiterleiten.[1174] Analysten der US Nachrichtendienste dürfen nur auf abgefangene Inhaltsdaten zugreifen, wenn die überwachte Zielperson mit einer Wahrscheinlichkeit von über 50% kein US-Staatsbürger ist.[1175] Kommt es insofern zu einer Erfassung von Kommunikation eines US-Staatsbürgers, nennt die US Intelligence Community dies „zufällig" („incidentally"). Über das auf die presidentielle Executive Order 12333 gestützte Programm zur Erfassung sowohl der technisch bedingt über die USA laufenden reinen Ausland-Ausland-Transittelekommunikation (*„foreign to foreign communication"*) als auch der außerhalb der USA direkt im Ausland abgegriffenen Daten werden nach *Wischmeyer* u.a. Telefongespräche, Verbindungsdaten, tlw. der gesamte Mobilfunkverkehr von gewissen ausgewählten Staaten, Internetdaten, Metadaten, SMS-Texte, Nutzerdaten von Apps, Webcam-Daten, Standortdaten von Mobiltelefonen und Computern, etc. erhoben. Mangels Anwendbarkeit des 4th Amendment, weil Betroffene sind grundsätzlich nur Nicht-US-Staatsbürger, gibt es hier keine verfassungsrechtliche Beschränkung.[1176] Letztlich kann aber auch selbst für US Staatsbürger nicht final ausgeschlossen werden, dass sie nicht einer „zufälligen" („incidentally") Überwachung ausgesetzt sind. *Wischmeyer* schreibt: *„Weder die Eigenschaft als U.S.-Person noch der Aufenthalt auf U.S.-Territorium noch ein völlig rechtskonformes Verhalten schließen eine Überwachung zu nachrichtendienstlichen Zwecken von Rechts wegen kategorisch aus. Vielmehr hängt es teils vom Zufall, teils von freier Entscheidung der Behörden und nur zu einem geringen Teil von zwingenden rechtlichen Vorgaben ab, wer und*

1173 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 25.

1174 *Wischmeyer,* Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen der nachrichtendienstlichen Tätigkeiten in den USA (2017) 51 ff; 60 ff; Überblick: *Lejeune,* Datenschutz in den Vereinigten Staaten von Amerika, CR 11/2013, 755 (756).

1175 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 29.

1176 *Wischmeyer*, Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeit in den USA (2017) 49; 61 f; *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 24 ff.

was vom Staat überwacht werden darf."[1177] Die NGO *Human Rights Watch* kam im Sommer 2014 zum Ergebnis, dass aktuell die Pressefreiheit, die mediale Berichterstattung als auch das Vertrauensverhältnis zwischen Mandant und Anwalt in den USA aufgrund der Telekommunikationsüberwachung beeinträchtigt wird.[1178]

Trotz sehr kritischer weltweiter und inner-amerikanischer Medienberichte (insbesondere zwischen 1999 – 2001; 2013 – 2015) hat sich mittlerweile herausgestellt, dass das US Überwachungssystem grundsätzlich als völlig verfassungskonform mit der United States Constitution (US Verfassung) und der Rechtsprechung des US Supreme Courts anzusehen ist. *Wischmeyer* kommt aus Perspektive des US Rechts zum Ergebnis: *„Trotz ihrer hohen Eingriffsintensität halten diese Programme* (…) *einer Kontrolle an den Maßstäben des U.S.-Verfassungsrechts stand. Das sagt allerdings weniger über die Stärke der rechtsstaatlichen Sicherungen der Programme als über die Schwäche der verfassungsrechtlichen Vorgaben aus.*"[1179] Der EuGH stellte im Urteil zur Aufhebung des Angemessenheitsbeschlusses 2000/520/EG („Safe Habor") der EU-Kommission eine Verletzung der EU-GRC durch US Recht fest: „*Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens* (…)*. Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz*".[1180] Der EGMR urteilte beim britischen Überwachungsprogramm („Five Eyes"-Allianz) eine Verletzung des Art 8 EMRK: „*[T]he Court considers that the decision to operate a bulk interception regime was one which fell within the wide margin of appreciation afforded to the Contracting State.* (…) *[A]n examination of those powers has identified two principal areas of concern; first, the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination. In view of these shortcomings and to the extent just outlined, the Court finds that the section 8(4) [RIPA*[1181]*] regime does not meet the "quality of law" requirement and is incapable of keeping the "interference" to what is "necessary in a democratic society". There has accordingly been a violation of Article 8 of the Convention.*"[1182]

1177 *Wischmeyer,* Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen der nachrichtendienstlichen Tätigkeiten in den USA (2017) 99.

1178 *Human Rights Watch*, US Surveillance Harming Journalism, Law, Democracy, abrufbar unter: https://www.hrw.org/news/2014/07/28/us-surveillance-harming-journalism-law-democracy (zuletzt abgerufen am 20.06.2019); *Pitzke* in spiegel.de (28.07.2014), Das Ende der Pressefreiheit, abrufbar unter: http://www.spiegel.de/politik/ausland/human-rights-watch-nsa-ueberwachung-schadet-journalismus-a-983139.html (zuletzt abgerufen am 20.06.2019).

1179 *Wischmeyer*, Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeit in den USA (2017) 26.

1180 EuGH Urteil v. 06.10.2015, C-362/14 („Schrems") Rn 94 f.

1181 UK Regulation of Investigatory Powers Act.

1182 EGMR Urteil v. 13.09.2018, Az. 58170/13; 62322/14; 24960/15 Rn 387.

Die gesetzliche Befugnis für den Zugriff der US Intelligence Community auf die bei den großen kalifornischen US Internetkonzernen aus dem Silicon Valley gespeicherten Daten und Profile von Menschen weltweit (PRISM) ergibt sich aus Abschnitt 702 (§ 1881a) FAA. Dabei handelt es sich um den sogenannten Foreign Intelligence Surveillance Amendment Act 2008 (FAA), der die Befugnis mit sich bringt, Massenüberwachungen speziell von Daten über außerhalb der USA befindliche Nicht-US-Staatsbürger durchzuführen, deren personenbezogenen Daten in den USA bei den Internetfirmen gespeichert sind (z.B. Datenzugriff auf Daten von Ausländern im Cloud Computing, Social Media, bei sonstigen Internet Plattformen[1183]).[1184] Eine Studie der *Universität Amsterdam* erläutert folgendes Fallbeispiel im Zusammenhang mit einem nachrichtendienstlichen US Datenzugriff auf die Daten der Universität Amsterdam in einer US Cloud ohne richterlichen Befehl: „*As part of a course of an interdisciplinary master's degree program in Digital Media at a Dutch university, teams of students are required to write papers on the possibility of guaranteeing the confidentiality of whistleblowers at websites such as Wikileaks.* (…). *Developers of a new Wikileaks site who are interested in the ideas developed by the students attend an evening seminar held during the course. The university concerned uses the cloud computing services of a large U.S. service provider for the great majority of the available ICT functions for students, such as document storage, email and the e-learning environment. The physical location of the servers on which the U.S. service providers store their data is not relevant to the question of whether U.S. legislation allows access to the student data. Under Title 50 USC, Section 1881a the competent U.S. authorities, such as the National Security Agency (NSA), can, in principle, gain access to the data of the entire student population of the university concerned held by the provider, for example for the purpose of acquiring foreign intelligence information about threats to the security of the United States. There are no constitutional safeguards in the United States for Dutch users of cloud computing services who are subject to U.S. jurisdiction, since the Fourth Amendment is not applicable."*[1185]

Im Vergleich zur EMRK und der EU-GRC ist zu verstehen, dass US-Staatsbürger und Nicht-US-Staatsbürger nach US Verfassungsrecht (4th Amendment US Verfassung) einer völlig unterschiedlichen verfassungsrechtlichen Schutzwürdigkeit hinsichtlich „Privacy" unterliegen, was insofern dem europäischen Verständnis der Gewährung von allgemeinen Menschenrechten unabhängig von der Staatsbürgerschaft widerspricht (Art 8 EMRK, Art 7 – Art 8 EU-GRC). Die amerikanische Grundsatzentscheidung zum 4th Amendment Schutz der US Constitution erfolgte im Februar 1990 vom US Supreme Court im Fall *United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)*. Der US Supreme Court sprach in dieser Entscheidung zum 4th Amendment aus: *„The Fourth Amendment does not apply to the*

1183 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 15 f; 26 f.

1184 *Snowden*, Permanent Record[2] (2019), 284 f; *Wischmeyer,* Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen der nachrichtendienstlichen Tätigkeiten in den USA (2017) 35 ff; *Lejeune,* Datenschutz in den Vereinigten Staaten von Amerika, CR 11/2013, 755 (755 f.); *Greenwald*, Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen (2014) 165 f; 185.

1185 *van Hoboken/ Arnbak/van Eijk*, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act (2012) 26, abrufbar unter: https://www.ivir.nl/publicaties/download/Cloud_Computing_Patriot_Act_2012.pdf (zuletzt abgerufen am 20.06.2019).

search and seizure by United States agents of property owned by a nonresident alien and located in a foreign country. (…) *The Fourth Amendment phrase "the people" seems to be a term of art used in select parts of the Constitution, and contrasts with the words "person" and "accused" used in Articles of the Fifth and Sixth Amendments regulating criminal procedures. This suggests that "the people" refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."*[1186] Nach dieser bis heute gültigen höchstgerichtlichen Rechtsprechung des US Supreme Court besteht kein Grundrechtsschutz für Nicht-US-Staatsbürger hinsichtlich dem Zugriff auf personenbezogenen Daten, die bei den großen US IT-Konzernen gespeichert sind, außer der Nicht-US-Staatsbürger weist eine ganz besondere Beziehung zur USA auf („*a sufficient relationship with the U.S. to allow him to call upon the Constitution for protection.*"[1187]). Wann genau eine solche „hinreichende Verbindung" zu den USA besteht, um als Nicht-US-Staatsbürger trotzdem unter den verfassungsrechtlichen Schutz des 4th Amendment zu fallen, sei nach Analyse *Wischmeyers* nicht eindeutig.[1188] Aus der reinen Perspektive des US Verfassungsrechts (4th Amendment) braucht die US Intelligence Community daher keine richterliche Genehmigung, wenn sie personenbezogene Daten von Nicht-US-Staatsbürgern (*„alien"* iSv. *United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)*) abfangen bzw. erhalten will, die keine besondere Beziehung zur USA haben (also bei 95% der Weltbevölkerung).[1189] In seiner Tätigkeit als Chief Privacy Adviser von Microsoft hatte *Caspar Bowden* intensiv versucht durch interne Diskussionen mit dem Microsoft Management auf die für Europäer als Nicht-US-Staatsbürger problematische US (Verfassungs-)Rechtslage hinsichtlich der Ausgestaltung des europäischen Cloud Geschäftsmodells einzuwirken, wurde nach seinen eigenen Angaben genau deswegen sofort gekündigt. *Bowden* erklärte kurz nachdem er seinen Job bei Microsoft verloren hatte: *„Ich habe Microsoft lange Jahre beim Datenschutz beraten. Bis ich plötzlich für den Konzern Cloud-Computing (Auslagern von Daten ins Netz, Anm.) promoten sollte. Also habe ich die US-Gesetze genau studiert. Was ich im Foreign Intelligence Surveillance Act (FISA 702) gefunden habe, war erschütternd. Also bin ich zu Microsoft gegangen und habe gesagt: Wenn ihr Cloud-Computing in Europa verkauft, liefert ihr der NSA direkten Zugang zu den Daten der Europäer. Nach einer Schockstarre kam ein Manager zu mir und sagte: »Das darfst du nicht sagen bei Microsoft, ich lasse dich feuern!« Ich sagte: »Probier es.« Zwei Monate später war ich gefeuert."*[1190] Nach Snowdens Enthüllungen wurde *Caspar*

1186 United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

1187 United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) 259, 260.

1188 *Wischmeyer,* Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen der nachrichtendienstlichen Tätigkeiten in den USA (2017) 48.

1189 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 24 ff; *Greenwald*, Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen (2014) 159 ff; 165 f.

1190 *Auer* in presse.com (02.09.2014), Interview mit Caspar Bowden: "Die größte Sicherheitslücke ist Microsoft", abrufbar unter: http://diepresse.com/home/techscience/internet/3862525/Caspar-Bowden_Die-groesste-Sicherheitsluecke-ist-Microsoft (zuletzt abgerufen am 20.06.2019).

Bowden ab Sommer 2013 zum Berater des Europäischen Parlaments bestellt.[1191] Auch hier hob *Bowden* diese für Europäer problematische US Rechtslage für den LIBE Ausschuss des EU-Parlaments nochmals intensiv hervor. (S. 25): *„Der 4. Zusatzartikel gilt nicht für Nicht-US-Personen außerhalb der USA."* (S. 28): „*Nach FISA besteht für Nicht-US-Personen kein von US Behörden anerkanntes Recht auf Privatsphäre."* (S. 29): *„[D]ie Nutzung personenbezogener Daten einer Nicht-US-Person oder das Eindringen in ihre Privatsphäre [unterliegt] in der operativen Praxis der USA keinerlei Einschränkung, solange die allgemeine Definition ausländischer Geheimdienstinformation zutrifft."* (S. 27): „*Anders ausgedrückt, in den USA kann rechtmäßig eine rein politische Überwachung der in US Clouds zugänglichen Daten ausländischer Personen vorgenommen werden"*.[1192] Auch *Wischmeyer* weist präzise darauf hin, dass Maßnahmen gegen Nicht-US-Staatsbürger, die sich im Ausland befinden (z.B. personenbezogene Daten von Europäern in US Clouds, personenbezogene Daten bei einem amerikanischen Social Media Dienst, etc.) keine verfassungsrechtliche Dimension aufweisen und deshalb auch keinem amerikanischen Grundrechtsschutz unterliegen können. Würde der US Gesetzgeber trotzdem gesetzliche Regelungen zum Datenschutz von Nicht-US-Staatsbürger erlassen, würde er insofern in einem verfassungsrechtlich gar nicht determinierten Raum gesetzgeberisch tätig werden, also etwas regeln, was er aus Verfassungsgründen gar nicht regeln muss.[1193] *Börding* führt dazu aus: „*Eine systemimmanente Diskriminierung von Drittstaatlern ist den maßgeblichen europäischen Datenschutzvorschriften hinsichtlich ihres sachlichen Anwendungsbereichs fremd. Dagegen knüpft das US-Recht teilweise ausdrücklich an die Nationalität des Betroffenen an. Ausländer ohne Wohnsitz in den USA können sich nicht auf wesentliche verfassungsrechtliche Grundsätze zur Privacy berufen, die staatliche Datenzugriffe betreffen* (…) *Wie sich bereits im Zusammenhang mit dem PRISM-Programm der NSA gezeigt hat, führt dies zu einer nachhaltigen Diskriminierung von Ausländern.*"[1194]

Abseits der klaren Verfassungsrechtslage zum 4th Amendment sind jedoch auch die kodifizierten einfachgesetzlichen Anforderungen an US Überwachungsprogramme zum Schutz von US Staatsbürgern, soweit sie sich innerhalb der FISA-Definition der „electronic surveillance" bewegen, zu beachten. Überwachungsprogramme z.B. gemäß FISA 50 U.S. Code § 1881a. („Procedures for targeting certain persons outside the United States other than United States persons") müssen durch Antrag beim FISC Gericht in regelmäßigen Abständen „zertifiziert" werden. Nach gerichtlicher FISC „Zertifizierung" können dann die behördlichen Anordnungen gegen die Unternehmen ergehen. Damit werden im einfachgesetzlichen FISA-Rahmen aufgrund der richterlichen Vorabkontrolle faktisch auch Nicht-US-Staatsbürger in einem gewissen Maß „mit-geschützt". Aufgrund der verfassungsrechtlichen Anforderungen aus dem 4th Amendment zum Schutz von US Bürgern folgt aus dem

1191 *telegraph.co.uk* (13.07.2015), Caspar Bowden, privacy campaigner – obituary, abrufbar unter: http://www.telegraph.co.uk/news/obituaries/11736359/Caspar-Bowden-privacy-campaigner-obituary.html (zuletzt abgerufen 20.06.2019).

1192 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 25; 27; 28; 29.

1193 *Wischmeyer,* Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen der nachrichtendienstlichen Tätigkeiten in den USA (2017) 99.

1194 *Börding*, Ein neues Datenschutzschild für Europa, CR 7/2016, 431 (434 f.).

Supreme Court Urteil *Verdugo-Urquidez* eindeutig nicht, dass sich der Schutz von im Ausland gesammelten Informationen von dem Schutzstandard, der im Inland besteht, unterscheiden darf. Insofern bedürfen auch die auf die presidentielle Executive Order 12333 gestützten Überwachungsprogramme (Überwachung direkt im Ausland oder „foreign to foreign communication" im US Inland) gemäß 4th Amendment vergleichbarer Schutzmechanismen zum Schutz von US Staatsbürgern wie sie in FISA kodifiziert sind. Nach *Wischmeyer* bleiben die Schutzmechanismen für US-Staatsbürger in der Executive Order 12333 hinter denen des gesetzlichen FISA-Rahmens zurück.[1195]

Als Folge auf die Snowden-Veröffentlichungen vom Sommer 2013 erfolgte eine politische Reaktion der USA, um auch Nicht-US-Staatsbürger – trotz der klaren Verfassungsrechtslage – einem gewissen Schutz zuzusichern. So wurde am 17. Januar 2014 vom damaligen US Präsidenten Obama die nicht-gesetzliche Presidential Policy Directive 28 („PPD-28") herausgegeben, welche das klare Ziel verfolgt, die von Edward Snowden aufgedeckten internen Missstände und Datenmissbräuche gegenüber verfassungsrechtlich nicht-geschützten Nicht-US-Staatsbürgern mit klaren, unmittelbar vom Oberbefehlshaber der US Armee ausgesprochenen präsidentiellen Anweisungen abzustellen bzw. zumindest stark einzudämmen.[1196] Bspw. lautete eine klar formulierten Anweisung von ex US Präsidenten und ex Oberbefehlshaber Barack Obama in der PPD-28 an die damals ihm unterstellte US Intelligence Community zum Schutz von Nicht-US-Staatsbürger: *„alle Personen sind unabhängig von ihrer Nationalität oder ihrem Wohnort würde- und respektvoll zu behandeln;"*[1197] Diese nicht-gesetzliche Presidential Policy Directive 28 („PPD-28") vom Januar 2014 ist auch eines der Kernelemente in der Argumentation der EU-Kommission vom 12. Juli 2016[1198] für die erneute Feststellung[1199] eines angemessenen Datenschutzniveaus der USA bei US Unternehmen, welche sich den von der US Federal Trade Commission (FTC) herausgegebenen Privacy-Shield-Grundsätzen unterwerfen und sich dafür in die bei der FTC eingerichtete „Datenschutzschild-Liste" zertifizieren.[1200] Ob im EU-US Privacy Shield tatsächlich die Anforderungen des EuGH Urteils „Schrems"[1201] umgesetzt wurden, ist umstritten.[1202] Das Europäische Parlament vertritt seit Sommer 2018 die Auffassung, „*dass die derzeitige Datenschutzschild-Regelung nicht das angemessene Schutzniveau bietet, das*

1195 *Wischmeyer,* Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen der nachrichtendienstlichen Tätigkeiten in den USA (2017) 35 ff; 60 ff; *van Hoboken/ Arnbak/van Eijk*, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act (2012) 17, abrufbar unter: https://www.ivir.nl/publicaties/download/Cloud_Computing_Patriot_Act_2012.pdf (zuletzt abgerufen am 20.06.2019).

1196 ErwGr 68 Durchführungsbeschluss (EU) 2016/1250 (Privacy Shield).

1197 ErwGr 69 Durchführungsbeschluss (EU) 2016/1250 (Privacy Shield).

1198 ErwGr 69 ff., ErwGr 123, ErwGr 136 ff. iVm. Art 1 Abs 1 Durchführungsbeschluss (EU) 2016/1250 (Privacy Shield).

1199 Die Angemessenheitsentscheidung der EU-Kommission 2000/520/EG „Safe Habor" gemäß Art 25 Abs 6 EG-Datenschutzrichtlinie, die US Unternehmen, welche sich den Safe Habor-Grundsätzen der US Federal Trade Commission (FTC) unterworfen hatten und sich in die dafür in die bei der FTC vorgesehene Liste eingetragen (zertifiziert) haben, wurde am 06. Oktober 2015 vom EuGH in der Rechtssache C-362/14 „Schrems" für ungültig erklärt.

1200 Art 1 Durchführungsbeschluss (EU) 2016/1250 (Privacy Shield).

1201 EuGH Urteil v. 06.10.2015 – C-362/14 („Schrems").

1202 *Mense*, EU-US-Privacy-Shield – der kleinste gemeinsame Nenner angemessenen Datenschutzes? ZD 2019, 351.

nach dem EU-Datenschutzrecht und der EU-Charta gemäß der Auslegung durch den Europäischen Gerichtshof erforderlich ist."[1203] Die Europäische Kommission bestätigte im Oktober 2019 das EU-US Privacy Shield mit konkreten Verbesserungsvorschlägen.[1204]

Am 23. März 2018 unterzeichnete US Präsident Trump ein neues Gesetz mit dem Namen „Cloud Act" („Clarifying Lawful Overseas Use of Data Act"). Das Gesetz kodifiziert eine nach Literaturmeinungen schon seit Jahrzehnten bestehende Praxis, nach der die USA die Ansicht vertritt und wahrscheinlich auch erfolgreich praktiziert, exterritorialen Zugriff auf Daten zu erhalten, wenn das von US Behörden angefragte amerikanische Unternehmen rechtlich oder tatsächlich in der Lage ist, Zugang zu den Daten, die im Drittstaat gespeichert sind, zu bekommen. Betroffen von solchen exterritorialen Datenherausgabepflichten an US Behörden und die US Intelligence Community sind nach diesen Literaturmeinungen insofern schon immer Unternehmen, die rechtlich oder tatsächlich von US Unternehmen mit Sitz in den USA beherrscht werden oder am US Markt tätig sind.[1205] *Spies* legte im Jahr 2014 (v.d. Busche/Voigt, Konzerndatenschutz, 1. Auflage) mit Hinweis auf die Studie der Universität Amsterdam[1206] dar: *„Laut der Studie wird häufig missverstanden, dass der Anwendungsbereich des US-Rechts im Gegensatz zum EU-Recht nicht davon abhängt, ob die Daten in den USA gespeichert sind, sondern ob der Cloud Anbieter Dienste in den USA anbietet (beispielsweise, weil er dort niedergelassen ist oder er eine Tochtergesellschaft eines US-Unternehmens ist). Daten von nicht in den USA ansässigen Personen sind nicht vom Schutz des Vierten Verfassungszusatzes* (…) *erfasst."*[1207] Im Jahr 2019 schreibt *Spies* (v.d. Busche/Voigt, Konzerndatenschutz, 2. Auflage): „*US Behörden können daher EU-Unternehmen, die Cloud-Dienste in den USA nutzen, zur Datenfreigabe auffordern* (…) *Auch das EU-Datenschutzrecht kann diesen Konflikt nicht lösen. Das Risiko eines Datenzugriffs durch Nicht-EU-Staaten kann auch vertraglich nur sehr begrenzt eingeschränkt werden.*"[1208] Hintergrund für den – trotz der an sich bereits vorher schon in der Fachliteratur berichteten Praxis – nun im Jahr 2018 erlassenen US Cloud Act ist, dass die bisherigen US amerikanischen Rechtsgrundlagen (Stored Communications Act – SCA; Patriot Act 2001, etc.), auf die sich bisher diese exterritorialen Zugriffe stützten, nicht präzise genug waren in puncto Zugriff auf Daten, die US-Unternehmen auf Servern ihrer Tochtergesellschaften

1203 *Europäisches Parlament,* Entschließung vom 26. Juni 2018 zur Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (2018/2645(RSP)) Rn 34.

1204 *Europäische Kommission*, COM(2019) 495 final.

1205 *Kroschwald,* Informationelle Selbstbestimmung in der Cloud (2016) 394 ff; *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 275 ff; *Barnitzke*, Microsoft: Zugriff auf personenbezogene Daten in EU-Cloud auf Grund US Patriot Act möglich, MMR-Aktuell 2011, 321103; *Lejeune,* CR 11/2013, 755 (756); *van Hoboken/ Arnbak/van Eijk*, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act (2012), abrufbar unter: https://www.ivir.nl/publicaties/download/Cloud_Computing_Patriot_Act_2012.pdf (zuletzt abgerufen am 20.06.2019).

1206 *van Hoboken/ Arnbak/van Eijk*, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act (2012), abrufbar unter: https://www.ivir.nl/publicaties/download/Cloud_Computing_Patriot_Act_2012.pdf (zuletzt abgerufen am 20.06.2019).

1207 *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz (2014) Teil 7 Rn 10. (das Zitat findet sich in Busche/Voigt (Hrsg) Konzerndatenschutz 2. Auflage 2019 nicht mehr).

1208 *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 11 – Rn 12.

außerhalb der USA speichern. Die Folge waren Rechtsstreitigkeiten zwischen US-amerikanischen IT-Unternehmen und der US Regierung (z.B. „Microsoft Warrant Case“[1209]). Ein solches US Supreme Court Verfahren mit Microsoft Inc. löste letztlich den relativ kurzfristen Erlass des US Cloud Acts zur gesetzlichen Klarstellung noch vor dem Urteil des US Supreme Court Urteil aus, wodurch es dann auch nicht mehr zu einem finalen Urteil durch den US Supreme Court kam.[1210] Sehr interessant ist dabei, was im Rahmen der gerichtlichen Verhandlungen am US Supreme Court im Februar 2018 zu Tage getreten ist, wo diese US amerikanische Praxis durch die Microsoft Inc. erstmals einer höchtsgerichtlichen Überprüfung unterzogen wurde. Im Verfahren mit Microsoft Inc. wollten die amerikanischen Höchtstrichter am US Supreme Court konkret in Erfahrung bringen, ob die etablierte US Praxis des weltweiten Datenzugriffs bisher zu völkerrechtlichen Problemen mit den betroffenen Staaten geführt habe. Der Vorsitzende Richter am US Supreme Court, *John Roberts*, erklärte nachdem ihm die dbzgl. Ergebnisse dann vorlagen: *„Es ist nicht die Schuld der [US-]Regierung, dass [die Daten] im Ausland sind. Und vermutlich kümmert das die [US-]Regierung auch nicht.* (…) *Und wenn es einen konkreten Einwand jener Regierung gibt, [in deren Land] sich die Daten befinden, steht es ihr frei, [den Einwand] zu erheben, und dann wird sich die [US-]Regierung damit zu befassen haben, aber soweit ich sehe ist das hier nicht der Fall.* (…) *Keine ausländische Regierung hat sich an dieses Gericht gewandt und gesagt, dass [der Gerichtsbeschluss über den Datenzugriff] gegen ihr Recht verstoßen würde. Das US-Außenministerium und die Abteilung für internationale Angelegenheiten im US-Justizministerium haben keine Beschwerden ausländischer Regierungen darüber vernommen, wie wir seit Jahrzehnten* […] *vorgehen.“*[1211] Ein hochrangiger US Justizbeamter fügte anschließend hinzu: *„Viele der Daten, die wir erhalten, kommen aus dem Ausland. Und wir haben keine Proteste ausländischer Regierungen gehört.“*[1212] Demgemäß wurde indirekt am US Supreme Court die relative Untätigkeit Europäischer Regierungen bei der Sicherstellung des Grundrechts Datenschutz gegenüber Nicht-EU-Drittstaaten von den amerikanischen Höchstrichtern herausgearbeitet.

Mit dem neuen US Cloud Act wird die Vorschrift 18. U.S.C. § 2713 hinsichtlich des weltweiten Datenzugriffs kodifiziert. Diese bezieht nun alle Server von US-Unternehmen bzw. von ausländischen Unternehmen im Ausland, die von US Unternehmen beherrscht werden oder am US Markt tätig sind, in den Wirkungsraum der US-amerikanischen Gesetzgebung

1209 *Becker* in spiegel.de (03.01.2018), Globaler Datenzugriff – US-Gericht entscheidet über unsere Privatsphäre, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/supreme-court-entscheidet-ueber-zukunft-unserer-privatsphaere-a-1186009.html (zuletzt abgerufen am 20.06.2019).

1210 *Sokolov* in heise.de (18.04.2018), Microsoft vs. USA: Supreme Court entscheidet nicht über internationalen Datenzugriff, abrufbar unter: https://www.heise.de/newsticker/meldung/Microsoft-vs-USA-Supreme-Court-entscheidet-nicht-ueber-internationalen-Datenzugriff-4026378.html (zuletzt abgerufen am 20.06.2019).

1211 *Sokolov* in heise.de (28.02.2018), Streit über internationalen Datenzugriff der USA: Microsoft hat schlechte Karten, abrufbar unter: https://www.heise.de/newsticker/meldung/Streit-ueber-internationalen-Datenzugriff-der-USA-Microsoft-hat-schlechte-Karten-3981796.html (zuletzt abgerufen am 20.06.2019).

1212 *Sokolov* in heise.de (28.02.2018), Streit über internationalen Datenzugriff der USA: Microsoft hat schlechte Karten, abrufbar unter: https://www.heise.de/newsticker/meldung/Streit-ueber-internationalen-Datenzugriff-der-USA-Microsoft-hat-schlechte-Karten-3981796.html (zuletzt abgerufen am 20.06.2019).

ex lege mit ein.[1213] Die Bestimmung 18. U.S.C. § 2713 gemäß US CLOUD Act lautet: „*A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States*."[1214] Zusammengefasst bestätigt und präzisiert der US CLOUD Act also die bisherige, von der Fachliteratur berichtete, Rechtsansicht der US Regierung[1215] des weltweiten Zugriffs von US-Behörden auf ausschließlich im Ausland gespeicherte Daten, grundsätzlich ungeachtet eines möglichweise entgegenstehenden ausländischen Rechts. Betroffen von der Herausgabepflicht z.B. gemäß US CLOUD Act sind weltweit all jene Personen, Unternehmen und Organisationen, die von einem US-Unternehmen kontrolliert ("maßgeblich beherrscht") werden oder am US Markt tätig sind (= Herausgabe von Daten ungeachtet ihres physischen Speicherortes).[1216] Nach *Gordon* reiche bereits eine Website in englischer Sprache eines ausländischen Cloud Providers (z.B. Swiss Cloud) aus, damit der erforderliche US-Bezug für die exterritoriale Anwendbarkeit des US Cloud Acts gegeben sei.[1217] Vor dem Hintergrund des mangelnden verfassungsrechtlichen Privatssphärenschutzes für Nicht-US-Staatsbürger (= EU-Bürger) mangels Anwendbarkeit des 4th Amendment der US Verfassung verlangt Mircrosoft in einer öffentlichen Aussendung vom 11. September 2018, dass aus Sicht des Microsoft Konzerns der globale Datenzugriff (der USA) trotzdem zu begrenzen sei.[1218] *Krempl* schreibt zusammenfassend: „*Der US-Konzern fordert in seinem Papier vor allem, dass Ermittler nur mit einer vorab eingeholten Richtergenehmigung an Cloud-Provider herantreten dürfen. Derlei rudimentäre Schutzvorkehrungen sieht der Cloud Act bislang nicht vor.*"[1219] Das bereits angeführte EU-US Privacy-Shield kann nach *Thiele* in diesem Zusammenhang auch keinen Rechtsschutz für Europäer bieten, da es beim

1213 Clarifying Lawful Overseas Use of Data Act (CLOUD Act) S.2383 — 115th Congress (2017-2018), abrufbar unter: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text; *Gausling*, MMR 2018, 578.

1214 Clarifying Lawful Overseas Use of Data Act (CLOUD Act) S.2383 — 115th Congress (2017-2018), abrufbar unter: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

1215 *Kroschwald,* Informationelle Selbstbestimmung in der Cloud (2016) 394 ff; *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing (2014) 275 ff; *Barnitzke*, Microsoft: Zugriff auf personenbezogene Daten in EU-Cloud auf Grund US Patriot Act möglich, MMR-Aktuell 2011, 321103; *Lejeune,* CR 11/2013, 755 (756); *van Hoboken/ Arnbak/van Eijk*, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act (2012), abrufbar unter: https://www.ivir.nl/publicaties/download/Cloud_Computing_Patriot_Act_2012.pdf (zuletzt abgerufen am 20.06.2019).

1216 *Gausling,* Offenlegung von Daten auf Basis des CLOUD Act, MMR 2018, 578.

1217 *Emch* in srf.ch (18.08.2019), Kuschen Schweizer Cloud-Anbieter vor den USA?, abrufbar unter: https://www.srf.ch/news/wirtschaft/washington-will-unsere-daten-kuschen-schweizer-cloud-anbieter-vor-den-usa (zuletzt abgerufen am 21.08.2019).

1218 *Microsoft Inc.*, SIX PRINCIPLES FOR INTERNATIONAL AGREEMENTS GOVERNING LAW- ENFORCEMENT ACCESS TO DATA, abrufbar unter: https://blogs.microsoft.com/uploads/prod/sites/5/2018/09/SIX-PRINCIPLES-for-Law-enforcement-access-to-data.pdf (zuletzt abgerufen am 20.06.2019).

1219 *Krempl* in golem.de (18.09.2018), Cloud Act – Microsoft will Datenzugriff der USA im Ausland begrenzen, abrufbar unter: https://www.golem.de/news/cloud-act-microsoft-will-datenzugriff-der-usa-im-ausland-begrenzen-1809-136606.html (zuletzt abgerufen am 19.09.2018).

EU-US-Privacy-Shield nur um die Zulässigkeit der Übermittlung von personenbezogenen Daten in die USA zu kommerziellen Zwecken an ein in die Privacy-Shield-Liste beim FTC eingetragenes US Unternehmen geht. Es trifft aber keine Aussagen über die Rechtmäßigkeit der Verarbeitung in den USA bzw. Übermittlungen auf Basis von exterritorialen gesetzlichen Zugriffsrechten von US Behörden. Eine Übermittlung von in Europa gespeicherte Daten an US Behörden durch europäische Unternehmen (z.B. US beherrscht oder am US Markt tätig) kann dabei mit Art 48 DSGVO in Konflikt treten.[1220] Wenn jedoch die US Behörde genug Druck auf das betroffene europäische Unternehmen aufbaut inklusive eines objektiv nachvollziehbaren Bedrohungszenarios (z.B. dramatische Sanktionen bei Nichtkooperation), könnte eine solche Übermittlung, trotz des klar widersprechenden Art 48 DSGVO, aus dann „zwingendem Interesse" gemäß Art 49 Abs 1 Satz 2 DSGVO ggf. doch gerechtfertigt werden und damit letztlich „compliant" mit der DSGVO sein (vgl. dbgzl. die Ansichten der *EU-Kommission*[1221] und der *Art 29 Datenschutzgruppe*[1222]).

Es besteht nun seit dem US Cloud Act für Drittstaaten aber auch die neue Möglichkeit zum Schutz der eigenen Staatsbürger als nicht vom 4th Amendment US Verfassung geschützte Nicht-US-Staatsbürger, ein internationales Abkommen mit den USA zu schließen und so die exterritorialen Auswirkung des US Cloud Acts auf die eigenen Staatsbürger juristisch zu mindern. Insofern besteht nach *Thiele* paradoxerweise mit dem Abschluss eines sogenannten „Executive agreements on access to data by foreign governments" (EA) gemäß US Cloud Act erstmals in der Geschichte auch für Nicht-US-Bürger und ausländische Unternehmen überhaupt die Möglichkeit, die eigenen Daten vor dem Zugriff von US-Behörden über ein solches Abkommen zu schützen. Dies geschieht dadurch, dass der betroffene Drittstaat mit den EAs die gesetzlichen Zugriffbeschränkungen des Cloud Act für anwendbar erklärt und die Jurisdiktion der US-Behörden und Gerichte auf Unternehmen in seinem Staat quasi exterritorial anerkennt und mit der Anerkennung des US Rechts gleichzeitig eine Form von kodifizierten Privatsphärenschutz für seine eigenen Bürger als Nicht-US-Staatsbürger vor US Behörden erlangt (Voraussetzung dafür ist eine vorhergehende positive Einstufung als "qualifying foreign government" durch den US Kongress). Aktuell bestehen nach *Thiele* keine solche Abkommen zwischen der EU und der USA.[1223]

1220 *Thiele,* U.S. CLOUD Act – Danaergeschenk für den Europäischen Datenschutz, ZIIR 2/2018, 128 ff; *Gausling,* MMR 2018, 578; *Haar* in iX 7/2018, 128 ff – US CLOUD Act regelt internationalen Datenzugriff, abrufbar unter: https://www.heise.de/ix/heft/Wolkenbruch-4089925.html (zuletzt abgerufen am 20.06.2019).

1221 *Europäische Kommission*, BRIEF OF THE EUROPEAN COMMISSION ON BEHALF OF THE EUROPEAN UNION AS AMICUS CURIAE IN SUPPORT OF NEITHER PARTY (2018) 14 f, abrufbar unter: https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html (zuletzt abgerufen am 20.06.2019).

1222 *Art 29 Datenschutzgruppe*, WP 261 (2018) 16.

1223 *Thiele,* US Cloud Act – Danaergeschenk für den Europäischen Datenschutz, ZIIR 2/2018, 128 ff (129).

Risiken

Das *Europäische Parlament* beschrieb in seinem umfassenden Bericht vom Juni 2001[1224] erstmals sehr umfangreich die Risiken für europäische Unternehmen. Einerseits anerkannte es zwar bereits damals ganz grundsätzlich, „*dass es Bestandteil des Aufgabengebiets von Auslandsnachrichtendiensten ist, sich für wirtschaftliche Daten wie Branchenentwicklungen, Entwicklung von Rohstoffmärkten, Einhaltung von Wirtschaftsembargos, Einhaltung der Lieferregeln für Dual-use-Güter etc. zu interessieren, und dass aus diesen Gründen einschlägige Unternehmen oftmals überwacht werden.*"[1225] Andererseits wies der Europäische Parlament jedoch auch sehr kritisch darauf hin, „*dass die Nachrichtendienste der USA nicht nur allgemeine wirtschaftliche Sachverhalte aufklären, sondern Kommunikation von Unternehmen gerade bei Auftragsvergabe auch im Detail abhören und dies mit der Bekämpfung von Bestechungsversuchen begründen; dass bei detailliertem Abhören das Risiko besteht, dass die Informationen nicht zur Bekämpfung der Bestechung, sondern zur Konkurrenzspionage verwendet werden, auch wenn die USA und das Vereinigte Königreich erklären, dass sie das nicht tun.*"[1226] Der ehemalige CIA Direktor James Woolsey Jr hatte im Jahr 2000 direkt und öffentlich auf die Kritik im Europäischen Parlament verlautbart: *„Ich reserviere den Begriff Wirtschaftsspionage dafür, wenn einer Industrie direkte Vorteile verschafft werden sollen. Ich nenne es nicht Wirtschaftsspionage, wenn die USA ein europäisches Unternehmen ausspionieren, um herauszufinden, ob es durch Bestechung Aufträge in Asien oder Lateinamerika zu erhalten versucht, die es auf ehrlichem Weg nicht gewinnen würde."*[1227]

Das Europäische Parlament führte im damaligen Bericht u.a. folgende drei Fälle an:

Nach Erkenntnissen des *Europäischen Parlaments* war es durch Abhören von Faxen und Telefonaten zwischen den Verhandlungspartnern Airbus und einer saudi-arabischen Fluglinie und einer anschließenden Informationsweitergabe an Boeing und Mc-Donnell-Douglas möglich, dass die amerikanischen Flugzeughersteller ein 6 Milliarden US-Dollar Geschäft erfolgreich zu ihren Gunsten abschließen konnten und Airbus völlig leer ausging. Dabei kam es durch die NSA-Überwachung auch zu einer Aufdeckung einer möglichen Bestechung durch Airbus.[1228] Nach *Spiegel* setzte sich diese Überwachung von Unternehmen des europäischen Airbus Konzerns fort, denn im Jahr 2015 berichtete der *Spiegel* über die verstärkte nachrichtendienstliche Zusammenarbeit zwischen Deutschland und den USA

1224 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)).

1225 *Europäisches Parlament,* Entschließung vom 05. September 2001 zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)) Erwägung Punkt O.

1226 *Europäisches Parlament,* Entschließung vom 05. September 2001 zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)) Erwägung Punkt P.

1227 *Rötzer* in heise.de (12.03.2000), Ex-CIA-Direktor bestätigt Wirtschaftsspionage mittels Echelon, abrufbar unter: https://www.heise.de/newsticker/meldung/Ex-CIA-Direktor-bestaetigt-Wirtschaftsspionage-mittels-Echelon-20861.html (zuletzt abgerufen am 20.06.2019).

1228 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 108 f.

zur Terrorabwehr seit dem Jahr 2001 folgendes[1229]: „*Die NSA hat offenbar mit Wissen des Bundesnachrichtendienstes Unternehmen und Behörden in Deutschland und im übrigen Westeuropa ausgespäht.* (…) *Bei den Selektoren von der NSA stellte sich spätestens 2008 heraus, dass sie nicht nur Terrorpaten und Waffenschmuggler betrafen. Die Suche zielte, unter anderem, auf den Rüstungskonzern EADS, den Hubschrauberhersteller Eurocopter und französische Behörden. Erst nach den Enthüllungen des Whistleblowers Edward Snowden entschloss sich der BND dazu, diesen Merkwürdigkeiten auf den Grund zu gehen.*“[1230]

Nach Erkenntnissen des *Europäischen Parlaments* und einer späteren Buchveröffentlichung im Jahr 2012 des ehemaligen Leiters der Informationssicherheit & Safety bei der Adam Opel AG, *Alexander Tsolka*[1231], konnte durch einen Mitschnitt eines von der NSA via Abhörstation Bad Aibling abgehörten Gesprächs zwischen dem damaligen Vorstandsvorsitzenden der Volkswagen AG und dem damaligen GM-Einkaufschef José Ignacio López die medial als „López Affäre“ bekannte Problematik für die Volkswagen AG Mitte Anfang der 1990er Jahre losgetreten werden, nachdem diese Abhördaten an General Motors weitergegeben wurden.[1232] Das *Europäische Parlament* appellierte in der Folge u.a. an die Bundesrepublik Deutschland, „*die weitere Gestattung von Abhören von Kommunikation durch Nachrichtendienste der USA auf ihrem Gebiet davon abhängig zu machen, dass diese im Einklang mit der EMRK stehen, d.h. dass sie dem Verhältnismäßigkeitsgrundsatz genügen, ihre Rechtsgrundlage zugänglich und die Wirkung für den Einzelnen absehbar ist, sowie dass eine entsprechend effiziente Kontrolle besteht.*“[1233]

Nach Erkenntnissen des *Europäischen Parlaments* wurde in den 1990er Jahren die Kommunikation des ursprünglichen Gewinners eines brasilianischen Milliardenauftrages zur Satellitenüberwachung des Amazonas, das europäische Konsortium Thomson-Alcatel, durch die NSA/CIA überwacht, wodurch es zur Aufdeckung von Korruption (Bestechungsgelder) kam und der damalige US Präsident Clinton erfolgreich bei der brasilianischen Regierung intervenieren konnte. Anschließend erfolgte eine Neuvergabe des Auftrags an das US Unternehmen Raytheon.[1234] Das Wochenmagazin *Focus* beschreibt im Jahr 2013 den Fall etwas anders als das Europäische Parlament im Jahr 2001 im damaligen Echelon-Bericht:

1229 DER SPIEGEL 19/2015, 20 ff, Der unheimliche Dienst, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/134762481 (zuletzt abgerufen am 20.06.2019).

1230 DER SPIEGEL 18/2015, 36 ff, 40.000 Unwahrheiten, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/134660862 (zuletzt abgerufen am 20.06.2019).

1231 *Tsolkas/Wimmer,* Wirtschaftsspionage und Intelligence Gathering (2012) 22.

1232 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 110; *Tsolkas/Wimmer,* Wirtschaftsspionage und Intelligence Gathering (2012) 22; *Baumann* in Frankfurter Rundschau (05.07.2013), Betreiben die USA Wirtschaftsspionage? abrufbar unter: https://www.fr.de/wirtschaft/betreiben-wirtschaftsspionage-11278668.html (zuletzt abgerufen am 20.06.2019).

1233 *Europäisches Parlament,* Entschließung vom 05. September 2001 zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)) Empfehlung 26.

1234 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 111; *Baumann* in Frankfurter Rundschau (05.07.2013), Betreiben die USA Wirtschaftsspionage? abrufbar unter: https://www.fr.de/wirtschaft/betreiben-wirtschaftsspionage-11278668.html (zuletzt abgerufen am 20.06.2019).

„1994 verlor die französische Thomson-CSF unerwartet einen 1,3-Milliarden-Auftrag für das brasilianische Projekt SIVAM, ein Überwachungssystem für den Amazonas. Jahre später erst bekamen die französischen Dienste mit, dass die französischen Manager über das damalige System Echelon abgehört wurden. So konnte US-Konkurrent Raytheon das Schmiergeld erhöhen.“[1235]

Bei der Ausgestaltung des aktuellen amerikanischen Überwachungssystems werden zudem zahlreiche technische Dienstleistungen an Privatunternehmen outgesourct („Private Contractors“).[1236] *Edward Snowden* beschreibt in seiner Biographie „Permanent Record“ im Kapitel „Homo contractus“ diese amerikanische Outsourcing-Praxis sehr detaillreich.[1237] Der *Spiegel* berichtete zu den Sorgen von Industrieunternehmen iZh. mit diesen „Private Contractors“ folgendes: „*Nach den Enthüllungen um den massenhaften Datenabgriff aus den USA ist die Nervosität deutscher Manager sogar noch gewachsen. Die EADS-Spitze um Tom Enders hat ihre Abwehrmaßnahmen erneut verschärft. »Viele Dokumente, die früher noch per E-Mail verschickt wurden, reichen wir nun in noch größerer Zahl persönlich an den Empfänger weiter«, sagt ein EADS-Mann. Elektronisch werde nur noch das versendet, was man auch ohne Bedenken am Schwarzen Brett oder »an der Kirchentür« aushängen könnte. Enders und seine Leute sind da kein Einzelfall. Viele treibe gerade die Sorge um, was die NSA denn mit all den Daten anfange, die sie vermutlich auch über deutsche Unternehmen sammelt, sagt Ulrich Brehmer, Vorstandsmitglied der Arbeitsgemeinschaft für Sicherheit der Wirtschaft. Er will damit noch nicht einmal andeuten, dass US-Geheimdienste gezielt Industrie-Know-how aus Deutschland abgreifen und an ihre Heimatfirmen verteilen. Brehmer ist eher kein Verschwörungstheoretiker. Ihm macht Sorge, dass die US-Geheimdienste mit privatwirtschaftlichen Beratern zusammenarbeiten. »Wer weiß denn, ob die nicht die eine oder andere Info an interessierte Seiten weiterverkaufen«, so Brehmer. Die Gefahr des Datenmissbrauchs sei »hoch«, sagt der Fachmann.*“[1238] Auch der ehemalige technische Direktor der NSA und spätere Whistleblower, *William Binney,* äußerste sich im August 2017 auf die Frage zum Risiko einer zweckwidrigen Weiterverwendung der abgefangenen Daten für kommerzielle Zwecke: *„Nun, sie haben all diese Daten und die Systeme werden von externen Firmen gewartet, die auch Zugriff darauf haben. So ist auch Edward Snowden, der ja für Booz Allen Hamilton gearbeitet hat, an seine Dokumente gekommen.*

1235 *Weber-Lamberdière* in focus.de (07.07.2013), Die langen Ohren Frankreichs: Wie uns die Grande Nation groß ausspioniert, abrufbar unter: https://www.focus.de/politik/ausland/tid-32242/spezialgebiet-wirtschaftsspionage-die-langen-ohren-frankreichs-wie-uns-die-grande-nation-gross-ausspioniert_aid_1036856.html (zuletzt abgerufen am 20.06.2019).

1236 *Rüb* in faz.net (11.06.2013), Amerikas Geheimdienste. Eine Truppe von mehr als 850.000 Mann, abrufbar unter: http://www.faz.net/aktuell/politik/ausland/amerika/amerikas-geheimdienste-eine-truppe-von-mehr-als-850-000-mann-12217135.html (zuletzt abgerufen am 20.06.2019); DER SPIEGEL 32/2013, 34, Wirtschaftsspionage – Der Feind in meinem Netz, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/105648238 (zuletzt abgerufen am 20.06.2019).

1237 *Snowden*, Permanent Record[2] (2019), 144 ff.

1238 DER SPIEGEL 32/2013, 34, Wirtschaftsspionage – Der Feind in meinem Netz, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/105648238 (zuletzt abgerufen am 20.06.2019).

Sie haben die Möglichkeit auf diese Daten zuzugreifen, und werden es wohl auch tun."[1239] Der Berichterstatter des Echelon-Berichts des Europäischen Parlaments aus dem Jahr 2001[1240], *Gerhard Schmid*[1241], erklärte am 05. September 2013 im Rahmen der Sitzung des Innenausschusses des Europäischen Parlaments: *„Die NSA verwendet 70% ihres Etats für Vertragsfirmen, angeblich sind auch Teile des Abhörgeschäfts an Private ausgelagert. Da stellt sich die Frage: Wer alles bekommt die Daten?"*[1242]

Zusammengefasst lässt sich nach Erkenntnissen des früheren Chefredakteurs des Nachrichtenmagazins „Der Spiegel" und heutigem Herausgeber der Tageszeitung „Die Welt", *Stefan Aust* und *Thomas Ammann*, stellvertretender Chefredakteur Wochenmagazin „Stern", zu den genannten Risiken folgendes sagen: *„Über die Methoden der Bespitzelung deutscher Großkonzerne weiß man bisher nichts. Aber alle Verfahren gegen deutsche Vorzeigeunternehmen wie Daimler oder Siemens, die irgendwo in der Welt gegen amerikanische Compliance-Regeln verstoßen hatten, wurden durch Informationen der NSA ins Rollen gebracht, wie uns ein hochrangiger deutscher Geheimdienst-Insider berichtete. Edward Snowden bestätigte das in seinem Interview mit der ARD: »Wenn es etwa bei Siemens Informationen gibt, die dem nationalen Interesse der Vereinigten Staaten nutzen – aber nichts mit der nationalen Sicherheit zu tun haben – dann nehmen sie sich diese Informationen trotzdem.« Offiziell geben die Börsenaufsicht SEC und das US-Justizministerium nichts bekannt über ihre Quellen für diese im globalen Wirtschaftskrieg wichtigen Informationen."*[1243]

In der Frankfurter Rundschau führt *Baumann* zusammenfassend aus: „*Der ehemalige NSA-Mitarbeiter Binney aber warnt, dass sich die gesammelten Daten einfach missbrauchen lassen. Schon der Fall Snowden zeige, wie einfach Informationen aus dem Datenpool gezogen werden könnten. Und da innerhalb der NSA zahlreiche Mitarbeiter von anderen Unternehmen arbeiteten, bestehe stets die Gefahr, dass diese Unternehmen Daten entwendeten, um sich damit in der freien Wirtschaft gegenüber Wettbewerbern einen Vorteil zu verschaffen.*"[1244]

Die Studie der *Universität Amsterdam* zum Cloud Computing weist zudem noch auch auf folgende Fragestellungen hin: „*It should also be noted here that only limited information is available about interdependencies and collaboration between the various organizations*

1239 *Dax* in futurzone.at (11.08.17), Interview mit William Binney, abrufbar unter: https://futurezone.at/netzpolitik/massenueberwachung-ist-gegen-terrorismus-wirkungslos/280.046.881 (zuletzt abgerufen am 20.06.2019).

1240 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI))

1241 *Schmid*, *Gerhard Dr.*, Abgeordneten-Datenbank des Europäischen Parlaments, abrufbar unter: http://www.europarl.europa.eu/meps/de/1239/GERHARD_SCHMID_home.html (zuletzt abgerufen am 20.06.2019).

1242 *Schmid* in europarl.europa.eu, Sprechzettel für die Sitzung des Innenausschusses des Europäischen Parlaments am 5.9.2013, 2, abrufbar unter: http://www.europarl.europa.eu/document/activities/cont/201312/20131203ATT75410/20131203ATT75410EN.pdf (zuletzt abgerufen am 20.06.2019).

1243 *Aust/Ammann*, Digitale Diktatur: Totalüberwachung, Datenmissbrauch, Cyberkrieg (2014) 288.

1244 *Baumann* in Frankfurter Rundschau (05.07.2013), Betreiben die USA Wirtschaftsspionage? abrufbar unter: https://www.fr.de/wirtschaft/betreiben-wirtschaftsspionage-11278668.html (zuletzt abgerufen am 20.06.2019).

and officials such as the Attorney General, the Director of National Intelligence, the NSA, the U.S. Marshals and the FBI and the extent to which their remits overlap. The Washington Post recently published a study of the complex interplay between the intelligence and security agencies in the United States."[1245]

6.2.3 Russland

Nach Feststellung des *Europäischen Parlaments* sind neben den UKUSA Staaten nur noch Russland und Frankreich in der Lage ein globales Telekommunikationsabhörsystem weltweit zu betreiben. Hintergrund ist, dass für den Betrieb eines solchen Abhörsystems Satellitenempfangsstationen im Bereich des Atlantiks, im Bereich des Indischen Ozeans und im pazifischen Raum Voraussetzung sind, wobei diese Empfangsstationen – als zusätzliche Herausforderung für Russland – alle außerhalb der Hoheitsgebiete und der politischen Einflussbereiche der UKUSA-Staaten liegen müssen. Russland verfügt als größtes Land der Erde über ausreichend eigene Territorien sowie über weitere zusätzliche Stützpunkte in Syrien, Vietnam, Kuba und Venezuela. Damit hätte Russland ausreichend Stützpunkte in allen diesen für den Betrieb eines globalen Abhörsystems erforderlichen geografischen Regionen. Der russische Nachrichtendienste FAPSI (Federal Agency of Government Communications and Information) und GRU (leitendes Zentralorgan des russischen Militärnachrichtendienstes) sollen nach Erkenntnissen des *Europäischen Parlaments* solche Empfangsstationen für Abhörmaßnahmen der weltweiten Telekommunikation betreiben.[1246]

Die Russische Föderation ist im Jahr 1996 dem Europarat beigetreten und hat anschließend die Europäische Menschenrechtskonvention EMRK unterzeichnet und ratifiziert. Russland hat sich durch den EMRK Beitritt verpflichtet die dort kodifizierten Menschenrechte – und in diesem Kontext insbesondere Art 8 EMRK – einzuhalten und zu garantieren. Insofern ist es Russland aus rein juristischer Perspektive nicht so leicht möglich hinsichtlich der Schutzwürdigkeit im Rahmen von Überwachungsmaßnahmen zwischen russischen Staatsbürgern und Nicht-russischen-Staatsbürgern so stark zu unterscheiden wie dies bspw. der USA als Nicht-EMRK-Mitglied möglich ist, denn die EMRK garantiert allgemeine von den Vertragsstaaten zu respektierende Menschenrechte. Im Dezember 2015 wurde Russland vom Europäischen Gerichtshof für Menschenrechte EGMR in Straßburg verurteilt, weil die geheime russische Telekommunikationsüberwachung gegen das in Europa und von Russland völkerrechtlich anerkannte Menschenrecht auf Achtung des Privatlebens verstößt (Art 8 EMRK). Nach Ansicht des EGMR fehlen im russischen Recht ausreichende Garantien gegen Willkür und Missbrauch geheimer Abhörpraktiken.[1247]

1245 *van Hoboken/ Arnbak/van Eijk*, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act (2012) 26, abrufbar unter: https://www.ivir.nl/publicaties/download/Cloud_Computing_Patriot_Act_2012.pdf (zuletzt abgerufen am 20.06.2019).

1246 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 81 ff; *Europäisches Parlament,* Entschließung vom 05. September 2001 zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)) Punkt E.

1247 EGMR Urteil v. 04.12.2015, Az. 47143/06; *Raab* in beck.de, EGMR: Russische Überwachungs gesetze verstoßen gegen EMRK, abrufbar unter:

Seit 01. September 2015 sind in Russland zudem auch private Unternehmen als datenverarbeitende Stellen, verpflichtet sämtliche personenbezogenen Daten über russische Bürger in Rechenzentren innerhalb der Russischen Föderation zu speichern. Der russischen Telekommunikations- und Medienaufsichtsbehörde Roskomnadzor (RKN) sind dabei von den Unternehmen die konkreten Standorte der Server mitzuteilen. Dieses russische „Datenschutzgesetz" hat zur Folge, dass Internetunternehmen wie bspw. Google Inc., Apple Inc., Booking.com, etc. gewisse personenbezogene Daten unmittelbar auf russische Server verschieben müssen.[1248]

6.2.4 Frankreich

Frankreich ist nach einer Analyse des *Europäischen Parlaments* neben Russland und den UKUSA-Staaten noch das einzige Land der Welt, welches die geographischen Voraussetzungen erfüllt, ein weltweites Telekommunikationsabhörsystem vergleichbar dem der UKUSA-Staaten zu betreiben. Frankreich verfügt über Territorien in Saint Pierre et Miquelan östlich von Kannada, Guadeloupe nordöstlich von Südamerika, Französisch Guyana an der Nordküste Südamerikas, Mayotte und La Réunion im Indischen Ozean sowie Nouvelle Calédonie, Wallis et Futana und Polynése Francais im Pazifik. Nach Erkenntnissen des *Europäischen Parlaments* und dem Wochenmagazin *Focus* soll der französische Nachrichtendienst DGSE (Direction générale de la sécurité extérieur) auch Empfangsstationen für Abhörmaßnahmen der weltweiten Telekommunikation betreiben und die im Meer verlegten Glasfaserkabel anzapfen.[1249] Im Jahr 2000 wurde das französische Abhörsystem – in Anlehnung an das als „Echelon-System" bezeichnete globale Abhörsystem der angelsächsischen „Five Eyes Allianz" – medial als „Frenchelon" bezeichnet.[1250] So sollen die „Super-Rechner" des französischen Geheimdienstes DGSE nach Berichten des *Focus* mit Stand 2013 bei einem nachrichtendienstlichen Budget von 650 Millionen Euro (Vergleich

https://rsw.beck.de/cms/?toc=ZD.ARC.201602&docid=376184 (zuletzt abgerufen 20.06.2019); *dpa/ahe/LTO-Redaktion* in LTO.de (07.12.2015), EGMR verurteilt Russland Verstoß gegen Grundrechte, abrufbar unter: https://www.lto.de/recht/nachrichten/n/egmr-russland-abhoer-missbrauch-privatsphaere-verfassungsgericht/ (zuletzt abgerufen 20.06.2019).

1248 *Triebe* in faz.net (04.09.2015), Datenspeicherung in Russland: Unbehagen über neues Datenschutzgesetz, abrufbar unter: http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/kreml-will-russische-nutzerdaten-in-russland-speichern-13784269.html (zuletzt abgerufen am 20.06.2019).

1249 *Europäisches Parlament*, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) 81 f; *Europäisches Parlament,* Entschließung vom 05. September 2001 zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)) Punkt E; *Weber-Lamberdière* in focus.de (07.07.2013), Die langen Ohren Frankreichs: Wie uns die Grande Nation groß ausspioniert, abrufbar unter: https://www.focus.de/politik/ausland/tid-32242/spezialgebiet-wirtschaftsspionage-die-langen-ohren-frankreichs-wie-uns-die-grande-nation-gross-ausspioniert_aid_1036856.html (zuletzt abgerufen am 20.06.2019).

1250 *Thorel* in zdnet.com (30.06.2000), Frenchelon – France has nothing to envy in Echelon, abrufbar unter: https://www.zdnet.com/article/frenchelon-france-has-nothing-to-envy-in-echelon/ (zuletzt abgerufen am 20.06.2019); *Wikipedia.de*, Frenchelon, abrufbar unter: https://en.wikipedia.org/wiki/Frenchelon (zuletzt abgerufen am 20.06.2019).

Budget NSA: Schätzungen zwischen 10 – 30 Milliarden US Dollar) ca. eine Milliarde abgefangene Kommunikationseinheiten bearbeiten können[1251]: „*Der französische Geheimdienst sammelt systematisch alle elektromagnetischen Signale ein, die den Datenverkehr zwischen Frankreich und Deutschland sowie vielen anderen Ländern betreffen. Ausspioniert werden also E-Mails, SMS, Telefonate, Facebook und Twitter. Gespeichert werden diese immensen Datenmengen mehrere Jahre lang.* (…)." [1252] Die frühere und im August 2017 verstorbene französische Handelsministerin *Nicole Bricq* forderte in einer öffentlichen Ansage im Herbst 2013 am Höhepunkt der NSA-Snowden-Affäre eine Intensivierung der französischen Spionage: *„Wirtschaftsspionage ist eine Realität. Da nützt kein Jammern. Ich denke, wir müssen besser sein und besser organisiert."*[1253] Das Wochenmagazin *Focus* schreibt auf Basis dem Magazin vorliegender Indizien (WikiLeaks) folgendes (Stand 2013): *„Der französische Auslandsgeheimdienst Direction Générale de la Sécurité Extérieure (DGSE) gibt alle heiklen Daten direkt an Großunternehmen wie Renault weiter – in einem abhörsicheren Raum im Untergeschoss des Amtssitzes am Boulevard Mortier in Paris."*[1254]

Europarechtlich ist aus Datenschutzsicht (Art 8 EU-GRC, DSGVO) zu beachten, dass das EU-Datenschutzrecht und die EU-Grundrechte-Charta im Politikbereich der „nationalen Sicherheit" (einschließlich des Schutzes des wirtschaftlichen Wohls des Staates, soweit es mit Fragen der Sicherheit des Staates zusammenhängt[1255]) nicht zur Anwendung gelangen; es gilt alleine französisches (Verfassungs-)Recht (vgl. Art 4 Abs 2 Satz 3 EUV iVm. Art 51 EU-GRC; ErwGr 16 iVm. Art 2 Abs 2 lit a DSGVO; Art 2 Abs 3 lit a DSRL-IJ; Art 1

1251 *Weber-Lamberdière* in focus.de (07.07.2013), Die langen Ohren Frankreichs: Wie uns die Grande Nation groß ausspioniert, abrufbar unter: https://www.focus.de/politik/ausland/tid-32242/spezialgebiet-wirtschaftsspionage-die-langen-ohren-frankreichs-wie-uns-die-grande-nation-gross-ausspioniert_aid_1036856.html (zuletzt abgerufen am 20.06.2019); *datenschutzbeauftragter-info.de* (08.10.2013), Wie Verbündete sich gegenseitig ausspionieren, abrufbar unter: https://www.datenschutzbeauftragter-info.de/wie-verbuendete-sich-gegenseitig-ausspionieren/ (zuletzt abgerufen am 20.06.2019).

1252 *Weber-Lamberdière* in focus.de (07.07.2013), Die langen Ohren Frankreichs: Wie uns die Grande Nation groß ausspioniert, abrufbar unter: https://www.focus.de/politik/ausland/tid-32242/spezialgebiet-wirtschaftsspionage-die-langen-ohren-frankreichs-wie-uns-die-grande-nation-gross-ausspioniert_aid_1036856.html (zuletzt abgerufen am 20.06.2019).

1253 *max/Reuters/dpa* in spiegel.de (29.10.2013), NSA-Spähaffäre. Frankreich will USA bei Wirtschaftsspionage übertrumpfen, abrufbar unter: http://www.spiegel.de/politik/ausland/frankreich-will-usa-bei-wirtschaftsspionage-uebertrumpfen-a-930723.html (zuletzt abgerufen am 20.06.2019).

1254 *Weber-Lamberdière* in focus.de (07.07.2013), Die langen Ohren Frankreichs: Wie uns die Grande Nation groß ausspioniert, abrufbar unter: https://www.focus.de/politik/ausland/tid-32242/spezialgebiet-wirtschaftsspionage-die-langen-ohren-frankreichs-wie-uns-die-grande-nation-gross-ausspioniert_aid_1036856.html (zuletzt abgerufen am 20.06.2019); *datenschutzbeauftragter-info.de* (08.10.2013), Wie Verbündete sich gegenseitig ausspionieren, abrufbar unter: https://www.datenschutzbeauftragter-info.de/wie-verbuendete-sich-gegenseitig-ausspionieren/ (zuletzt abgerufen am 20.06.2019).

1255 Gemäß den Erläuterungen zur EU-Grundrechte-Charta (C 303/20) stützt sich Art 8 EU-GRC direkt auf Art 16 AEUV (ex Art 286 EG-Vertrag) und auf die EG-Datenschutzrichtlinie 95/46/EG: vgl. ErwGr 13 iVm. Art 3 Abs 2 DSRL 95/46/EG; bzw. Art 94 Abs 2 iVm. ErwGr 16 und Art 2 Abs 2 lit a DSGVO; siehe auch **Kapitel 1.1.5.**

Abs 3 ePrivacy-RL).[1256] Vgl. dazu **Kapitel 1.1.5.** bzgl. der Ansicht des *Europäischen Parlaments* zur Thematik (Wirtschafts-)Spionage.

Frankreich ist jedoch an die völkerrechtlichen Anforderungen aus Art 8 EMRK und die Judikatur des EGMR zur Auslandsaufklärung gebunden.[1257] Zusätzlich gelten für Frankreich auch die Anforderungen aus der Entschließung des Europäischen Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs (96/C 329/01).[1258]

6.2.5 Bundesrepublik Deutschland

Auslandsaufklärung im Inland

Die Bundesrepublik Deutschland ist aus historischen Gründen (Abtretung aller deutschen Überseegebiete nach dem I. Weltkrieg 1919 an die Ententemächte[1259]) geographisch nicht in der Lage wie die UKUSA Staaten bzw. Frankreich oder Russland Empfangstationen für ein weltweites Telekommunikationsabhörsystem zu betreiben.[1260] Deutschland spielt trotzdem hinsichtlich der Kontrolle der europäischen Telekommunikation eine Schlüsselrolle. Der weltweit größte Netzwerkknoten mit dem Namen DE-CIX (Deutsche Commercial Internet Exchange) befindet sich in Frankfurt am Main auf deutschem Staatsgebiet. Die Bundesrepublik Deutschland betreibt dort eine Form von strategischer Fernmeldekontrolle („Auslandsaufklärung im Inland").[1261] Technisch wird dabei in ausgewählte Glasfaserleitungen auf deutschem Boden eine Abzweigung für den Geheimdienst BND eingebaut. In dieser Abzweigung wird dann das durchgeleitete Licht, welches die Daten transportiert, gebrochen (Prisma) und in ein Glasfaserkabel des BND gelenkt. Der BND erhält auf diese Weise eine ungefilterte und vollständige Kopie der über deutschen Boden gerouteten Auslands-Telekommunikation.[1262]

Aus Datenschutzsicht ist zu beachten, dass das EU-Datenschutzrecht und die EU-Grundrechte-Charta im Politikbereich der „nationalen Sicherheit" (einschließlich des Schutzes des wirtschaftlichen Wohls des Staates, soweit es mit Fragen der Sicherheit des Staates zusammenhängt[1263]) nicht zur Anwendung gelangen; es gilt alleine deutsches

1256 *Art 29 Datenschutzgruppe* WP 228 (2014) 42.

1257 EGMR Urteil v. 29.06.2006, Az. 54934/00; EGMR Urteil v. 04.12.2015, Az. 47143/06; EGMR Urteil vom 12.01.2016, Az. 37138/14; EGMR Urteil v. 19.06.2018, Az. 35252/08; EGMR Urteil vom 13.09.2018, Az. 58170/13; Az. 62322/14; Az. 24960/15.

1258 Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs Amtsblatt Nr. C 329 vom 04/11/1996 S. 0001 – 0006.

1259 Art 119 Versailler Vertrag (RGBl 1919 S. 687).

1260 *Europäisches Parlament,* Entschließung vom 05. September 2001 zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)) Punkt E.

1261 BVerwG Urteil v. 30. Mai 2018, Az. BVerwG 6 A 3.16 = NVwZ 2018, 1476.

1262 *Mascolo/Steinke* in sueddeutsche.de (28.05.2018), Überwachung am De-Cix: Betreiber des weltgrößten Internetknotens wirft BND Rechtsbruch vor, abrufbar unter: https://www.sueddeutsche.de/digital/ueberwachung-am-de-cix-betreiber-des-weltgroessten-internetknotens-wirft-bnd-rechtsbruch-vor-1.3994191 (zuletzt abgerufen am 20.06.2019).

1263 Gemäß den Erläuterungen zur EU-Grundrechte-Charta (C 303/20) stützt sich Art 8 EU-GRC direkt auf Art 16 AEUV (ex Art 286 EG-Vertrag) und auf die EG-Datenschutzrichtlinie

(Verfassungs-)Recht (vgl. Art 4 Abs 2 Satz 3 EUV iVm. Art 51 EU-GRC; ErwGr 16 iVm. Art 2 Abs 2 lit a DSGVO; Art 2 Abs 3 lit a DSRL-IJ; Art 1 Abs 3 ePrivacy-RL).[1264] Vgl. dazu **Kapitel 1.1.5** bzgl. der Ansicht des *Europäischen Parlaments* zur Thematik (Wirtschafts-)Spionage.

Der deutsche Gesetzgeber unterscheidet bei der Auslandsaufklärung des BND folglich zwischen der als (europa-)rechtskonform angesehenen „*Aufklärung von wirtschaftspolitisch bedeutsamen Vorgängen*" und einer als unzulässig betrachteten „*Wirtschaftsspionage*", definiert als „*Informationsgewinnung und -nutzung zur Erzielung von Wettbewerbsvorteilen*".[1265]

Deutschland ist wie Frankreich an die völkerrechtlichen Anforderungen des Art 8 EMRK gebunden[1266] und unterliegt bei der operativen Durchführung der strategischen Fernmeldeaufklärung den vom EGMR definierten Vorgaben an Nachrichtendienste.[1267] Zudem gilt für Deutschland auch die EU-Anforderungen gemäß der Entschließung des Europäischen Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs (96/C 329/01).[1268]

Zur Sicherstellung des Fernmeldegeheimnisses (Art 10 GG) im Rahmen der innerdeutschen strategischen Fernmeldekontrolle („Auslandsaufklärung im Inland") erfolgt eine Herausfilterung der dem Art 10 GG unterliegenden deutschen Telekommunikationsdaten (§ 6 Abs 4 BND-G). Die Schwierigkeit besteht wie folgt: Inländische und ausländische Telekommunikation ist in der heutigen Zeit nur mehr schwer zu unterschieden. Wenn zwei Deutsche sich über den US-Kurznachrichtendienst WhatsApp Mitteilungen hin und herschicken, handelt es sich technisch um ausländischen Datenverkehr, da dies über die Leitungen und die Server eines US-Unternehmens geschieht (WhatsApp Inc. bzw. facebook Inc.). Faktisch kommunizieren aber zwei deutsche Staatsbürger bzw. sich im deutschen Inland aufhältige Drittstaatsbürger miteinander. Rechtskonform überwacht werden darf aber nur „Auslandskommunikation" (Ausland-Ausland-Fernmeldeaufklärung; § 6 Abs 1 BND-G). Der BND soll mittlerweile technisch in der Lage sein, auch eine solche rein deutsche bzw. inländische Kommunikation, die technisch aber über Dienstleister in Drittstaaten wie den USA geht (Bsp. WhatsApp), grundrechtskonform mit Art 10 GG von der strategischen Überwachung erfolgreich herauszufiltern. Der BND arbeitet dabei mit komplexen und mehrdimensionalen Filtern, womit sichergestellt werden soll, dass rein deutscher bzw. inländischer Datenverkehr, auch wenn er über US Dienstleister wie WhatsApp läuft, nicht überwacht wird. Dazu werden vom BND bspw. Geodaten, Browser- und Programmeinstellungen verwendet, um

---

95/46/EG: vgl. ErwGr 13 iVm. Art 3 Abs 2 DSRL 95/46/EG; bzw. Art 94 Abs 2 iVm. ErwGr 16 und Art 2 Abs 2 lit a DSGVO; siehe auch **Kapitel 1.1.5.**

1264 *Art 29 Datenschutzgruppe* WP 228 (2014) 42.

1265 BT-Drs. 18/9041, 22; 24; § 6 Abs 1 und Abs 5 BND-G idF. BGBl. 2016 I. S. 3346 (Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes).

1266 BGBl. 2002 II. 1054.

1267 EGMR Urteil v. 29.06.2006, Az. 54934/00; EGMR Urteil v. 04.12.2015, Az. 47143/06; EGMR Urteil vom 12.01.2016, Az. 37138/14; EGMR Urteil v. 19.06.2018, Az. 35252/08; EGMR Urteil vom 13.09.2018, Az. 58170/13; Az. 62322/14; Az. 24960/15.

1268 Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs Amtsblatt Nr. C 329 vom 04/11/1996 S. 0001 – 0006.

erfolgreich die von Art 10 GG geschützte Kommunikation herauszufiltern. Diese Mechanismen sind nach Angaben der Deutschen Bundesregierung zu 99 Prozent wirksam. Wenn dann doch irrtümlich eine dem Art 10 GG unterliegende E-Mail oder eine Messenger Kommunikation durchrutsche, werde sie von Hand entfernt.[1269] Der Betreiber des Netzwerkknotens DE-CIX klagte trotzdem die Bundesrepublik Deutschland, da er durch ein Gutachten des ehemaligen Präsidenten des Bundesverfassungsgerichts *Hans-Jürgen Papier* zur Erkenntnis kam, dass die in Frankfurt am Main stattfindende „Auslandsaufklärung im Inland" mit Hilfe von Filtern – nach abweichender Ansicht *Papiers* und *DE-CIX* – umfassend vom verfassungsrechtlichen Fernmeldegeheimnis nach Art 10 GG geschützt sei und damit klar rechtswidrig sei (vgl. **Kapitel 2.2.1**).[1270] Als Reaktion darauf stellte der Deutsche Bundestag diese Abhörpraxis auf ein neues rechtliches Fundament und normierte eine klare Trennung zwischen der „Fernmeldeaufklärung" gemäß BND-G und den „Beschränkungsmaßnahmen nach dem G 10" mit klaren Rechtsgrundlagen für die deutsche Ausland-Ausland-Fernmeldeaufklärung sowohl *vom Ausland* aus als auch *vom Inland* aus:

- Die nachrichtendienstliche Telekommunikationsüberwachung von nach GG grundrechtlich geschützten Personen erfolgt unverändert gemäß §§ 3, 5 und § 8 G 10.[1271]
- Die Fernmeldeaufklärung von Ausländern im Ausland *vom Ausland* aus stützt sich als Rechtsgrundlage auf die Generalklausel § 1 Abs 2 BND-G (weil Ausländer im Ausland nicht von Art 10 GG geschützt werden).
- Die Fernmeldeaufklärung von Telekommunikation von Ausländern im Ausland *vom Inland* aus (z.B. via Datenausleitung beim Netzwerkknoten DE-CIX in Frankfurt) stützt sich auf die Rechtsgrundlage § 6 BND-G (nach *Karl/Soiné* sind Ausländer im Ausland bei Datenerhebung im Inland z.B. bei DE-CIX nicht von Art 10 GG geschützt).[1272]
- Die Auslandsaufklärung mittels Online Durchsuchungen und Quellen-TKÜs („Bundestrojaner") stützt sich nach Angaben der *Deutschen Bundesregierung* direkt auf § 1 Abs 2 BND-G ohne Richtervorbehalt (Anfragebeantwortung vom März 2018).[1273]

Nach Ansicht der *Deutschen Bundesregierung* und *Karl/Soiné* unterfällt die nachrichtendienstliche Erfassung von Telekommunikation sowohl von Ausländern im Ausland *vom*

1269 *Wenzel* in Frankfurter Rundschau (29.05.2018), Der Geheimdienst liest mit, abrufbar unter: http://www.fr.de/kultur/netz-tv-kritik-medien/netz/de-cix-der-geheimdienst-liest-mit-a-1514929 (zuletzt abgerufen am 20.06.2019); *Mascolo/Steinke* in sueddeutsche.de (28.05.2018), Überwachung am De-Cix: Betreiber des weltgrößten Internetknotens wirft BND Rechtsbruch vor, abrufbar unter: https://www.sueddeutsche.de/digital/ueberwachung-am-de-cix-betreiber-des-weltgroessten-internetknotens-wirft-bnd-rechtsbruch-vor-1.3994191 (zuletzt abgerufen am 20.06.2019).

1270 *Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, 1 ff; *Ermert* in heise.de (16.09.2016), NSA-Skandal und BND-Überwachung: Internet-Knoten De-CIX klagt gegen die Bundesrepublik, abrufbar unter: https://www.heise.de/newsticker/meldung/NSA-Skandal-und-BND-Ueberwachung-Internet-Knoten-De-CIX-klagt-gegen-die-Bundesrepublik-3325186.html (zuletzt abgerufen am 20.06.2019); *Kurz* in netzpolitik.org (16.09.2016), Klage gegen den BND wegen Überwachung am Internetknoten DE-CIX, abrufbar unter: https://netzpolitik.org/2016/klage-gegen-den-bnd-wegen-ueberwachung-am-internetknoten-de-cix/ (zuletzt abgerufen am 20.06.2019).

1271 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses; *Karl/Soiné*, NJW 2017, 919.

1272 *Karl/Soiné*, NJW 2017, 919; BT-Drs. 18/9041, 22 f.

1273 BT-Drs. 19/1434, 15 (Antwort auf Frage 45).

Ausland aus (§ 1 Abs 2 BND-G) als auch von Ausländern im Ausland *vom Inland* aus (§ 6 BND-G) nicht per se unter den Schutz des Art 10 Abs 1 GG (vgl. **Kapitel 2.2.1**).[1274] Der Betreiber DE-CIX verlor Ende Mai 2018 einen Prozess beim BVerwG in Leipzig.[1275] Diese Frage ist höchstgerichtlich vom BVerfG in Karlsruhe zu entscheiden.[1276]

Nach Berichten des Wochenmagazins *Spiegels* und *heise.de* wurden von Deutschland auch europäische Tochtergesellschaften deutscher Konzerne nachrichtendienstlich überwacht: *„Nach SPIEGEL-Informationen standen auf Spähllisten des Auslandsgeheimdienstes [BND] Dutzende Firmen in der Europäischen Union, deren Muttergesellschaften in deutscher Hand sind.* (…)*"*[1277] Dabei könnte nach *Spiegel* und *heise.de* im Rahmen der Überwachung der ausländischen Tochtergesellschaften deutscher Konzerne auch nach Art 10 GG verfassungsrechtlich geschützte „deutsche" Kommunikation überwacht worden sein und damit wären ggf. deutsche Bürger (mit-)überwacht worden (vgl. **Kapitel 2.2.1**).[1278]

1274 *Karl/Soiné*, NJW 2017, 919 (920); **aA** *Papier*, NVwZ – Extra 15/2016, 1 ff.

1275 BVerwG Urteil v. 30. Mai 2018, Az. BVerwG 6 A 3.16 = NVwZ 2018, 1476; *Sehl* in lto.de (31.05.2018), Geheimdienst darf weiter Rechenzentren anzapfen, abrufbar unter: https://www.lto.de/recht/hintergruende/h/bverwg-6a316-bnd-internet-knoten-betreiber-ueberwachung-geheimdienst-daten-grundrechte/ (zuletzt abgerufen am 20.06.2019).

1276 *Denkler* in sueddeutsche.de (21.10.2016), Neue BND-Gesetz – Der Fulltake aller Daten wird möglich, abrufbar unter: http://www.sueddeutsche.de/politik/neues-bnd-gesetz-bnd-bekommt-eine-lizenz-zum-datensammeln-1.3212099 (zuletzt abgerufen am 20.06.2019); *bundesregierung.de* (30.12.2016), Klare Regeln für Auslandsaufklärung, abrufbar unter: https://www.bundesregierung.de/Content/DE/Artikel/2016/06/2016-06-28-gesetz-bnd-ausland-ausland-fernmeldeaufklaerung.html (zuletzt abgerufen am 20.06.2019); *Meister* in netzpolitik.org (30.06.2016), Das neue BND-Gesetz: Alles, was der BND macht, wird einfach legalisiert. Und sogar noch ausgeweitet., abrufbar unter: https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/ (zuletzt abgerufen am 20.06.2019); *Krempl* in heise.de (06.06.2016), "BND-Reform": Koalition will das Internet im NSA-Stil überwachen, abrufbar unter: https://www.heise.de/newsticker/meldung/BND-Reform-Koalition-will-das-Internet-im-NSA-Stil-ueberwachen-3228466.html (zuletzt abgerufen am 20.06.2019).

1277 *spiegel.de* (06.07.2018), BND hörte Filialen deutscher Unternehmen in der EU ab, abrufbar unter: http://www.spiegel.de/politik/deutschland/bundesnachrichtendienst-bnd-hoerte-filialen-deutscher-firmen-in-der-eu-ab-a-1217016.html (zuletzt abgerufen am 20.06.2019).

1278 *Holland* in heise.de (07.07.2018), BND spionierte EU-Filialen deutscher Firmen aus, abrufbar unter: https://www.heise.de/newsticker/meldung/BND-spionierte-EU-Filialen-deutscher-Firmen-aus-4104511.html (zuletzt abgerufen am 20.06.2019); *spiegel.de* (06.07.2018), BND hörte Filialen deutscher Unternehmen in der EU ab, abrufbar unter: http://www.spiegel.de/politik/deutschland/bundesnachrichtendienst-bnd-hoerte-filialen-deutscher-firmen-in-der-eu-ab-a-1217016.html (zuletzt abgerufen am 20.06.2019); *Schmid/Sulzbacher* in standard.at (06.07.2018), BND spähte österreichische Firma vor Kauf durch deutsche Rheinmetall aus, abrufbar unter: https://derstandard.at/2000082963575/BND-spaehte-oesterreichische-Firma-vor-deren-Kauf-durch-deutsche-Rheinmetall (zuletzt abgerufen am 20.06.2019).

Beispiel Telekommunikationsüberwachung Österreichs durch Deutschland

Der BND schöpft in Frankfurt am Main beim Netzwerkknoten DE-CIX – nach hM in Übereinstimmung mit Art 10 GG[1279] (aA hierzu *Papier* und *DE-CIX*[1280]) – nach Medienberichten die komplette aus dem A1 Telekom Netz (derzeit größter österreichischer Telekom Provider) angelieferte österreichische (Internet-)Telekommunikation ab. Nach *Moechel* geschieht dabei folgendes: „*Am weltgrößten Internetknoten in Frankfurt laufen die Netze der internationalen Datentransporteure zusammen, einer davon ist die A1-Telekom. Über die DE-CIX werden Internetverkehr, Telefonate und Metadaten zu anderen Carriern weitergeleitet, es handelt sich also in erster Linie um Auslandskommunikation.* (…) *Die Datenströme aus Österreich werden an der wichtigsten Verbindung zum Frankfurter Knoten DE-CIX komplett auf Leitungen des BND kopiert*. (…) *Die gesamte Glasfaserleitung wird über einen sogenannten Splitter auf einen zweiten Faserstrang kopiert. Sehr verkürzt gesagt, werden an ultraschnellen Switches rein transportbezogene, also irrelevante Daten aussortiert, die relevanten Daten werden je nach Protokoll (E-Mail, http, VoIP etc) auf Serverbatterien aufgeteilt und dort gespeichert. Erst dann treten die „Selektoren" der jeweiligen Geheimdienste auf den Plan, das sind Telefonnummern, E-Mail-Adressen, Chat-IDs usw., die den Überwachungszielen zugeordnet werden.* (…) *Ausgewählte Ergebnisse der Auswertung gehen vom BND an das Heeresnachrichtenamt in Wien zurück.* "[1281]

Die im Sommer 2018 über die Tageszeitung *Standard*[1282] und über das Wochenmagazin *Profil*[1283] an die Öffentlichkeit gespielten Selektoren zur deutschen Telekommunikationsüberwachung Österreichs zeigen, dass selbst im äußerst engen Verhältnis zwischen Deutschland und Österreich relativ intensiv überwacht wird. So kundschaftete Deutschland gemäß diesen Medienberichten gezielt tausende Ziele in Österreich u.a. sämtliche österreichische Ministerien inklusive dem Bundeskanzleramt und alle ausländischen Botschaften, die Universität Wien, die TU Wien, die Universität für Veterinärmedizin in Wien, die Donau-Universität Krems und die Universität Graz sowie die Technische Universität Graz, die Wirtschaftskammer Österreich, die Bank Austria, die Raiffeisen Zentral Bank, Magna Europa, die VOEST Alpine Stahl, den Feuerwehr-Spezialfahrzeuge-Hersteller Rosenbauer sowie auch den sozialdemokratischen ex Finanzminister Hannes Androsch, etc. aus.[1284]

1279 BVerwG Urteil v. 30. Mai 2018, Az. BVerwG 6 A 3.16 = NVwZ 2018, 1476; *Sehl* in lto.de (31.05.2018), Geheimdienst darf weiter Rechenzentren anzapfen, abrufbar unter: https://www.lto.de/recht/hintergruende/h/bverwg-6a316-bnd-internet-knoten-betreiber-ueberwachung-geheimdienst-daten-grundrechte/ (zuletzt abgerufen am 20.06.2019).

1280 *Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, 1 ff.

1281 *Moechel* in fm4.orf.at (24.06.2018), Wie der BND die Kommunikation in Österreich überwacht, abrufbar unter: http://fm4.orf.at/stories/2920556/ (zuletzt abgerufen am 20.06.2019).

1282 *Schmid/Sulzbacher* in standard.at (15.06.2018), Die Liste: Wen der deutsche Geheimdienst in Österreich ausspähte, abrufbar unter: https://derstandard.at/2000081647150/Die-Liste-Wen-der-deutsche-Geheimdienst-in-Oesterreich-ausspaehte (zuletzt abgerufe am 20.06.2019).

1283 *Nikbakhsh/Zotter* in profil.at (20.06.2018), BND-Affäre: Die Deutschen spähten Unis aus – und die Firma von Hannes Androsch, abrufbar unter: https://www.profil.at/oesterreich/bnd-affaere-deutschen-unis-firma-hannes-androsch-10148301 (zuletzt abgerufe am 20.06.2019).

1284 *Schmid/Sulzbacher* in standard.at (15.06.2018), Die Liste: Wen der deutsche Geheimdienst in Österreich ausspähte, abrufbar unter: https://derstandard.at/2000081647150/Die-Liste-Wen-der-

Moechel schreibt: *„Wenn es bis 2006 etwa 2.200 Selektoren waren, dann sind es 2018 mindestens zehnmal soviel. Mit den rasanten Zuwächsen in der mobilen Kommunikation und im Datenverkehr insgesamt wächst auch die Zahl der Selektoren.“*[1285]

6.2.6 China

China verfolgt nach *Philip N. Howard* (Oxford University)[1286] eine andere Strategie was die Anstrengungen zur Telekommunikationserfassung betrifft. Während die UKUS Staaten im Rahmen der „Five Eyes“ Allianz weitgehend in der Lage sein sollen, den globalen Internet-Traffic zu überwachen (vgl. **Kapitel 6.2.2**), stelle China im Bereich der IT-Infrastruktur eine sehr große Herausforderung dar, weil China die direkte Kontrolle über seine Technologienutzer habe und chinesische Hardware seit Jahren sehr erfolgreich in westliche Länder exportiert werde, wodurch das unter chinesischen Einfluss stehende Infrastrukturnetzwerk ständig wachse:[1287] Ein chinesischer Technologie-Offizieller formulierte dies nach *Howard* wie folgt: *„Die große Frage ist nicht, ob China eine Gesellschaft von Weltgeltung errichten kann, während es das Internet bekämpft, sondern die Frage ist, ob es diese Gesellschaft errichten kann, während es gleichzeitig ein riesiges chinaspezifisches Intranet errichtet.“*[1288] China baue dabei sein eigenes Netzwerk erfolgreich durch Hardware, Software, Telekommunikationsstandards und Informationspolitik sowie auch Nachrichtenproduktion aus. Dies umfasse direkte Hilfen an befreundete Regierungen in Gestalt von Funksendern und Finanzierungen für nationale Satelliten chinesischer Produktion, Bereitstellung von Content und Technologie für Verbündete und potentiell Verbündete mit Budgetschwierigkeiten sowie Absichtserklärungen. Ein äußerst wichtiges Instrument der chinesischen Netzwerkkontrolle sei dabei die Kontrolle der Partei über die Mittelsmänner, die diese Hardware bauen und Verbindungsdienstleistungen anbieten.[1289] Bspw. der US Kongress warnte schon mehrfach vor der Verwendung chinesischer IT-Produkte und veröffentlichte im Jahr 2012 folgendes Statement: “*Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.”*[1290] Wird

deutsche-Geheimdienst-in-Oesterreich-ausspaehte (zuletzt abgerufe am 20.06.2019); *fsc* in standard.at (20.06.2018), Wie Grazer Professoren und Androsch ins Netz des BND gerieten, abrufbar unter: https://www.derstandard.de/story/2000081932542/wie-zwei-grazer-professoren-und-hannes-androsch-ins-netz-des (zuletzt abgerufe am 20.06.2019).

1285 *Moechel* in fm4.orf.at (24.06.2018), Wie der BND die Kommunikation in Österreich überwacht, abrufbar unter: http://fm4.orf.at/stories/2920556/ (zuletzt abgerufen am 20.06.2019).

1286 Professor Philip N. Howard: https://www.oii.ox.ac.uk/people/philip-howard/ (zuletzt abgerufen am 20.06.2019).

1287 *Howard*, Finale Vernetzung (2016) 34; 210 ff.

1288 *Howard*, Finale Vernetzung (2016) 216.

1289 *Howard*, Finale Vernetzung (2016) 37 f; 89; 214; 216;218.

1290 *U.S. House of Representatives*, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (2012) vi, abrufbar unter: https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf (zuletzt abgerufen am 20.06.2019).

chinesische Hard- und/oder Software verwendet, bestehe das Risiko, dass entsprechende Hintertüren und verborgene Zugriffsmöglichkeiten in der Netzwerk-Technologie verankert wurden. Der US Kongress warnte insofern im Jahr 2012 eindringlich: *„[U]nder Chinese law, ZTE and Huawei would be obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security.“*[1291]

Auch ausländische Konzerne müssen sich den Anforderungen Chinas beugen. Seit 28. Feburar 2018 werden bspw. von Apple Inc. die iCloud Daten von Nutzern in China nicht mehr in den USA gespeichert. Der Betrieb der iCloud und sonstigen Apple Diensten für chinesische Nutzer, die alle jeweils mit der Apple-ID verknüpft sind, wurde durch das chinesische Unternehmen Guizhou-Cloud-Big-Data (GCBD) übernommen. Damit haben chinesische Behörden direkten Zugriff auf die iCloud Daten chinesischer Nutzer, die nun bei GCBD in China und nicht bei bei Apple Inc. gespeichert sind.[1292]

China selbst wehrt sich ebenso massiv gegen westliche Einflüsse, in dem das chinesische Gerätenetzwerk nach außen durch die „Great Firewall of China“ (Projekt Goldener Schild) vollkommen abgegrenzt wird. Innerhalb Chinas wird der gesamte digitale Netzwerkverkehr vollumfänglich überwacht, Schlüsselbegriffe werden herausgefiltert, IP-Adressen werden gesperrt, Suchergebnisse zensiert, Mitteilungen blockiert und Blogger überwacht. Beim Projekt Goldener Schild handelt sich nach *Howard* insofern um eines der größten nationalen Sicherheitsprojekte der Welt.[1293]

1291 *U.S. House of Representatives, Investigative Report* on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (2012) 3, abrufbar unter: https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf (zuletzt abgerufen am 20.06.2019).

1292 *Wurzel* in tagesschau.de (28.02.2018), iCloud zieht nach China, abrufbar: https://www.tagesschau.de/ausland/icloud-china-101.html (zuletzt abgerufen am 20.06.2019); *Nellis/Cadell* in reuters.com (24.02.2018), Apple moves to store iCloud keys in China, raising human rights fears, abrufbar unter: https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060 (zuletzt abgerufen am 20.06.2019).

1293 *Howard*, Finale Vernetzung (2016) 37 f; 89; 214; 216;218

7 Zusammenfassung und Ausblick

7.1 Zusammenfassung

Am Beginn der Arbeit (**Kapitel 2**) werden die im Zusammenhang mit dem Datenschutz relevanten nationalen und europäischen Grundrechte besprochen, die sich aus diesen Grundrechten ergebenden staatlichen Schutzpflichten und abschließend das Verhältnis zwischen den Europäischen Grundrechten der EU-GRC, dem sekundärrechtlichem europäischen Datenschutzrecht und den nationalen Grundrechten dargelegt. Art 7 EU-GRC entspricht dabei weitgehend Art 8 EMRK, beide Bestimmungen schützen „private" Daten. Art 8 EU-GRC korrespondiert weitgehend mit dem deutschen Recht auf informationelle Selbstbestimmung (Art 2 Abs 1 iVm. Art 1 Abs 1 GG) bzw. dem österreichischen Grundrecht auf Datenschutz (§ 1 DSG [2000]). Es zeigt sich jedoch, dass das deutsche Grundrecht auf informationelle Selbstbestimmung (Art 2 Abs 1 iVm. Art 1 Abs 1 GG) und das österreichische Grundrechte auf Datenschutz (§ 1 DSG) hinsichtlich der Erlaubnisnormen für Eingriffe in ihren Schutzbereich dem formellen Gesetzesbegriff folgen, während Art 7 und Art 8 EU-GRC und auch Art 8 EMRK dem materiellen Gesetzesbegriff folgen, womit nach EU-GRC und EMRK auch untergesetzliches Recht (z.B. Durchführungsverordnungen der EU-Kommission ohne Beteiligung des EU-Parlaments) einen Grundrechtseingriff und damit eine Datenverarbeitung legitimieren kann.

Bei der Abgrenzung zwischen DSGVO und ePrivacy-RL 2002/58/EG am IT-gestützten Arbeitsplatz wird klar herausgearbeitet, dass die europarechtlichen Bestimmungen hinsichtlich der Vertraulichkeit der Kommunikation (Art 5 ff ePrivacy-RL) keine Anwendung im Beschäftigtenverhältnis finden können. Dies ergibt sich allerdings nicht eindeutig aus den Begriffsbestimmungen der bis 20. Dezember 2020 gültigen TK-Rahmen-RL 2002/21/EG bzw. der ab 21. Dezember 2020 anwendbaren Richtlinie Kodex für die elektronische Kommunikation (EU) 2018/1972, sondern primär an der mangelnden öffentlichen Zugänglichkeit eines unternehmensinternen elektronischen Kommunikationsdienstes gemäß Art 3 ePrivacy-RL 2002/58/EG. Für die beiden aktuell vorliegenden Entwürfe einer ePrivacy-VO sieht dies wie folgt aus: Im Entwurf der EU-Kommission wären die Art 5 ff ePrivacy-VO bzgl.Vertraulichkeit der Kommunikation nicht auf das Arbeitsverhältnis anwendbar. Der Entwurf des Europäischen Parlaments würde eine Anwendbarkeit der Art 5 ff ePrivacy-VO auch im Arbeitsverhältnis ermöglichen (**Kapitel 3.1 – 3.4)**. Art 8 ePrivacy-VO regelt den Zugriff auf Informationen am Endgerät von Endnutzern und wäre nach dem Entwurf der EU-Kommission nicht im Beschäftigtenverhältnis anwendbar, nach dem Entwurf des EU-Parlaments wäre eine Anwendbarkeit denkbar möglich (**Kapitel 3.3.1**).

Das aktuell gültige nationale deutsche einfachgesetzliche Fernmeldegeheimnis (§ 88 TKG 2004) und die speziellen telekommunikationrechtlichen Datenschutzbestimmungen (§§ 91 ff TKG 2004) sind im Verhältnis Arbeitgeber und Beschäftigter auch bei erlaubter Privatnutzung mangels Vorliegens eines öffentlich zugänglichen elektronischen Kommunikationsdienstes spätestens seit Geltung der DSGVO nicht (mehr) anwendbar (vgl. Art 95 DSGVO iVm. Art 3 ePrivacy-RL 2002/58/EG), sondern werden von der DSGVO

C. Jaksch, *Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes*,
AutoUni – Schriftenreihe 143, https://doi.org/10.1007/978-3-658-29450-2_7

umfassend verdrängt. Vergleichbares gilt für die speziellen datenschutzrechtlichen Bestimmungen auf der Dienstebene (§§ 11 ff TMG). Diese Bestimmungen werden vom Anwendungsvorrang der DSGVO ebenso weitgehend verdrängt. Damit gilt in Deutschland im Beschäftigtendatenschutz auch bei erlaubter Privatnutzung zwischen Arbeitgeber und Beschäftigten alleine die DSGVO und Teil 1 und Teil 2 des nationalen deutschen BDSG (**Kapitel 3.1–3.4**).

Für Österreich ergibt sich dasselbe Ergebnis (**Kapitel 3.1–3.4**), es gilt weiter alleine die DSGVO und das nationale österreichische DSG.

Der Einsatz von neuen Technologien am IT-gestützten Arbeitsplatz ist folglich schwerpunktmäßig anhand der DSGVO und den nationalen Datenschutzgesetzen zu prüfen:

Als Rechtsgrundlagen für den Einsatz eines Digitalen Assistenten, von Big Data Systemen und von Enterprise Search kommen Art 6 Abs 1 lit f DSGVO bzw. § 26 Abs 1 Satz 1 BDSG in Frage, wenn entsprechende effektive technische und organisatorische Maßnahmen zur Risikoeindämmung gesetzt werden (siehe **Kapitel 5**). Jedenfalls ausgenommen – und damit unter strengen Einwilligungsvorbehalt – ist die optional einsetzbare Sprachsteuerung, wo für die Erhebung der Audiodaten (=digitale Sprache) sowohl eine straf- als auch eine ausdrückliche datenschutzrechtliche Einwilligung erforderlich ist. Aus Gründen der Datensicherheit müssen die Sprachbefehle an den Digitalen Assistenten auch zu Zwecken der Spracheridentifikation verarbeitet werden (ErwGr 51 Satz 3 iVm. Art 9 Abs 2 lit a DSGVO). Für die vom Digitalen Assistenten aus den Audiodateien transkribierten digitalen Texte gelten die allgemeinen Erlaubnistatbestände Art 6 Abs 1 lit f DSGVO bzw. § 26 Abs 1 Satz 1 BDSG. Der Digitale Assistent wird so eingerichtet, dass er nicht final für den Nutzer entscheidet, sondern primär Vorschläge erstellt, über welche der menschliche Nutzer dann selbst final entscheiden kann. Damit ergäbe sich auch keine zusätzliche Anwendung des Art 22 DSGVO hinsichtlich automatisierter Einzelentscheidungen.

Die Datenverarbeitung nach Treu und Glauben und Transparenz wird durch ausreichende Informationen sichergestellt, sowie hinsichtlich der Anforderungen an die für die Sprachsteuerung erforderlichen „Lautsprecher" empfiehlt sich eine Orientierung an der Empfehlung der deutschen *BNetzA* hinsichtlich Digitaler Assistenten (siehe **Kapitel 5**).[1294]

Die Zweckbindung wird sichergestellt, dass die für die Datensicherheit (Art 32 DSGVO) erforderlichen personenbezogenen Protokolldaten z.B. bei der Datenspeicherung klar getrennt werden (Nichtverkettbarkeit) von allen übrigen Daten. Erforderliche Nutzerprofile über nur Teilaspekte des beruflichen Wirkens, die für den Betrieb des Digitalen Assistenten erforderlich sind, werden ausschließlich pseudonym erhoben und verschlüsselt gespeichert. Damit wird auch der Grundsatz der Datenminimierung sichergestellt (siehe **Kapitel. 5**). Hinsichtlich einer möglichen Privatnutzung des Endgeräts besteht eine Abschaltpflicht des Digitalen Assistenten durch die Beschäftigten, damit in das Nutzerprofil des Digitalen Assistenten keine privaten Daten einfließen können, sondern ausschließlich dienstlich veranlasste Informationen. Die Datenspeicherung erfolgt nach konkret nach Erforderlichkeitskriterien zu definierenden Fristen.

1294 *BNetzA*, Prüfkritieren digitale Assistenzsysteme – Z21e6216-Grundsatz v. 11.04.2017 , abrufbar unter: https://fragdenstaat.de/anfrage/alexa-siri-co-kunstliche-intelligenz-uberprufungs unterlagen/#nachricht-82803 (zuletzt abgerufen am 15.07.2018).

Die Datensicherheit und IT-Security erfolgt am Stand der Technik, entsprechend den geltenden IT-Standards (ISO/IEC 27001:2013, Critical Security Controls for Effective Cyber Defense" bzw. „IT-Grundschutz).

Der gesamte Betrieb des Digitalen Assistenten wird durch eine ausreichend präzise formulierte Betriebsvereinbarung flankiert, wo exakt die Zwecke, die Datenkategorien und Empfänger benannt werden und so weitgehend wie möglich Transparenz hinsichtlich der Verarbeitungsvorgänge und der angebundenen Dienste geschaffen wird. Adaptierungen, die in der Betriebsvereinbarung erfolgen sollten, sind ein ausdrückliches Verbot der Weiterverarbeitung des Nutzerprofils zu anderen Zwecken als den Betrieb des Digitalen Assistenten durch den Arbeitgeber sowie entsprechende Kontrollrechte des Betriebsrats, dass dieses Verbot vom Arbeitgeber auch eingehalten wird, und ein Beweismittel- und –verwertungsverbot für Datenverarbeitungen und Datenanalysen von Beschäftigtendaten (z.B. „People Analytics") entgegen der BV bzw. ohne freiwillige Einwilligung der betroffenen Beschäftigten.

Folgende Maßnahme sind dabei insb. zu berücksichtigen und ggf. direkt in der BV zu regeln:

Cloud Computing:

- Es wird eine Private Cloud herangezogen, oder im Falle einer Public Cloud primär ein Anbieter, der sich in europäischem Eigentum befindet und ausschließlich innerhalb des europäischen Rechtsraums (EU-GRC, EMRK) die Cloud betreibt und die Daten dort verarbeitet; ggf, Ausnahmen von diesem strengen Grundsatz bei personenbezogenen Daten, die gemäß interner Datenklassifizierung als grundsätzlich wenig risikobehaftet einzustufen sind.
- Die hohen Vertraulichkeitsrisiken iZh mit elektronischer Kommunikation in der heutigen Zeit werden in **Kapitel 6** umfassend herausgearbeitet und man kann ihnen bspw. wie folgt begegnen:
  - Verschlüsselung am Stand der Technik inkl. Schlüssel grundsätzlich beim Cloud Anwender und nicht beim Cloud Anbieter; ggf. Ausnahmen von diesem strengen Grundsatz bei personenbezogenen Daten, die gemäß interner Datenklassifizierung als grundsätzlich wenig risikobehaftet einzustufen sind.
  - ausreichende Verschlüsselung des Datentransports am Stand der Technik vom der Cloud zum Cloud Anwender vor dem Hintergrund der umfassenden staatlichen Telekommunikationsabhörprogramme (**Kapitel 6**).
- Sicherstellung der Transparenz über sämtliche (denkmögliche) Empfänger inklusive gesetzliche Herausgabepflichten an staatliche Stellen von EU-Mitgliedstaaten (Art 28 Abs 3 lit a DSGVO) sowie ausdrückliches Verbot der Herausgabe an Nicht-EU-Staaten ohne existierendes MLAT Abkommen[1295] (Art 48 DSGVO). Die dbzgl. Risiken werden in **Kapitel 6** dargestellt.
- Sicherstellung der Nicht-Verkettbarkeit durch technische und organisatorische Maßnahmen, dass die beim Cloud Anbieter gespeicherten Daten nicht für (rechtswidrige) weitere Zwecke verarbeitet werden können.

1295 Mutual Legal Assistance Treaty.

Digitaler Assistent

- Für die Sprachsteuerung und damit verbundene Erstellung von Audiodateien ist eine straf- (§ 201 dStGB bzw. § 120 öStGB) und ausdrückliche datenschutzrechtliche Einwilligung (Art 9 Abs 2 lit a DSGVO) erforderlich. Als Maßnahme zur Datensicherheit vor unbefugten Datenzugriffen über die Sprachsteuerung des Digitalen Assistenten hat eine Authentifizierung des Sprechers über seine Sprache (Stimmprofil) zu erfolgen. Aus diesem Gründ liegen folglich auch besondere Kategorien personenbezogener Daten (digitale Sprache zur Sprecherauthentifizierung) vor. Der Nutzer hat jederzeit die Möglichkeit die Audiodateien seiner Sprachbefehle zu löschen. Ggf. weiter gespeichert bleiben – bei Erforderlichkeit für die Suchmaschinenverbesserung (Korrelationen Suchanfragen und Suchmaschinenergebnisse) oder bzgl. der elektronischen Kommunikation im Betrieb – die transkribierten Texte der Suchanfragen bzw. über Sprachsteuerung diktierte elektronische Kommunikation. [1296]
- Freiwilligkeit der Einwilligung hinsichtlich der Sprachsteuerung (Audiodateien) besteht, da der Nutzer die Sprachsteuerung des Digitalen Assistenten nicht benutzen muss, sondern auch per Tastatur mit dem Digitalen Assistenten kommunizieren kann ohne tatsächliche Nachteile (ausgenommen die geringere Usability) zu erleiden.
- Profiling (Art 4 Nr 4 DSGVO), welches für den Betrieb des Digitalen Assistenten Voraussetzung ist, erfolgt nicht durch ein umfassendes Profil des Nutzers, sondern es werden im Rahmen des Profilings ausschließlich nur Teilaspekte des beruflichen Wirkens des Betroffenen verarbeitet. Zudem wird das Level der Detailliertheit des Profils an den Erfordernissen für den Betrieb des Digitalen Assistenten orientiert und ist so wenig eingriffsintensiv wie möglich ausgestaltet. Darüberhinaus erfolgt eine Pseudonymisierung, weitere Maßnahmen im Zusammenhang mit Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen werden je Einzelfall umgesetzt und es erfolgt eine ausreichend starke Verschlüsselung der pseudonymen Nutzerprofile in der Cloud.[1297]
- Es werden konkrete Speicherfristen für die unterschiedlichen Metadaten und Inhaltsdaten des Digitalen Assistenten definiert und das von einem Nutzer erstellte Profil wird nach Beendigung des Dienstverhältnisses beim Arbeitgeber gelöscht. Abseits des Betriebs des Digitalen Assistenten und der Sicherstellung der Vertraulichkeit und Integrität (Art 5 Abs 1 lit f DSGVO) lässt sich kein weiteres berechtigtes Interesse an der Verarbeitung des Nutzerprofils identifizieren. Eine Einsicht des Arbeitgeber in das Nutzerprofil (z.B. zur Leistungskontrolle, Charaktereinschätzung und Potentialanalyse im Rahmen von Big Data „People Analytics) lässt sich i.d.R. – abseits einer informierten und ausdrückliche Einwilligung des betroffenen Beschäftigten – datenschutzrechtlich nicht rechtfertigen.

Big Data

- Klare Definition zu welchen Zwecken Big Data im Beschäftigtenverhältnis eingesetzt wird (z.B. ausdrückliches Verbot von „People Analytics“ der Beschäftigten durch Big Data Vorhersagen z.B. über den Karrierelauf oder Charaktereigenschaften, etc.).

1296 *Schnaber/Krieger-Lamina/Peissl*, Studie Arbeiterkammer Wien „Digitale Assistenten“ (2019) 24; 35; ErwGr 51 Satz 3 iVm. Art 9 Abs 1 DSGVO.

1297 *Art 29 Datenschutzgruppe*, WP 251rev.01. (2018) 14; *Kroschwald*, Informationelle Selbstbestimmung in der Cloud (2016) 219 ff.

- Zwecktrennung (Nicht-Verkettbarkeit) durch logische Separierung, durch zweckdienliche Daten, durch Anonymisierung / Aggregierung vor der Verkettung;[1298]
- Lückenlose Dokumentation des Big Data Verfahrens (Transparenz);[1299]
- Sicherstellung der Intervenierbarkeit – Betroffenen muss die Ausübung ihrer Betroffenenrechte wirksam möglich ist. Dies gilt auch bei Pseudonymen;[1300]
- Verwertungsregeln, die diskriminierende Suchkriterien und die Verwertung unzulässiger Auswertungen in rechtlichen Verfahren verbieten;[1301]
- Anwendung von effektiven Pseudonymisierungs-, Anonymisierungs und Verschlüsselungstechniken.[1302]

Enterprise Search:

- Wichtigste Maßnahme ist, dass die Enterprise Search das Rechte und Rollenkonzept jedes angebundenen Datenquellsysteme übernehmen kann und umfassend respektiert, womit Nutzer über die Enterprise Search nur solche Informationen überhaupt suchen dürfen, die sie auch bei einer normalen Suche in Quellsystemen ohne Enterprise Search suchen könnten, denn bereits Suchergebnisse mit Dokumenten mit Hinweis der mangelnden Zugriffsrechte sind bereits zuviel Information für unbefugte Nutzer.
- Eine Enterprise Search Suchmaschine darf nur auf solche Enterprise Social Collaboration Tools zugreifen, bei welchem im Rahmen von Nutzungsbedingungen eindeutig klar gestellt wurde, dass nur eine dienstliche Nutzung im Rahmen von Projektarbeiten erfolgt (Wikis, Enterprise Social Media, Bloqs, etc.). Eine Indexierung der eMail-Postfächer bei erlaubter Privatnutzung ist ausgeschlossen und nicht erlaubt.
- Der Suchindex der Enterprise Search wird durch ausreichende technische und organisatorische Maßnahmen wie Verschlüsselung vor unbefugten Zugriffen geschützt.
- Personenbezogene Protokolldaten der Enterprise Search werden ausschließlich zur Sicherstellung der Datensicherheit (Art 32 DSGVO) erhoben und verarbeitet. Die Datenspeicherung erfolgt datengetrennt (Nichtverkettbarkeit) ausschließlich gemäß Art 32 DSGVO. Protokolldaten zur Suchmaschinenoptimierung werden ausschließlich in anonymisierter Form verarbeitet. Personenbezogene Daten sind hier grundsätzlich nicht erforderlich.

Datentransfers in Drittstaaten:

Nicht durch die DSGVO konnte mA das Problem mit Datenverarbeitungen und Datentransfers in Drittstaaten im Zusammenhang mit den umfangreichen Telekommunikationsabhörprogrammen diverser Staaten bzw. nationalen Zugriffsrechten auf Cloudanbieter inkl. gesetzlicher Herausgabepflicht der Schlüssel gelöst werden. Es bestehen weiter große

1298 *Weichert*, ZD 2013, 251.
1299 *Weichert*, ZD 2013, 251.
1300 *Weichert*, ZD 2013, 251.
1301 *Roßnagel,* ZD 2013, 562; *Europäisches Parlament*, Entschließung des Europäischen Parlaments vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatssphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)) Erwägungen M und N.
1302 *Europäisches Parlament*, Entschließung des Europäischen Parlaments vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatssphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)) Erwägung I und Erwägung 11.

Datenschutzrisiken sowohl für die in der Cloud gespeicherten als auch die am Transportweg in den internationalen Telekommunikationsnetzwerken befindlichen personenbezogenen Daten (vgl. **Kapitel 6**). Abhilfe bieten letztlich nur umfassende technische Datensicherheitsmaßnahmen (starke Verschlüsselung in jeder Phase). Trotz der hohen rechtlichen Anforderungen (Art 44 ff DSGVO) und damit verbundenen zu treffenden juristischen Maßnahmen (z.B. EU-Standardverträge, Binding Corporate Rules, rechtliche Gutachten zu internationalen Datenübermittlungen gemäß Art 49 Abs 1 DSGVO), hatte bereits *Caspar Bowden* (ex-Chief Privacy Adviser von Microsoft) am europäischen Datenschutzrecht kritisiert, dass *„eine unrealistische und legalistische Perspektive eine Vernachlässigung des Schutzes der EU-Bürger ermöglicht.“*[1303] Auch *Spies* stellt zu dieser Thematik fest: „*Das Risiko eines Datenzugriffs durch Nicht-EU-Staaten kann auch vertraglich nur sehr begrenzt eingeschränkt werden.*“[1304] Demgemäß lassen sich mit kosten- und bürokratischen Aufwand Datentransfers in unsichere Drittstaaten rechtskonform legitimieren (Compliance). Durch diese juristischen Maßnahmen kann jedoch mA nicht zugleich der politisch erhoffte Mehrwert an tatsächlichem Schutz für EU-Bürger vor Zugriffen in Drittstaaten erreicht werden (vgl. **Kapitel 6**). Die EU strebt politisch ein hohes Datenschutzniveau an, kann aber in einer globalisierten Welt vor dem Hintergrund stark divergierender Grundrechtspositionen für Unternehmen den Datenschutz bei internationalen Datentransfers mit den damit verbundenen erheblichen wirtschaftlichen Konsequenzen nicht absolut durchsetzen (vgl. Art 1 Abs 1 DSGVO), sondern nur in Abwägung mit den in diesem Bereich divergierenden Grundrechtspositionen (vgl. **Kapitel 1.1.5.**). Dabei müssen insb. Art 7 EU-GRC (Privatleben, Kommunikation) und Art 8 EU-GRC (Datenschutz) mit Art 16 EU-GRC (Unternehmerische Freiheit) und Art 17 EU-GRC (Eigentum) in einem angemessenen Interessensausgleich gebracht werden.

7.2 Ausblick

Die vorläufigen Antworten der Arbeit auf die gestellten rechtswissenschaftlichen Forschungsfragen sind eingebettet in die gesellschaftlichen Zukunftsszenarien einer weiteren Digitalisierung der Welt mit dem damit einhergehenden zunehmenden Einsatz von KI und Robotisierung (Industrie 4.0. sowie Arbeit 4.0).

Daten(schutz)rechtliche Fragen in der allgemeinen Conditio Humana mit ihren politischen Systemen werden in Zukunft eine noch verstärktere Rolle spielen als bisher. In einem viel größeren Kontext geht es dabei auch um Fragen zur Demokratie und wie sie in Zukunft gelebt werden wird. Autoren aus der Gesellschaftspolitik und Soziologie befassen sich seit einigen Jahren mit den zu erwartenden erheblichen Auswirkungen dieser neuen Tendenzen, die unser aller Leben verändern werden, mit allen Chancen und Risiken dabei, insbesondere aber auch mit den großen Fragen zur persönlichen Freiheit und Autonomie.

1303 *Bowden* in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013) 35.

1304 *Spies* in von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019) Teil 7 Rn 11 – Rn 12.

Fragen der Programmierung von "Umgebungsintelligenz" beispielsweise in selbstfahrenden Fahrzeugen unter Berücksichtigung von Grundwerten und Normen, oder die grundsätzliche Frage, in welchen Lebensbereichen und Situationen allein Programmcodes entscheiden sollen und wie hoch dabei der "Preis für Unfreiheit" ist, sind gesellschaftlich zu diskutieren. Es besteht nämlich die Gefahr, dass die Gesellschaft erneut wieder politisch primär nach Effizienz-Kriterien in Richtung einer neuen technisch gesteuerten Perfektion gestaltet wird (vgl. Geschichte des Datenschutzes in **Kapitel 1**) und die Fähigkeit nach moralischem Handeln wieder zurückgedrängt wird. Die Frage dabei ist – ist "smart" wirklich smart?

Die Rechstwissenschaft hat sich diesen neuen Gesellschaftsszenarien zu stellen und über diese Arbeit hinausgehenden Forschungsprojekte zu entwickeln v.a. rund um den persönlichen Grundrechtsschutz und der Demokratie angesichts der weiteren Digitalisierung und den damit verbundenen Herausforderungen.[1305]

1305 *Morozov*, Smarte Neue Welt. Digitale Technik und die Freiheit des Menschen (2013) 16 ff; *Hofstetter,* Das Ende der Demokratie. Wie die künstliche Intelligenz die Politik übernimmt und uns entmündigt (2018) 431.

Literaturverzeichnis

Juristische Kommentare

Arndt/Fetzer/Scherer/Graulich (Hrsg), TKG[2] (2015)
Bäumlin/Azzola (Hrsg), AK-GG (1984) Band I
Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl (Hrsg), DSG (2018)
Büchner/Ehmer/Geppert et al (Hrsg), TKG[2] (2000)
Burgstaller/Minichmayr, E-Commerce-Recht[2] (2011)
Calliess/Ruffert (Hrsg), EUV/AEUV[5] (2016)
Dammann/Simitis, EG-Datenschutzrichtlinie (1997)
Dohr/Pollirer/Weiß, DSG – Datenschutzgesetz (1988)
Ehmann/Helfrich, EG Datenschutzrichtlinie Kurzkommentar (1999)
Epping/Hillgruber (Hrsg), BeckOK Grundgesetz [41. Edition] (Stand: 15.11.2018)
Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer BDSG [aF][4] (2014)
Eßer/Kramer/v. Lewinski (Hrsg), Auernhammer DSGVO BDSG[6] (2018)
Fabrizy, StGB[13] (2018)
Feiel/Lehofer, Telekommunikationsgesetz 2003 Praxiskommentar (2004)
Feiler/Forgó, EU-DSGVO (2017)
Fischer (Hrsg), Strafgesetzbuch mit Nebengesetzen[66] (2019)
Geppert/Schütz (Hrsg), Beck'scher TKG-Kommentar[4] (2013)
Gersdorf/Paal (Hrsg), BeckOK Informations- und Medienrecht[24.Edition] (Stand: 01.05.2019)
Gola (Hrsg), DS-GVO[2] (2018)
Gola/Heckmann (Hrsg), BDSG[13] (2019)
Gola/Schomerus, BDSG [aF][12] (2015)
Graf (Hrsg), BeckOK StPO mit RiStBV und MiStra[33. Edition] (Stand: 01.04.2019)
Hoeren/Sieber/Holznagel (Hrsg), Multimedia-Recht[48. EL] (Februar 2019)
Höpfel/Ratz (Hrsg), WK StGB[2] (Stand: Stand 17.10.2017)
Jarass (Hrsg), Charta der Grundrechte der EU[3] (2016)
Kilian/Heusen (Hrsg), Computerrecht[34. Ergänzungslieferung] (2018)
Kindhäuser/Neumann/Paeffgen (Hrsg), Strafgesetzbuch[5] (2017)
Knyrim (Hrsg), DatKomm (Stand 01.10.2018, rdb.at)
Köhler/Bornkamm (Hrsg), UWG[37] (2019)
Kühling/Buchner (Hrsg), DS-GVO BDSG[2] (2018)
Leukauf/Steininger (Hrsg), Kommentar zum Strafgesetzbuch[4] (2017)
Maunz/Dürig (Hrsg), Grundgesetz-Kommentar[86. EL] (Januar 2019)
Meyer-Ladewig/Nettesheim/von Raumer (Hrsg), Europäische Menschenrechtskonvention[4] (2017)
Neumayr/Reissner (Hrsg), ZellKomm[3] (Stand 1.1.2018, rdb.at)
Paal/Pauly (Hrsg), DS-GVO BDSG[2] (2018)

C. Jaksch, *Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes*,
AutoUni – Schriftenreihe 143, https://doi.org/10.1007/978-3-658-29450-2

Palandt (Hrsg), Bürgerliches Gesetzbuch[78] (2019)

Pollirer/Weiss/Knyrim, DSG[2] (Stand 26.11.2015, rdb.at)

Ricardi (Hrsg), Betriebsverfassungsgesetz[16] (2018)

Riesz/Schilchegger (Hrsg), TKG (2016)

Rolfs/Giesen/Kreikebohm/Udsching (Hrsg), BeckOK Arbeitsrecht[51 Edition] (Stand 01.03.2019)

Rummel/Lukas (Hrsg), ABGB[4] (Stand: 1.5.2018, rdb.at)

Scheurle/Mayen (Hrsg), Telekommunikationsgesetz[3] (2018)

Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg), Datenschutz-Grundverordnung mit Bundesdatenschutzgesetz (2018)

Schwimann/Neumayr (Hrsg), ABGB-TaKomm[4] (2017)

Simitis/Hornung/Spiecker gen. Döhmann (Hrsg), Datenschutzrecht (2019)

Spindler/Schmitz (Hrsg), TMG[2] (2018)

Spindler/Schmitz/Gleis (Hrsg), TDG (2004)

Spindler/Schuster (Hrsg), Recht der elektronischen Medien[3] (2015)

Strasser/Jabornegg/Resch, ArbVG (Stand: 1.4.2019, rdb.at)

Stratil (Hrsg), TKG 2003[4] (2013)

Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch[22 Lfg] (Stand Mai 2010)

v. Heintschel-Heinegg (Hrsg), BeckOK StGB[42. Edition] (Stand 01.05.2019)

Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] (Stand: 01.05.2019)

Wolff/Brink (Hrsg), BeckOK Datenschutzrecht[28. Edition] [aF] (Stand: 01.05.2018)

Zankl, E-Commerce-Gesetz[2] (2016)

Juristische Fachbücher

Balaha/Marka/Zellhofer/Liebel, Rechtsfragen des Cloud Computing (2011)

Barnitzke, Rechtliche Rahmenbedingungen des Cloud Computing (2014)

Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009)

Brodil/Risak, Arbeitsrecht in Grundzügen[10] (2019)

Bull, Datenschutz oder Die Angst vor dem Computer (1984)

Chadoian, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung (2015)

Däubler, Gläserne Belegschaften[8] (2019)

Drackert, Die Risiken der Verarbeitung personenbezogener Daten (2014)

Dütz/Thüsing, Arbeitsrecht[23] (2018)

Elixmann, Datenschutz und Suchmaschinen (2012)

Ennöckl, Der Schutz der Privatssphäre in der elektronischen Datenverarbeitung (2014)

Feiler/Horn, Umsetzung der DSGVO in der Praxis (2018)

Forgó/Helfrich/Schneider (Hrsg), Betrieblicher Datenschutz[3] (2019)

Gola, Datenschutz am Arbeitsplatz[5] (2014)

Greve, Datenschutz in der Unternehmenskommunikation. Eine technologiebasierte rechtliche Zuordnung (2006)

Gridl, Datenschutz in globalen Telekommunikationssystemen (1999)

Grünanger/Goricnik (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018)

Henke, Die Datenschutzkonvention des Europarates (1986)

Herrmann, Das Recht der Suchmaschinen – Ausgewählte Rechtsprobleme der Suchmaschine Google (2010), Dissertation Universität Wien, Betreuer ao. Univ.-Prof. Dr. Wolfgang Zankl

Jabornegg/Resch/Födermayr, Arbeitsrecht[6] (2017)

Jahnel, Handbuch Datenschutzrecht (2010)

Jandt/Steidle (Hrsg), Datenschutz im Internet (2018)

Jotzo, Der Schutz personenbezogener Daten in der Cloud (2013)

Knyrim, Datenschutzrecht[3] (2015)

Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018)

Kramer (Hrsg), IT-Arbeitsrecht (2017)

Kroschwald, Informationelle Selbstbestimmung in der Cloud (2016)

Kühling/Martini et al., Die DSGVO und das nationale Recht (2016)

Kustor, Unternehmensinterne Untersuchungen (2010)

Lachenmann, Datenübermittlung im Konzern (2016)

Lange, Datenflut – Fluch oder Segen. Wie Sie mit Enterprise Search einfach und sicher Informationen finden (2009)

Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis[2] (2019)

Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016)

Mallmann, Datenschutz in Verwaltungs-Informationssystemen: Zur Verhältnismäßigkeit des Austausches von Individualinformationen in der normvollziehenden Verwaltung (1976)

Mayer/Kucsko-Stadlmayer/Stöger, Bundesverfassungsrecht[11] (2015)

Merten/Papier/Kucsko-Stadlmayer (Hrsg), Handbuch der Grundrechte Band VII/1 Grundrechte in Österreich[2] (2014)

Müller/Schlothauer/Schütrumpf (Hrsg), MAH Strafverteidigung (2014)

Paefgen, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2017)

Rebhahn, Mitarbeiterkontrollen am Arbeitsplatz (2009)

Roßnagel (Hrsg), Das neue Datenschutzrecht (2018)

Roßnagel (Hrsg), Europäische Datenschutz-Grundverordnung (2016)

Roßnagel/Banzhaf/Grimm (Hrsg), Datenschutz im Electronic Commerce (2003)

Schantz/Wolff (Hrsg), Das neue Datenschutzrecht (2017)

Schmidt, Datenschutz für „Beschäftigte“ (2016)

Schwichtenberg, Datenschutz in drei Stufen (2018)

Siemen, Datenschutz als Europäisches Grundrecht (2006)

Sievers, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes (2002)

Steidle, Multimedia-Assistenten im Betrieb (2005)

Thüsing (Hrsg), Beschäftigtendatenschutz und Compliance[2] (2014)

Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht (2018)

Tsolkas/Wimmer, Wirtschaftsspionage und Intelligence Gathering (2012)

von dem Busche/Voigt (Hrsg), Konzerndatenschutz (2014)

von dem Busche/Voigt (Hrsg), Konzerndatenschutz[2] (2019)

Weth/Herberger/Wächter (Hrsg), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014)

Widmaier/Müller/Schlothauer (Hrsg), Münchner Anwaltshandbuch Strafverteidigung[2] (2014)

Wiederin, Privatssphäre und Überwachungsstaat (2003)

Wischmeyer, Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeit in den USA (2017)

Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009)

Zöllner/Loritz/Hergenröder, Arbeitsrecht[7] (2015)

Juristische Aufsätze und Beiträge

Barnitzke, Microsoft: Zugriff auf personenbezogene Daten in EU-Cloud auf Grund US Patriot Act möglich, MMR-Aktuell 2011, 321103

Bergauer, Zur Rechtmäßigkeit der (Weiter)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 6/2018, 231

Böhm/Wybitul, Arbeitnehmerdaten in der Cloud, ArbRAktuell 2015, 539

Börding, Ein neues Datenschutzschild für Europa, CR 7/2016, 431

Breyer, Verarbeitungsgrundsätze und Rechenschaftspflicht nach Art. 5 DS-GVO, DuD 5/2018, 311

Brodil, Datenschutz und Arbeitsrecht – Es bleibt alles anders, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 1

Brodil, Datenschutz und Arbeitsrecht – Was ändert sich durch die Datenschutz-Grundverordnung? DRdA 2018, 463

Brodil, Arbeitnehmerdatenschutz und Datenschutz-Grundverordnung (DSGVO), ecolex 2018, 486

Brodil, Eine nicht dem AN offengelegte Kommunikationsüberwachung am Arbeitsplatz verletzt das in Art 8 EMRK geschützte Recht auf Privatleben, ZAS 2018/33, 203

Brodil, Sensible Daten im Arbeitsverhältnis – Nochmals zur Erfassung von § 9 Z 11 DSG 2000, in Kietaibl/Schörghofer/Schrammel (Hrsg), Rechtswissenschaft und Rechtskunde – Liber Amicorum für Robert Rebhahn (2014) 1

Brodil, Individualarbeitsrechtliche Fragen der Kontrolle des Arbeitnehmers, in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 69

Brodil, Die Registrierung von Vermittlungsdaten im Arbeitsverhältnis, ZAS 2004/01, 17

Buchner, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 3/2016, 155

Burkert, Die Konvention des Europarates zum Datenschutz, CR 9/1988, 751

Busch/Falb, Erhebung und Verarbeitung von Arbeitnehmerdaten in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 48

Eickelpasch, Anpassung des deutschen Datenschutzrechts an die DSGVO, Sonderveröffentlichung zu RDV 06/2017, 5

Feiler/Fina, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303

Felten/Mosler, IKT am Arbeitsplatz: Nutzung und Kontrolle in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 481

Forgó/Hänold/Schütze, The Principle of Purpose Limitation and Big Data in Corrales (Hrsg), New Technology, Big Data and the Law (2017)

Forgó/Krügel, Die Subjektivierung der Zweckbindung, DuD 12/2005, 732

Forgó/Otto, Datenschutzrechtliche Neuerungen im TK-Recht, ecolex 2011,177

Fritsch/Haslinger, Checkliste Betriebsvereinbarung – das Prüfschema, in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 158

Gausling, Offenlegung von Daten auf Basis des CLOUD Act, MMR 2018, 578

Gerhartl, Datenschutz im Arbeitsrecht – Betrachtungen im Kontext der neuen Rechtslage, ASok 2018, 223

Gerhartl, Datenverarbeitung im Arbeitsverhältnis, ecolex 2018, 496

Gola/Jaspers, Zweckänderungen bei der Weiterverarbeitung von Beschäftigtendaten, RDV 3/2018, 145

Goricnik, Adaption und Neu-Abschluss von Betriebsvereinbarungen zum Datenschutz im Lichte der DS-GVO, in Haslinger/Krisch/Riesenecker-Caba (Hrsg), Beschäftigtendatenschutz (2017) 146

Goricnik, Kollektivvereinbarungen als Erlaubnistatbestände für Datenverarbeitungen im Beschäftigungskontext, DRdA 2018, 10

Goricnik, Kontrolle Internet/E-Mail am Arbeitsplatz, Dako 2016/1, 7

Grünanger, Auswirkungen der DSGVO auf den Arbeitnehmer-Datenschutz in Österreich, ZAS 2017/55, 284

Härting, Zweckbindung und Zweckänderung im Datenschutzrecht, NJW 2015, 3284

Hattenberger, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in Resch (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien (2005) 13

Helbing, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 3/2015, 145

Herrmann/Soiné, Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, NJW 2011, 2922

Hessel, „My friend Cayla" – eine nach § 90 TKG verbotene Sendeanlage, abrufbar unter: http://www.jurpc.de/jurpc/show?id=20170013 (zuletzt abgerufen am 20.06.2019)

Hoeren, Big Data und Datenqualität – ein Blick auf die DS-GVO, ZD 2016, 459

Hofmann, Anforderungen aus DS-GVO und NIS-RL an das Cloud Computing, ZD-Aktuell 2017, 05488

Jaburek/Blaha, Die technische Umsetzung der eMail in IT-LAW.AT (Hrsg), e-Mail – elektronische Post im Recht (2003) 1

Kamarinou/Millard/Singh, Machine Learning with Personal Data (2016). Queen Mary School of Law Legal Studies Research Paper No. 247/2016, abrufbar unter: https://ssrn.com/abstract=2865811 (zuletzt abgerufen am 20.06.2019)

Karl/Soiné, Neue Rechtsgrundlagen für die Ausland-Ausland-Fernmeldeaufklärung, NJW 2017, 919

Kastelitz, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogender Daten in Knyrim (Hrsg), Datenschutz-Grundverordnung (2016)

Keppeler, Was bleibt vom TMG-Datenschutz nach der DS-GVO? MMR 2015, 779

Klein, Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633

Knyrim, Suchmaschinen andersrum: Datenschutzrechtliche Implikationen von Suchmaschinen und Web-Analyse-Tools in Österreichische Juristenkommission (Hrsg), Alles unter Kontrolle? (2009) 115

Körber, TKG-Novelle 2011, MMR 2011, 215

Körber-Risak, DSGVO und Betriebsverfassungsrecht, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 55

Kotschy, Datenschutz in systematischer Einordnung zum Arbeitsrecht in Brodil (Hrsg), Datenschutz im Arbeitsrecht Mitarbeiterüberwachung versus Qualitätskontrolle. Wiener Oktobergespräche 2009 (2010) 1

Kotschy, Zweckbindungsprinzip und zulässige Weiterverarbeitung – Debattenbeitrag zur Datenschutz-Grundverordnung (2016), abrufbar unter: https://bim.lbg.ac.at/sites/files/bim/kotschy_zweckbindungsprinzip_-endfassung.pdf (zuletzt abgerufen am 20.06.2019)

Kotschy/Reimer, Die Überwachung der Internet-Kommunikation am Arbeitsplatz, ZAS 2004, 29.

Kroschwald, Kollektive Verantwortung für den Datenschutz in der Cloud, ZD 2013, 388

Lejeune, Datenschutz in den Vereinigten Staaten von Amerika, CR 11/2013, 755

Lutterbeck, 20 Jahre Dauerkonflikt: Die Novellierung des Bundesdatenschutzgesetzes*,* in Sokol (Hrsg), 20 Jahre Datenschutz – Individualismus oder Gemeinschaftssinn? (1998) 7

Martini/Wagner/Wenzel, „Rechtliche Zulässigkeit einer Personenkennziffer", ZD-Aktuell 2017, 04272

Mense, EU-US-Privacy-Shield – der kleinste gemeinsame Nenner angemessenen Datenschutzes? ZD 2019, 351

Monreal, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO, ZD 2016, 507

Müller-Peltzer/Franck, Gruß Bot! Aktuelle Rechtsfragen zum Einsatz von Chatbots, in Taeger (Hrsg), Recht 4.0 (2017) 241

Nebel/Richter, Datenschutz bei Internetdiensten nach der DS-GVO – Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD 2012, 407

Oberhofer, Datenschutz und Arbeitsrecht in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 457

Oberwetter, Arbeitnehmerrechte bei Lidl, Aldi & Co, NZA 2008, 609

Ohrtmann/Schwiering, Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 2984

Papier, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, 1

Prankl, Umgang mit Arbeitnehmerdaten bei Beendigung des Arbeitsverhältnisses, in Körber-Risak/Brodil (Hrsg), Datenschutz und Arbeitsrecht (2018) 77

Raffler/Hellich, Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer e-mails zulässig? NZA 1997, 862

Schaar, „Steuer-ID darf kein allgemeines Personenkennzeichen werden!", ZD 2011, 49

Schleipfer, Das 3-Schichten-Modell des Multimediadatenschutzrechts, DuD 2004, 727

Schleipfer, Datenschutzkonformer Umgang mit Nutzungsprofilen – Sind IP-Adressen, Cookies und Fingerprints die entscheidenden Details beim Webtracking? ZD 2015, 399

Schleipfer, Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 2017, 460

Schleipfer, Nutzungsprofile unter Pseudonym – Die datenschutzrechtlichen Bestimmungen und ihre Anwendung im Internet, RDV 4/2008, 143

Schmidt, Der Nebel lichtet sich: Das BAG systematisiert die Erlaubnistatbestände des Beschäftigten datenschutzrechts, RDV 2017/6, 284

Schnaber/Krieger-Lamina/Peissl, Studie Arbeiterkammer Wien „Digitale Assistenten" (2019) 29 ff, abrufbar unter: https://www.arbeiterkammer.at/beratung/konsument/Datenschutz/Studie_Alexa_Sprachassistenten_2019.pdf (zueletzt abgerufen am 06.07.2019)

Specht-Riemenschneider/Schneider, Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, 503

Schultze-Melling, Datenschutz jenseits und diesseits des Atlantiks – Ein Nachruf zum Tod von Alan F. Westin und Wilhelm Steinmüller, ZD 2013, 145

Schwenke, § 90 TKG – Anwendbarkeit des Verbotes von "Minispionen" im Zeitalter smarter Geräte, K&R 5/2017, 297

Soiné, Die strafprozessuale Online-Durchsuchung, NStZ 2018, 497

Sonntag, Informationstechnologie: Grundlagen, in Jahnel/Mader/Staudegger (Hrsg) IT-Recht[3] (2012) 1

Stadler, Das österreichische Datenschutzgesetz als Markstein der Verfassungspolitik und des Informationsrechts, JBl 1979, 358

Steinmüller, Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann, RDV 2007/4, 158

Steinmüller/Podlech, Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann, FIfF-Kommunikation 03/2007, 15, abrufbar unter: https://www.fiff.de/publikationen/fiff-kommunikation/fk-2007/fk-3-2007/03_2007_steinmueller.pdf (zuletzt abgerufen am 20.06.2019)

Stiemerling, "Künstliche Intelligenz" – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge, CR 12/2015, 762

Taeger, Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017/1, 3

Thiele, Rechtssicherer Umgang mit elektronischen Accounts ausgeschiedener Mitarbeiter, jusIT 2014, 1

Thiele, U.S. CLOUD Act – Danaergeschenk für den Europäischen Datenschutz, ZIIR 2/2018, 128

Vogelgesang/Hessel, Spionagegeräte im Kinderzimmer? ZD 2017, 269

von Grafenstein, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit, DuD 12/2015, 789

von Lewinski, Geschichte des Datenschutzrechts von 1600 bis 1977 in Arndt/Betz et al (Hrsg), Freiheit – Sicherheit – Öffentlichkeit: 28. Assistententagung Öffentliches Recht, Heidelberg 2008 (2009) 196

von Lewinski, Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive, in Schmidt/Weichert (Hrsg), Datenschutz – Grundlagen, Entwicklungen und Kontroversen (2012) 23

Weichert, Big Data und Datenschutz – Chancen und Risiken einer neuen Form der Datenanalyse, ZD 2013, 251

Weichert, Cloud Computing und Datenschutz, DuD 2010, 679

Weichert, Datenschutz bei Suchmaschinen, in D. Lewandowski (Hrsg) Handbuch Internetsuchmaschinen (2009) 285

Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491

Materialien Europäische Kommission

European Commission, BRIEF OF THE EUROPEAN COMMISSION ON BEHALF OF THE EUROPEAN UNION AS AMICUS CURIAE IN SUPPORT OF NEITHER PARTY (2018) 14 f, abrufbar unter: https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html (zuletzt abgerufen am 20.06.2019)

European Commission, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Final Report (2015)

COCOM11-20, 04th October 2011, Questionnaire on the implementation of the Article 5(3) of the ePrivacy Directive

COM(2019) 495 final.

COM(2017) 10 final.

COM(2016) 590 final.

KOM(2012) 10 endg.

KOM(2012) 9 endg.

KOM(2010) 609 endg.

KOM(95) 375 endg.

KOM(92) 422 endg. (abgedruckt in BT-Drs. 12/8329)

KOM(90) 314 endg.

KOM(87) 290 endg.

Materialien Europäisches Parlament

Bowden in Generaldirektion Interne Politikbereiche Fachabteilung C Bürgerrechte und Konstitutionelle Angelegenheiten (Hrsg), Das Überwachungsprogramm der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger – Themenpapier (2013), abrufbar unter: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_DE.pdf (zuletzt abgerufen am 20.06.2019)

Europäisches Parlament, Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE(zuletzt abgerufen am 20.06.2019)

Europäisches Parlament, Entschließung vom 05. September 2001 zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52001IP0264(01)&qid=1561982366845&from=DE (zuletzt abgerufen am 20.06.2019)

Europäisches Parlament, Bericht vom 21. Februar 2014 über das Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres (2013/2188(INI)), abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//DE (zuletzt abgerufen am 20.06.2019)

Europäisches Parlament, Entschließung vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres (2013/2188(INI)), abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//DE (zuletzt abgerufen am 20.06.2019)

Europäisches Parlament, Entschließung vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatssphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung (2016/2225(INI)), abrufbar unter: http://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_DE.pdf (zuletzt abgerufen am 20.06.2019)

Europäisches Parlament, Bericht vom 27. Oktober 2017 über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017) 0010 – C8-0009/2017 – 2017/0003(COD)), abrufbar unter: http://www.europarl.europa.eu/doceo/document/A-8-2017-0324_DE.html (zuletzt abgerufen am 20.06.2019)

Europäisches Parlament, Entschließung vom 26. Juni 2018 zur Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (2018/2645(RSP)), abrufbar unter: http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_DE.html (zuletzt abgerufen am 20.06.2019)

Materialien Europäischer Rat

Europäischer Rat, Interinstitutional File:2017/0003(COD) vom 22. Februar 2019, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6771_2019_INIT&from=EN (zuletzt abgerufen am 20.06.2019)

Materialien Europarat

Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), abrufbar unter: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e (zuletzt abgerufen am 02.07.2019)

Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, abrufbar unter: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (zuletzt abgerufen am 20.06.2019)

Council of Europe, Chart of signatures and ratifications of Treaty, abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (zuletzt abgerufen am 02.07.2019)

Stellungnahmen Art. 29 Datenschutzgruppe / Europäischer Datenschutzausschuss

Art 29 Datenschutzgruppe, WP 261 (2018), Guidelines on Article 49 of Regulation 2016/679, abrufbar unter: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49771 (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 251rev.01 (2018), Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, abrufbar unter: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54169 (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 249 (2017), Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz, abrufbar unter: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54650 (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 247 (2017), Stellungnahme 01/2017 zum Vorschlag für eine Verordnung über die Privatsphäre, abrufbar unter: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49780 (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 243 rev.01 (2017), Leitlinien in Bezug auf Datenschutzbeauftragte, abrufbar unter: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48137 (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 228 (2014), Arbeitsdokument „Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken“, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 225 (2014), LEITLINIEN FÜR DIE UMSETZUNG DES URTEILS DES GERICHTSHOFS DER EUROPÄISCHEN UNION IN DER RECHTSSACHE C-131/12 „GOOGLE SPANIEN UND INC / AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) UND MARIO COSTEJA GONZÁLEZ“, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 224 (2014), Stellungnahme 9/2014 zur Anwendung der Richtlinie 2002/58/EG auf die Nutzung des virtuellen Fingerabdrucks, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 223 (2014), Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe WP 221 (2014), Erklärung der nach Artikel 29 eingesetzten Datenschutzgruppe über die Auswirkungen der Entwicklung von Big-Data-Technologien auf den Schutz natürlicher Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten in der EU, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 217 (2014), Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 203 (2013), Opinion 03/2013 on purpose limitation, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 202 (2013), Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 196 (2012), Stellungnahme 05/2012 zum Cloud Computing, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 171 (2010), Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 169 (2010), Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 158 (2009), Arbeitsunterlage 1/2009 über Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung bei grenzübergreifenden zivilrechtlichen Verfahren (pre-trial discovery), abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 148 (2008), Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 126 (2006), Stellungnahme 8/2006 zur Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp126_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 118 (2006), Stellungnahme 2/2006 der Artikel 29-Datenschutzgruppe zu Datenschutzfragen bei Filterdiensten für elektronische Post, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp118_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 55 (2002), Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 48 (2001), STELLUNGNAHME DER ARTIKEL 29 DATENSCHUTZGRUPPE ZUR VERARBEITUNG PERSONENBEZOGENER DATEN VON BESCHÄFTIGTEN, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48sum_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe WP 42 (2001), Empfehlung 1/2001 Beurteilungsdaten von Beschäftigten, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp42_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 37 (2000), Arbeitsdokument Privatsphäre im Internet, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_de.pdf (zuletzt abgerufen am 20.06.2019)

Art 29 Datenschutzgruppe, WP 36 (2000), Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000 KOM(2000)385, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp36_de.pdf (zuletzt abgerufen am 20.06.2019)

Europäischer Datenschutzausschuss, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 (2018), abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf (zuletzt abgerufen am 20.06.2019)

Stellungnahmen Datenschutzbehörden und Regulierungsbehörden

BNetzA, Prüfkritieren digitale Assistenzsysteme – Z21e6216-Grundsatz v. 11.04.2017, abrufbar unter: https://fragdenstaat.de/anfrage/alexa-siri-co-kunstliche-intelligenz-uberprufungsunterlagen/#nachricht-82803 (zuletzt abgerufen am 20.06.2019)

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Sprachassistenten (2017)

Datenschutzkonferenz, Kurzpapier Nr. 14 Beschäftigtendatenschutz (2018)

Datenschutzkonferenz, Kurzpapier Nr. 4 – Datenübermittlung in Drittländer (2017)

Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines – Firmeninterne Warnsysteme und Beschäftigtendatenschutz (2018)

Datenschutzkonferenz, Positionsbestimmung vom 26. April 2018 zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018

Düsseldorfer Kreis, Orientierungshilfe Cloud Computing (2014)

Düsseldorfer Kreis, Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen (2013)

Düsseldorfer Kreis, Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“ (2005)

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (2016)

Materialien Gesetzgebung Deutschland

BT-Drs. 19/11181

BT-Drs. 19/4674

BT-Drs. 19/2653

BT-Drs. 19/1434

BT-Drs. 18/13013

BT-Drs. 18/12356

BT-Drs 18/11655

BT-Drs 18/11325

BT-Drs. 18/9142

BT-Drs. 18/9041

BT-Drs 18/8317

BT-Drs. 17/8814

BT-Drs. 17/8454

BT-Drs 17/5707

BT-Drs 16/13657

BT-Drs. 16/3656

BT-Drs. 16/3078

BT-Drs 15/2316

BT-Drs. 14/6098

BT-Drs 14/4329

BT-Drs. 13/10667

BT-Drs 13/8016

BT-Drs. 13/7218

BT-Drs. 13/3609

BT-Drs. 12/8329 (abgedruckt KOM(92) 422 endg.)

BT-Drs. 7/1059

BT-Drs. 8/3825

BT-Drs. VI/3826

BT-Drs. VI/2654

BT-Plenarprotokoll 17/198, S. 23862C – 23862D.

Bundesministeriums des Innern, für Bau und Heimat, Referentenentwurf vom 21.06.2018, Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU

Bundesministeriums des Innern, Referentenentwurf des Bundesministeriums des Innern Stand: 2. Ressortabstimmung (11.11.2016 16:13), Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU

Hessischer Landtag 6. Wahlperiode Drucksache Nr. 3065

Hessischer Landtag 7. Wahlperiode Drucksache Nr. 1495

Hessischer Landtag, Drucksache 16/7646

Materialien Gesetzgebung Österreich

72 BlgNr 14. GP.
AA-10 v. 20.04.2018 zu IA 189/A 26. GP.
AB 98 BlgNr 26. GP.
AB 1761 BlgNr 25. GP.
AB 1024 BlgNr 14. GP.
ErläutRV 68 BlgNr 26. GP.
ErläutRV 17 BlgNr 26. GP
ErlRV 1389 BlgNr 24. GP.
ErläutRV 817 BlgNr 21. GP.
ErläutRV 1613 BlgNr 20 GP.
ErläutRV 72 BlgNr 14. GP.
RV 509 BlgNr 26. GP.

Rechtsprechungsverzeichnis

BAG Urteil v. 29.06.2017, Az. 2 AZR 597/16
BAG Beschluss v. 27.05.1986, Az. 1 ABR 48/84
BGH Urteil v. 16.05.2017, Az. VI ZR 135/13
BGH Urteil v. 03.06.2014, Az. III ZR 391/13
BGH Urteil v. 04.06.2013, Az. 1 StR 32/13
BGH Urteil v. 13.01.2011, Az. III ZR 146/10
BVerfG Beschluss v. 27.06.2018, Az. 2 BvR 1405/17
BVerfG Beschluss v. 16.06.2009, Az. 2 BvR 902/06
BVerfG Beschluss v.14.07.1999, Az. 1 BvR 2226/94
BVerfG Beschluss v. 25.03.1992, Az. 1 BvR 1430/88
BVerfG Urteil v. 27.02.2008, Az. 1 BvR 370/07
BVerfG Urteil v. 27.07.2005, Az. 1 BvR 668/04
BVerfG Urteil v. 15.12.1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil)
BVerwG Urteil v. 30. Mai 2018, Az. BVerwG 6 A 3.16 = NVwZ 2018, 1476
DSB Bescheid v. 28.05.2018 DSB-D216.471/0001-DSB/2018 (Österreichische Datenschutzbehörde)
DSK Bescheid v. 13.05.2014 DSB-D600.328-001/0001-DSB/2014 (Datenschutzbehörde Österreich)
DSK Bescheid v. 26.06.2013 K506.250-005/0002-DVR/2013 (Datenschutzbehörde Österreich)
DSK Bescheid v. 30.04.2013 K600.322-005/0003-DVR/2013 (Datenschutzbehörde Österreich)
EGMR Urteil v. 13.09.2018, Az. 58170/13; Az. 62322/14; Az. 24960/15
EGMR Urteil v. 19.06.2018, Az. 35252/08
EGMR Urteil v. 05.09.2017, Az. 61496/08
EGMR Urteil v. 12.01.2016, Az. 37138/14
EGMR Urteil v. 04.12.2015, Az. 47143/06

EGMR Urteil v. 14.03.2013, Az. 24117/08

EGMR Urteil v. 18.05.2010, Az. 26839/05

EGMR Urteil v. 16.10.2007, Az. 74336/01

EGMR Urteil v. 03.04.2007, Az. 62617/00

EGMR Urteil v. 29.06.2006, Az. 54934/00

EuGH GA v. 19.12.2018, C-40/17 („Fashion ID“)

EuGH GA v. 25.06.2013, C-131/12 („Google Spain SL u.a.”)

EuGH Urteil v. 01.10.2019, C-673/17 („Planet49 GmbH“)

EuGH Urteil v. 29.07.2019, C-40/17 („Fashion ID“)

EuGH Urteil v. 13.06.2019, C-193/18 („Google GMail“)

EuGH Urteil v. 10.07.2018, C-25/17 („Zeugen Jehovas“)

EuGH Urteil v. 05.06.2018, C-210/16 („Wirtschaftsakademie Schleswig-Holstein“)

EuGH Urteil v. 21.12.2016, C-203/15, C-698/15 („Tele2 Sverige“)

EuGH Urteil v. 19.10.2016, C-582/14 („Breyer“)

EuGH Urteil v. 06.10.2015, C-362/14 („Schrems“)

EuGH Urteil v. 13.05.2014, C-131/12 („Google Spain SL u.a.“)

EuGH Urteil v. 24.11.2011, C-468/10 („ASNEF“), C-469/10 („FECEMD“)

EuGH Urteil v. 09. 11. 2010, C-92/09, C-93/09 („Schecke”)

EuGH, Rs. 6/64, Slg. 1964, S. 1251, 1269 („Costa/ENEL”)

LAG Berlin-Brandenburg Urteil v. 14.01.2016, Az. 5 Sa 657/15

LAG Berlin-Brandenburg Urteil v. 16.02.2011, Az. 4 Sa 2132/10

LAG Hamm Urteil vom 10.07.2012, Az. 14 Sa 1711/10

LAG Niedersachsen Urteil v. 31.05.2010 12, Az. Sa 875/09

Oberverwaltungsgericht für das Land Nordrhein-Westfalen, Beschluss v. 13.03.2002, Az. 13 B 32/02

OGH 29.08.2019, 6Ob152/19z = MR 2019,224 = ZTR 2019,169 - Mikaela S.

OGH 23.05.2019, 6 Ob A1/18t

OGH 20.12.2018, 6Ob131/18k = ecolex 2019/151 S 346 (Zemann) - ecolex 2019,346 (Zemann) = iFamZ 2019/78 S 117 (Deixler-Hübner) - iFamZ 2019,117 (Deixler-Hübner) = jusIT 2019/29 S 85 (Thiele) - jusIT 2019,85 (Thiele) = EvBl-LS 2019/66 = RZ 2019/11 S 91 (Spenling) - RZ 2019,91 (Spenling) = Thiele, ZIIR 2019,147 = ZIIR 2019,168 = RdW 2019/252 S 316 - RdW 2019,316 = Jahnel, jusIT 2019/42 S 123 - Jahnel, jusIT 2019,123 = Jus-Extra OGH-Z 6509 = Jus-Extra OGH-Z 6510 = Jahnel, VbR 2019/99 S 158 - Jahnel, VbR 2019,158 = MR 2019,190 (Walter) = NZ 2019/110 S 315 - NZ 2019,315 - E-Mails und Chatprotokolle

OGH 13.04.2011, 15 Os 172/10y = EvBl 2011/62 S 419 – EvBl 2011,419 = jusIT 2011/44 S 93 (Karel) – jusIT 2011,93 (Karel) = MR 2011,153 (Hasberger) = Jus-Extra OGH-St 4538 = Jus-Extra OGH-St 4552 = Jus-Extra OGH-St 4553 = RdW 2011/316 S 317 (Info aktuell) – RdW 2011,317 (Info aktuell) = Rn 2011/23 S 252 – Rn 2011,252 = JBl 2011,726 (Reindl-Krauskopf) = Rn 2011,223 EÜ190 – Rn 2011 EÜ190 – ÖBB-Online-Tickets Stammdatenauskunft

OGH 20.12.2006, 9ObA109/06d

OGH 01.10.2002, 11 Os 64/02

OGH 13.06.2002, 8 ObA 288/01p

OGH 17.06.1998, 13 Os 68/98

OLG Dresden Beschluss v. 05.09.2012, Az. 4 W 961/12

OLG Köln Urteil v. 14.12.2015, Az. 12 U 16/13

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)

VfGH 29.11.2017, G 223/2016

VfGH 29.06.2012, B 1031/11 = VfSlg. 19.657

VfGH 14.03.2012, U 466/11 = VfSlg 19.632/2012

VfGH 15.06.2007, G147/06

VwGH 24.04.2013, 2011/17/0293 = VwSlg 18612 A/2013

VwGH 27.05.2009, 2007/05/0280

Sonstige Fachbücher

Aly/Roth, Die restlose Erfassung – Volkszählen, Identifizieren, Aussondern im Nationalsozialismus[2] (2005)

Aust/Ammann, Digitale Diktatur: Totalüberwachung, Datenmissbrauch, Cyberkrieg (2014)

Black, IBM und der Holocaust (2001)

Christl/Spiekermann, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy (2016)

Damaschke, Siri Handbuch (2016)

Greenwald, Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen (2014)

Hofstetter, Das Ende der Demokratie. Wie künstliche Intelligenz die Politik übernimmt und uns entmündigt (2016)

Hofstetter, Sie wissen alles. Wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen (2014)

Howard, Finale Vernetzung (2016)

Mazzucato, Das Kapital des Staates – Eine andere Geschichte von Innovation und Wachstum (2014)

Meier/Klein, Die Zukunft der Büroarbeit bei Volkswagen – Der digitale Assistent, Vortrag Volkswagen AG (2017)

Morozov, Smarte Neue Welt. Digitale Technik und die Freiheit des Menschen (2013)

Rost (Hrsg), Die Netz-Revolution: Auf den Weg in die Weltgesellschaft (1996)

Sander/Spengler, Die Entwicklung der Datenverarbeitung von Hollerith Lochkartenmaschinen zu IBM Enterprise-Servern (2011), abrufbar unter: https://www.informatik.uni-leipzig.de/cs/Literature/History/SandnerSpengler.pdf (zuletzt abgerufen am 20.06.2019)

Schaar, Datenschutz im Internet (2002)

Schaar, Trügerische Sicherheit. Wie die Terrorangst uns in den Ausnahmezustand treibt (2017)

Schönberger, Big Data – Die Revolution, die unser Leben verändern wird (2014)

Schütt, Der Weg zum Digitalen Unternehmen[2] (2015)

Snowden, Permanent Record[2] (2019)

Onlineressourcen

Ackerman in wired.com (10.05.2011), The iPhone 4S' Talking Assistant Is a Military Veteran, abrufbar unter: https://www.wired.com/2011/10/siri-darpa-iphone/ (zuletzt abgerufen am 20.06.2019)

amazon Inc., Alexa for Business, abrufbar unter: https://aws.amazon.com/de/alexaforbusiness/ (zuletzt abgerufen am 20.06.2019)

Arbeitsplatz 4.0., Suchmaschine fürs Intranet gesucht? Das gibts zu beachten…, abrufbar unter: https://www.arbeitsplatz40.de/intranet-suche/ (zuletzt abgerufen am 20.06.2019)

Auer in presse.com (02.09.2014), Interview mit Caspar Bowden: "Die größte Sicherheitslücke ist Microsoft", abrufbar unter: http://diepresse.com/home/techscience/internet/3862525/Caspar-Bowden_Die-groesste-Sicherheitsluecke-ist-Microsoft (zuletzt abgerufen am 20.06.2019)

Bager in c't – Magazin für Computertechnik, Gelenkte Menschen, 16/2015, abrufbar unter: https://www.heise.de/ct/ausgabe/2015-16-Digitale-Assistenten-und-ihre-Anwender-Wer-steuert-wen-2734536.html (zuletzt abgerufen am 20.06.2019)

Bagre in diepresse.com (17.02.2017), Deutschland verbietet Verkauf von Puppe Cayla, abrufbar unter: https://diepresse.com/home/techscience/technews/5171332/Deutschland-verbietet-Verkauf-von-Puppe-Cayla (zuletzt abgerufen am 20.06.2019)

Bamford in wire.com (15.03.2012), The NSA Is Building the Country's Biggest Spy Center (Watch What You Say), abrufbar unter: https://www.wired.com/2012/03/ff-nsadatacenter/ (zuletzt abgerufen am 20.06.2019)

Barnig, PAL: personalized assistant that learns, abrufbar unter: http://www.web3.lu/pal-personalized-assistant-that-learns/ (zuletzt abgerufen am 20.06.2019)

Baumann in Frankfurter Rundschau (05.07.2013), Betreiben die USA Wirtschaftsspionage? abrufbar unter: https://www.fr.de/wirtschaft/betreiben-wirtschaftsspionage-11278668.html (zuletzt abgerufen am 20.06.2019)

Becker in spiegel.de (03.01.2018), Globaler Datenzugriff – US-Gericht entscheidet über unsere Privatsphäre, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/supreme-court-entscheidet-ueber-zukunft-unserer-privatsphaere-a-1186009.html (zuletzt abgerufen am 20.06.2019)

Bleich in heise.de (13.07.2013), Globaler Abhörwahn – Wie digitale Kommunikation belauscht wird, abrufbar unter: https://www.heise.de/ct/ausgabe/2013-16-Wie-digitale-Kommunikation-belauscht-wird-2317919.html (zuletzt abgerufen 20.06.2019)

Borchers in heise.de (15.12.2008), Vor 25 Jahren: Informationelle Selbstbestimmung wird Grundrecht, abrufbar unter: https://www.heise.de/newsticker/meldung/Vor-25-Jahren-Informationelle-Selbstbestimmung-wird-Grundrecht-189834.html (zuletzt abgerufen am 20.06.2019)

Bosker in huffingtonpost.com (24.01.2013), SIRI RISING: The Inside Story Of Siri's Origins — And Why She Could Overshadow The iPhone, abrufbar unter: http://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone_n_2499165.html (zuletzt abgerufen am 20.06.2019)

Bremmer in computerwoche.de (23.09.2016), IBM Watson wird digitaler Büro-Assistent, abrufbar unter: https://www.computerwoche.de/a/ibm-watson-wird-digitaler-buero-assistent,3323791 (abgerufen am 20.06.2019)

bundesregierung.de (30.12.2016), Klare Regeln für Auslandsaufklärung, abrufbar unter: https://www.bundesregierung.de/Content/DE/Artikel/2016/06/2016-06-28-gesetz-bnd-ausland-ausland-fernmeldeaufklaerung.html (zuletzt abgerufen am 20.06.2019)

bundestag.de (27.06.2019), Bundestag stimmt zwei Gesetzen zum Datenschutzrecht zu, abrufbar unter: https://www.bundestag.de/dokumente/textarchiv/2019/kw26-de-datenschutz-649218 (zuletzt abgerufen am 27.06.2019)

bundestag.de, Beschluss des Volkszählungsgesetzes 1983, abrufbar: https://www.bundestag.de/dokumente/textarchiv/2012/38024038_kw10_kalender_volkszaehlung/207898 (zuletzt abgerufen am 20.06.2019)

Carrol in the Guardian (14.06.2013), Welcome to Utah, the NSA's desert home for eavesdropping on America, abrufbar unter: https://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility (zuletzt abgerufen 20.06.2019)

Christl, Kommerzielle Digitale Überwachung im Alltag. Studie im Auftrag der Bundesarbeitskammer (2014), abrufbar unter: https://www.arbeiterkammer.at/infopool/wien/Digitale_Ueberwachung_im_Alltag.pdf (zuletzt abgerufen am 20.06.2019)

Culik/Forte, ABIDA-Dossier Oktober 2017, Big Data-Überwachung am Arbeitsplatz – Grenzen der Zulässigkeit durch aktuelle Gerichtsentscheidungen, abrufbar unter: http://www.abida.de/sites/default/files/Dossier_Ueberwachung.pdf

Daoud, Rechtliche Aspekte bei der Einführung einer Enterprise Search Lösung (2016), abrufbar unter: https://www.researchgate.net/publication/312937768_Rechtliche_Aspekte_bei_der_Einfuhrung_einer_Enterprise_Search-Losung_Eduard_Daoud_Legal_aspects_when_introducing_an_Enterprise_Search_Solution#pf4 (zuletzt abgerufen am 20.06.2019).

DARPA Werbevideo zum PAL Project 2003 – 2008: https://www.youtube.com/watch?v=BFKNFlOocQ (zuletzt abgerufen am 20.06.2019)

DARPA, Personal Assistant That Learns (PAL), abrufbar unter: https://www.darpa.mil/about-us/timeline/personalized-assistant-that-learns (zuletzt abgerufen am 20.06.2019)

datenschutzbeauftragter-info.de (08.10.2013), Wie Verbündete sich gegenseitig ausspionieren, abrufbar unter: https://www.datenschutzbeauftragter-info.de/wie-verbuendete-sich-gegenseitig-ausspionieren/ (zuletzt abgerufen am 20.06.2019)

David Bernet, „Democracy, im Rausch der Daten", Dokumentarfilm (2015), abrufbar unter: https://www.youtube.com/watch?v=VcHNximMb18

Dax in futurzone.at (11.08.17), Interview mit William Binney, abrufbar unter: https://futurezone.at/netzpolitik/massenueberwachung-ist-gegen-terrorismus-wirkungslos/280.046.881 (zuletzt abgerufen am 20.06.2019)

Denkler in sueddeutsche.de (21.10.2016), Neue BND-Gesetz – Der Fulltake aller Daten wird möglich, abrufbar unter: http://www.sueddeutsche.de/politik/neues-bnd-gesetz-bnd-bekommt-eine-lizenz-zum-datensammeln-1.3212099 (zuletzt abgerufen am 20.06.2019)

DER SPIEGEL 19/2015, 20 ff, Der unheimliche Dienst, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/134762481 (zuletzt abgerufen am 20.06.2019)

DER SPIEGEL 18/2015, 36 ff, 40.000 Unwahrheiten, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/134660862 (zuletzt abgerufen am 20.06.2019)

DER SPIEGEL 32/2013, 34, Wirtschaftsspionage – Der Feind in meinem Netz, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/105648238 (zuletzt abgerufen am 20.06.2019)

DER SPIEGEL 07/2001, 36, Der programmierte Massenmord, abrufbar unter: http://magazin.spiegel.de/EpubDelivery/spiegel/pdf/18479605 (zuletzt abgerufen am 20.06.2019).

DER SPIEGEL 8/1989, 44, NSA: Amerikas großes Ohr, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/13494509 (zuletzt abgerufen am 20.06.2019)

DER SPIEGEL 12/1983, 109, Interview mit Wilhelm Steinmüller, abrufbar unter: https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/14021551 (zuletzt abgerufen am 20.06.2019)

dpa in heise.de (15.03.2019), Bundesverfassungsschutz soll Befugnis für Online-Durchsuchungen erhalten, abrufbar unter: https://www.heise.de/newsticker/meldung/Bundesverfassungsschutz-soll-Befugnis-fuer-Online-Durchsuchungen-erhalten-4336985.html (zuletzt abgerufen am 20.06.2019)

dpa/ahe/LTO-Redaktion in LTO.de (07.12.2015), EGMR verurteilt Russland Verstoß gegen Grundrechte, abrufbar unter: https://www.lto.de/recht/nachrichten/n/egmr-russland-abhoer-missbrauch-privatsphaere-verfassungsgericht/ (zuletzt abgerufen 20.06.2019)

Drösser in zeit.de (19.03.2015), Künstliche Intelligenz: Sie haben verstanden, abrufbar unter: http://www.zeit.de/2015/10/kuenstliche-intelligenz-computer-simultan-dolmetscher (zuletzt abgerufen am 20.06.2019)

Emch in srf.ch (18.08.2019), Kuschen Schweizer Cloud-Anbieter vor den USA?, abrufbar unter: https://www.srf.ch/news/wirtschaft/washington-will-unsere-daten-kuschen-schweizer-cloud-anbieter-vor-den-usa (zuletzt abgerufen am 21.08.2019).

Ermert in heise.de (02.07.2013), NSA-Abhörskandal PRISM: Internet-Austauschknoten als Abhörziele Update, abrufbar unter: https://www.heise.de/newsticker/meldung/NSA-Abhoerskandal-PRISM-Internet-Austauschknoten-als-Abhoerziele-1909604.html (zuletzt abgerufen am 20.06.2019)

Ermert in heise.de (16.09.2016), NSA-Skandal und BND-Überwachung: Internet-Knoten De-CIX klagt gegen die Bundesrepublik, abrufbar unter: https://www.heise.de/newsticker/meldung/NSA-Skandal-und-BND-Ueberwachung-Internet-Knoten-De-CIX-klagt-gegen-die-Bundesrepublik-3325186.html (zuletzt abgerufen am 20.06.2019)

Ertel in datenschutz-notizen.de (19.02.2013), Löschen des E-Mail-Accounts ausgeschiedener Beschäftigter, abrufbar unter: https://www.datenschutz-notizen.de/loeschen-des-e-mail-accounts-ausgeschiedener-beschaeftigter-343254/ (zuletzt abgerufen am 20.06.2019)

fask.uni-mainz.de, Künstliche Intelligenz: Spracherkennung und Sprachverstehen, abrufbar unter: http://www.fask.uni-mainz.de/user/warth/Ki.html (zuletzt abgerufen am 20.06.2019)

Finnegan/Maier in computerwoche.de (02.02.2018), Alexa for Business – So macht KI Ihr Büroleben leichter, abrufbar unter: https://www.computerwoche.de/a/so-macht-ki-ihr-bueroleben-leichter,3332223 (zuletzt abgerufen am 20.06.2019)

Forbes Insights, The Digital Workplace in the Cognitive Era (2016), abrufbar unter: https://www.ibm.com/downloads/cas/ZQPDGNNX (zuletzt abgerufen am 20.06.2019)

Friedewald/Quinn/Hansen/Heesen/Hess/Lamla/Matt/Roßnagel/Trepte/Waidner, White Paper Datenschutz-Folgenabschätzung[3] (2017), abrufbar unter: https://www.forum-privatheit.de/wp-content/uploads/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf (zuletzt abgerufen am 20.06.2019).

Fuest/Jüngling/Kaiser in welt.de (23.02.2014), WhatsApp-Nutzer fürchten Analyse ihrer Daten, abrufbar unter: https://www.welt.de/wirtschaft/article125102992/WhatsApp-Nutzer-fuerchten-Analyse-ihrer-Daten.html (zuletzt abgerufen am 20.06.2019)

futurezone.at (18.06.13), "NSA-Analysten haben Zugriff auf alles", abrufbar unter: https://futurezone.at/netzpolitik/nsa-analysten-haben-zugriff-auf-alles/24.598.068 (zuletzt abgerufen am 20.06.2019)

Gallmeyer in tagesschau.de (01.11.2017), Au revoir Ausnahmezustand, abrufbar unter: https://www.tagesschau.de/ausland/frankreich-ausnahmezustand-111.html (zuletzt abgerufen am 20.06.2019)

GDD (08.05.2018), Zulässigkeit des Tracking nach der DS-GVO, abrufbar unter: https://www.gdd.de/aktuelles/startseite/zulaessigkeit-des-tracking-nach-der-ds-gvo (zuletzt abgerufen am 20.06.2019)

Postinett in handelsblatt.com (01.12.2017), Sprachgesteuertes Büro – Alexa muss jetzt arbeiten gehen, abrufbar unter: https://www.handelsblatt.com/unternehmen/it-medien/sprachgesteuertes-buero-alexa-muss-jetzt-arbeiten-gehen/20658226.html (zuletzt abgerufen am 20.06.2019)

Glaser in heise.de (29.05.2015), Wurstförmige Hypercomputer, abrufbar unter: https://www.heise.de/tr/blog/artikel/Wurstfoermige-Hypercomputer-2669252.html (zuletzt abgerufen 20.06.2019)

Greenwald in the Guardian (07.06.2013), NSA Prism program taps in to user data of Apple, Google and others, abrufbar unter: https://www.theGuardian.com/world/2013/jun/06/us-tech-giants-nsa-data (zuletzt abgerufen am 20.06.2019)

Grunert in faz.net (22.06.2017), Bundestrojaner: Durch die Hintertür zur Online-Überwachung; abrufbar unter: https://www.faz.net/aktuell/politik/online-durchsuchung-quellen-tkue-bundestrojaner-wird-gesetz-15071053.html (zuletzt abgerufen am 20.06.2019)

Haar in iX 7/2018, 128 ff – US CLOUD Act regelt internationalen Datenzugriff, abrufbar unter: https://www.heise.de/ix/heft/Wolkenbruch-4089925.html (zuletzt abgerufen am 20.06.2019).

hade./dpa/Reuters in faz.net (18.05.2017), Facebook hat doch gelogen, abrufbar unter: http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/der-facebook-boersengang/facebook-hat-bei-uebernahme-von-whatsapp-doch-gelogen-15021650.html (zuletzt abgerufen am 20.06.2019)

Håkansson, KTH Royal Institute of Technology (Königliche Technische Hochschule Stockholm), AI and privacy GDPR seminar (2017), abrufbar unter: https://www.youtube.com/watch?v=L6vK3deWG4A (zuletzt abgerufen am 20.06.2019)

Holland in heise.de (07.07.2018), BND spionierte EU-Filialen deutscher Firmen aus, abrufbar unter: https://www.heise.de/newsticker/meldung/BND-spionierte-EU-Filialen-deutscher-Firmen-aus-4104511.html (zuletzt abgerufen am 20.06.2019)

Homepage Europäische Kommission, Vivian Reading, abrufbar unter: http://ec.europa.eu/archives/commission_2010-2014/reding/ (zuletzt abgerufen am 20.06.2019)

Horvath, Wissenschaftliche Dienste Deutscher Bundestag (Fachbereich WD 10), Aktueller Begriff Big Data, abrufbar unter: https://www.bundestag.de/blob/194790/c44371b1c740987a7f6fa74c06f518c8/big_data-data.pdf (zuletzt abgerufen am 20.06.2019)

Human Rights Watch, US Surveillance Harming Journalism, Law, Democracy, abrufbar unter: https://www.hrw.org/news/2014/07/28/us-surveillance-harming-journalism-law-democracy (zuletzt abgerufen am 20.06.2019)

humanrights.ch (04.09.2017), Ausnahmezustand in Frankreich, abrufbar unter: https://www.humanrights.ch/de/internationale-menschenrechte/nachrichten/terrorbekaempfung/ausnahmezustand-frankreich-aufweichung-menschenrechte (zuletzt abgerufen am 20.06.2019)

Ililau, army.mil (18.09.2010),'Big Red One' debuts new communication system, abrufbar unter: https://www.army.mil/article/45376/ (zuletzt abgerufen am 20.06.2019)

Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (IWGDPT), Resolution on Privacy Protection and Search Engines (2006), abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2006/2006-IWGDPT-Common_Position_Search_Engines-de.pdf (zuletzt abgerufen am 20.06.2019)

irights.info (23.10.2014), Interview mit Yvonne Hofstetter, was ist wirklich neu an „Big Data“, abrufbar unter: https://irights.info/artikel/yvonne-hofstetter-was-ist-wirklich-neu-an-big-data/24147 (zuletzt abgerufen am 20.06.2019)

Kesssler in futurezone.at (24.02.2015), “Gesamte Telekommunikation in Österreich wird gespeichert”, abrufbar unter: https://futurezone.at/netzpolitik/gesamte-telekommunikation-in-oesterreich-wird-gespeichert/116.081.559 (zuletzt abgerufen am 20.06.2019)

Kling in zdnet.de (11.10.2017), Datenschutz-Panne: Google Home Mini hört dauernd mit: http://www.zdnet.de/88315221/datenschutz-panne-google-home-mini-hoert-dauernd-mit/?inf_by=5a390395681db884538b494e (zuletzt abgerufen am 20.06.2019)

Koederitz in ibm.com (25.07.2017), Kognitive Technologie: Sichere Landung auf dem kognitiven Planeten, abrufbar unter: https://www.ibm.com/de-de/blogs/think/2017/07/25/banking-4-0/ (zuletzt abgerufen am 20.06.2019)

Krempl in golem.de (18.09.2018), Cloud Act – Microsoft will Datenzugriff der USA im Ausland begrenzen, abrufbar unter: https://www.golem.de/news/cloud-act-microsoft-will-datenzugriff-der-usa-im-ausland-begrenzen-1809-136606.html (zuletzt abgerufen am 19.09.2018)

Krempl in heise.de (03.08.2011), Datenschützer bemängelt schleichende Ausweitung der Steuer-ID, abrufbar unter: https://heise.de/-1317621 (zuletzt abgerufen am 20.06.2019).

Krempl in heise.de (06.06.2016), "BND-Reform": Koalition will das Internet im NSA-Stil überwachen, abrufbar unter: https://www.heise.de/newsticker/meldung/BND-Reform-Koalition-will-das-Internet-im-NSA-Stil-ueberwachen-3228466.html (zuletzt abgerufen am 20.06.2019)

Kubiv in macwelt.de (06.11.2012), Siri: 40 Jahre Forschung für intelligenten Sprachassistenten, abrufbar unter: https://www.macwelt.de/news/Siri-als-intelligenter-Sprachassistent-40-Jahre-Forschung-7022972.html (zuletzt abgerufen am 20.06.2019)

Kurz in netzpolitik.org (16.09.2016), Klage gegen den BND wegen Überwachung am Internetknoten DE-CIX, abrufbar unter: https://netzpolitik.org/2016/klage-gegen-den-bnd-wegen-ueberwachung-am-internetknoten-de-cix/ (zuletzt abgerufen am 20.06.2019)

Lardinois in readwrite.com (13.10.2008), Semantic Stealth Startup Siri Raises $8.5 Million, abrufbar unter: http://readwrite.com/2008/10/13/semantic_stealth_startup_siric/ (zuletzt abgerufen am 20.06.2019)

Le Monde.fr/AFP/Reuters in lemonde.fr. (06.07.2017), Le Parlement adopte la sixième et dernière prorogation de l'état d'urgence, abrufbar unter: http://www.lemonde.fr/politique/article/2017/07/06/les-deputes-examinent-la-prorogation-de-l-etat-d-urgence_5156770_823448.html (zuletzt abgerufen am 20.06.2019)

Lewandowski, Whitepaper Enterprise Search (2010), abrufbar unter: https://searchstudies.org/wp-content/uploads/2019/04/Whitepaper-Enterprise-Search-Was-die-Nutzer-erwarten-und-warum-Social-Media-so-entscheidend-ist.pdf (zuletzt abgerufen am 20.06.2019)

Leyendecker/Goetz in sueddeutsche.de (04.10.2014), Codewort Eikonal – der Albtraum der Bundesregierung, abrufbar unter: http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432 (zuletzt abgerufen am 20.06.2019)

Mascolo/Leyendecker /Goetz in sueddeutsche.de (04.10.2014), Codewort Eikonal – der Albtraum der Bundesregierung, abrufbar unter: http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432 (zuletzt abgerufen am 20.06.2019)

Mascolo/Steinke in sueddeutsche.de (28.05.2018), Überwachung am De-Cix: Betreiber des weltgrößten Internetknotens wirft BND Rechtsbruch vor, abrufbar unter: https://www.sueddeutsche.de/digital/ueberwachung-am-de-cix-betreiber-des-weltgroessten-internetknotens-wirft-bnd-rechtsbruch-vor-1.3994191 (zuletzt abgerufen am 20.06.2019)

max/Reuters/dpa in spiegel.de (29.10.2013), NSA-Spähaffäre. Frankreich will USA bei Wirtschaftsspionage übertrumpfen, abrufbar unter: http://www.spiegel.de/politik/ausland/frankreich-will-usa-bei-wirtschaftsspionage-uebertrumpfen-a-930723.html (zuletzt abgerufen am 20.06.2019)

Meineck in spiegel.de (09.04.2017), Funktioniert Sprechen so gut wie Tippen?, abrufbar unter: http://www.spiegel.de/netzwelt/apps/spracherkennung-fuer-ios-und-android-im-test-wie-gut-funktioniert-das-a-1134324.html (zuletzt abgerufen am 20.06.2019)

Meister in netzpolitik.org (30.06.2016), Das neue BND-Gesetz: Alles, was der BND macht, wird einfach legalisiert. Und sogar noch ausgeweitet., abrufbar unter: https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/ (zuletzt abgerufen am 20.06.2019)

Mendonca in ETtech (22.08.2016), How Capgemini is using IBM's Watson to assign employees to projects, abrufbar unter: http://tech.economictimes.indiatimes.com/news/corporate/how-capgemini-is-using-ibms-watson-to-assign-employees-to-projects/53803797 (zuletzt abgerufen am 20.06.2019)

Meyer in computerwoche.de (10.04.2001), IBM und der Holocaust: War Watson einer der größten Verbrecher? abrufbar unter: https://www.computerwoche.de/a/ibm-und-der-holocaust-war-watson-einer-der-groessten-verbrecher,559460 (zuletzt abgerufen am 20.06.2019)

Microsoft Inc., SIX PRINCIPLES FOR INTERNATIONAL AGREEMENTS GOVERNING LAW- ENFORCEMENT ACCESS TO DATA, abrufbar unter: https://blogs.microsoft.com/uploads/prod/sites/5/2018/09/SIX-PRINCIPLES-for-Law-enforcement-access-to-data.pdf (zuletzt abgerufen am 20.06.2019)

Moechel in fm4.orf.at (24.06.2018), Wie der BND die Kommunikation in Österreich überwacht, abrufbar unter: http://fm4.orf.at/stories/2920556/ (zuletzt abgerufen am 20.06.2019)

Nellis/Cadell in reuters.com (24.02.2018), Apple moves to store iCloud keys in China, raising human rights fears, abrufbar unter: https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060 (zuletzt abgerufen am 20.06.2019)

Nikbakhsh/Zotter in profil.at (20.06.2018), BND-Affäre: Die Deutschen spähten Unis aus – und die Firma von Hannes Androsch, abrufbar unter: https://www.profil.at/oesterreich/bnd-affaere-deutschen-unis-firma-hannes-androsch-10148301 (zuletzt abgerufe am 20.06.2019)

Niklas in haufe.de (07.02.2018), Zulaessigkeit von Big Data Analysen, abrufbar unter: https://www.haufe.de/personal/arbeitsrecht/datenschutz-zulaessigkeit-von-big-data-analysen_76_441566.html (zuletzt abgerufen am 20.06.2019)

Obertreis in tagesspiegel.de (18.11.2016) 20 Jahre Telekom-Börsengang – Eine Aktie fürs Volk, abrufbar unter: http://www.tagesspiegel.de/wirtschaft/20-jahre-telekom-boersengang-eine-aktie-fuers-volk/14852362.html (zuletzt abgerufen am 20.06.2019)

Öchsner in sueddeutsche.de (08.07.2010), Steuer-Identifikationsnummer – Elf Ziffern, die Angst machen, abrufbar unter: http://www.sueddeutsche.de/geld/steuer-identifikationsnummer-elf-ziffern-die-angst-machen-1.971540
(zuletzt abgerufen am 20.06.2019)

Patalong in spiegel.de (08.06.2013), Daten-Überwachungszentrum in Utah Festung der Cyberspione, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/bluffdale-das-datensammel-zentrum-der-nsa-a-904355.html (zuletzt abgerufen 20.06.2019)

Pitzke in spiegel.de (28.07.2014), Das Ende der Pressefreiheit, abrufbar unter: http://www.spiegel.de/politik/ausland/human-rights-watch-nsa-ueberwachung-schadet-journalismus-a-983139.html (zuletzt abgerufen am 20.06.2019)

Postinett in handelsblatt.com (25.06.2018), Sprachassistenten Hotels, Banken, Autos – Alexa erobert die Unternehmenswelt, abrufbar unter: https://www.handelsblatt.com/technik/thespark/sprachassistenten-hotels-banken-autos-alexa-erobert-die-unternehmenswelt/22730722.html (zuletzt abgerufen am 20.06.2019)

Raab in beck.de, EGMR: Russische Überwachungsgesetze verstoßen gegen EMRK, abrufbar unter: https://rsw.beck.de/cms/?toc=ZD.ARC.201602&docid=376184 (zuletzt abgerufen 20.06.2019)

Rosenbach/Stark/Stock in spiegel.de (10.06. 2013), Prism Exposed Data Surveillance with Global Implications, abrufbar unter: http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761.html (zuletzt abgerufen 20.06.2019)

Rost, Interview mit Prof. DDr. Podlech vom November 2008, abrufbar unter: https://www.maroki.de/pub/video/podlech/start_video_podlech.html (zuletzt abgerufen am 20.06.2019)

Rost, Interview mit Prof. Dr. Lutterbeck vom März 2009, abrufbar unter: https://www.maroki.de/pub/video/lutterbeck/start_video_lutterbeck.html (zuletzt abgerufen am 20.06.2019)

Rost, Interview mit Prof. Dr. Steinmüller vom März 2009, abrufbar unter: https://www.maroki.de/pub/video/steinmueller/start_video_steinmueller.html (zuletzt abgerufen am 20.06.2019)

Rötzer in heise.de (12.03.2000), Ex-CIA-Direktor bestätigt Wirtschaftsspionage mittels Echelon, abrufbar unter: https://www.heise.de/newsticker/meldung/Ex-CIA-Direktor-bestaetigt-Wirtschafts spionage-mittels-Echelon-20861.html (zuletzt abgerufen am 20.06.2019)

Rötzer in heise.de (24.03.2007), Innenministerium: Verfassungsschutz, MAD und BND können Online-Durchsuchungen durchführen, aburfbar unter: https://www.heise.de/newsticker/meldung/Innenministerium-Verfassungsschutz-MAD-und-BND-koennen-Online-Durchsuchungen-durchfuehren-161153.html (zuletzt abgerufen am 20.06.2019)

Roush in xconomy.com (14.06.2010), The Story of Siri, from Birth at SRI to Acquisition by Apple—Virtual Personal Assistants Go Mobile, abrufbar unter: http://www.xconomy.com/san-francisco/2010/06/14/the-story-of-siri-from-birth-at-sri-to-acquisition-by-apple-virtual-personal-assistants-go-mobile/ (zuletzt abgerufen am 20.06.2019)

Rüb in faz.net (11.06.2013), Amerikas Geheimdienste. Eine Truppe von mehr als 850.000 Mann, abrufbar unter: http://www.faz.net/aktuell/politik/ausland/amerika/amerikas-geheimdienste-eine-truppe-von-mehr-als-850-000-mann-12217135.html (zuletzt abgerufen am 20.06.2019)

Safire in nytimes.com (05.06.2003), Dear Darpa Diary, abrufbar unter: http://www.nytimes.com/2003/06/05/opinion/dear-darpa-diary.html (zuletzt abgerufen am 20.06.2019)

Schmid in europarl.europa.eu, Sprechzettel für die Sitzung des Innenausschusses des Europäischen Parlaments am 5.9.2013, 2, abrufbar unter: http://www.europarl.europa.eu/document/activities/cont/201312/20131203ATT75410/20131203ATT75410EN.pdf (zuletzt abgerufen am 20.06.2019).

Schmid, *Gerhard Dr*., Abgeordneten-Datenbank des Europäischen Parlaments, abrufbar unter: http://www.europarl.europa.eu/meps/de/1239/GERHARD_SCHMID_home.html (zuletzt abgerufen am 20.06.2019)

Schmid/Sulzbacher in standard.at (06.07.2018), BND spähte österreichische Firma vor Kauf durch deutsche Rheinmetall aus, abrufbar unter: https://derstandard.at/2000082963575/BND-spaehte-oesterreichische-Firma-vor-deren-Kauf-durch-deutsche-Rheinmetall (zuletzt abgerufen am 20.06.2019)

Schmid/Sulzbacher in standard.at (15.06.2018), Die Liste: Wen der deutsche Geheimdienst in Österreich ausspähte, abrufbar unter: https://derstandard.at/2000081647150/Die-Liste-Wen-der-deutsche-Geheimdienst-in-Oesterreich-ausspaehte (zuletzt abgerufe am 20.06.2019)

Schmitt in zeit.de (09.02.2017) Künstliche Intelligenz: Verstehst du, was ich will? Besser, als du glaubst, abrufbar unter: http://www.zeit.de/2017/05/kuenstliche-intelligenz-chatbots-alexa-siri-kommunikation (zuletzt abgerufen am 20.06.2019)

Schneider in telemedicus.info (05.02.2014), EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt, abrufbar unter: https://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html (zuletzt abgerufen am 20.06.2019)

Schonfeld in techcrunch.com (28.04.2010), Silicon Valley Buzz: Apple Paid More Than $200 Million For Siri To Get Into Mobile Search, abrufbar unter: https://techcrunch.com/2010/04/28/apple-siri-200-million/ (zuletzt abgerufen am 20.06.2019)

Schonschek, Interne Suchmaschinen: So geht's datenschutzkonform, abrufbar unter: https://www.datenschutz-praxis.de/fachartikel/wie-sich-interne-suchmaschinen-datenschutzkonform-einsetzen-lassen/ (zuletzt abgerufen am 20.06.2019)

Schulzki-Haddouti in heise.de (26.02.1998), Abhör-Dschungel. Geheimdienste lesen ungeniert mit – Grundrechte werden abgebaut, abrufbar unter: http://heise.de/-286194 (zuletzt abgerufen am 20.06.2019)

Sehl in lto.de (31.05.2018), Geheimdienst darf weiter Rechenzentren anzapfen, abrufbar unter: https://www.lto.de/recht/hintergruende/h/bverwg-6a316-bnd-internet-knoten-betreiber-ueberwachung-geheimdienst-daten-grundrechte/ (zuletzt abgerufen am 20.06.2019)

Singer, Wissenschaftliche Dienste Deutscher Bundestag (Fachbereich WD 10), Aktueller Begriff Cloud Computing, abrufbar unter: https://www.bundestag.de/blob/191178/22a75530 89d81c2e06866e15fc354a0e/cloud_computing-data.pdf (zuletzt abgerufen am 20.06.2019)

Sokolov in heise.de (12.03.2018), Jahrelange Datenschutzverletzung: Telekom Austria drohen 218 Euro Strafe, abrufbar unter: https://www.heise.de/newsticker/meldung/Jahrelange-Daten schutzverletzung-Telekom-Austria-drohen-218-Euro-Strafe-3990676.html?seite=all (zuletzt abgerufen am 20.06.2019)

Sokolov in heise.de (18.04.2018), Microsoft vs. USA: Supreme Court entscheidet nicht über internationalen Datenzugriff, abrufbar unter: https://www.heise.de/newsticker/meldung/Microsoft-vs-USA-Supreme-Court-entscheidet-nicht-ueber-internationalen-Datenzugriff-4026378.html (zuletzt abgerufen am 20.06.2019)

Sokolov in heise.de (28.02.2018), Streit über internationalen Datenzugriff der USA: Microsoft hat schlechte Karten, abrufbar unter: https://www.heise.de/newsticker/meldung/Streit-ueber-internationalen-Datenzugriff-der-USA-Microsoft-hat-schlechte-Karten-3981796.html (zuletzt abgerufen am 20.06.2019)

Soldatow in sueddeutsche.de (23.09.2017), Was Wikileaks-Dokumente über Russlands Überwachungsapparat verraten, abrufbar unter: http://www.sueddeutsche.de/digital/geheimdienst-was-wikileaks-dokumente-ueber-russlands-ueberwachungsapparat-verraten-1.3678453 (zuletzt abgerufen am 20.06.2019)

Söldner/Volk in heise.de (iX 4/2017, S. 70) IBMs Watson für den Arbeitsplatz. Ausgewertet. abrufbar unter: https://www.heise.de/select/ix/2017/4/1490442995260423 (zuletzt abgerufen am 20.06.2019)

spiegel.de (06.07.2018), BND hörte Filialen deutscher Unternehmen in der EU ab, abrufbar unter: http://www.spiegel.de/politik/deutschland/bundesnachrichtendienst-bnd-hoerte-filialen-deutscher-firmen-in-der-eu-ab-a-1217016.html (zuletzt abgerufen am 20.06.2019)

spiegel.de (27.09.2016), Datenschützer geht gegen Facebook vor, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/whatsapp-und-facebook-datenschuetzer-droht-wegen-daten abgleich-a-1114120.html (zuletzt abgerufen am 20.06.2019)

sri.com, Presentation PAL Technologies for the Military, abrufbar unter: https://www.sri.com/sites/default/files/brochures/sri_palmilitary.pdf (zuletzt abgerufen am 20.06.2019)

standard.at (19.11.2010), Telekom Austria ging vor 10 Jahren an die Börse, abrufbar unter: http://derstandard.at/1289608302892/Telekom-Austria-ging-vor-10-Jahren-an-die-Boerse (zuletzt abgerufen am 20.06.2019)

standard.at (20.06.2018), Wie Grazer Professoren und Androsch ins Netz des BND gerieten, abrufbar unter: https://www.derstandard.de/story/2000081932542/wie-zwei-grazer-professoren-und-hannes-androsch-ins-netz-des (zuletzt abgerufe am 20.06.2019)

Stark in spiegel.de (09.03.2009), GEHEIMDIENSTE Digitale Spionage, abrufbar unter: http://www.spiegel.de/spiegel/print/d-64497190.html (zuletzt abgerufen am 20.06.2019)

Stevens in engadget.com (30.07.2009), DARPA's CALO project, the militaristic Clippy, set to invade iPhones this year, abrufbar unter: https://www.engadget.com/2009/07/30/darpas-calo-project-the-militaristic-clippy-set-to-invade-iph/ (zuletzt abgerufen am 20.06.2019)

Stocker, Enterprise Search: Potenziale und Fallstricke (2015) 2 ff, abrufbar unter: https://www.researchgate.net/publication/274388399_Enterprise_Search_Potenziale_und_Fallstricke (zuletzt abgerufen am 20.06.2019)

Stocker, Enterprise Search: Potenziale und Fallstricke (2015), abrufbar unter: https://www.researchgate.net/publication/274388399_Enterprise_Search_Potenziale_und_Fallstricke (zuletzt abgerufen am 20.06.2019)

Studie Ovum, Virtual digital assistants to overtake world population by 2021, abrufbar unter: https://ovum.informa.com/resources/product-content/virtual-digital-assistants-to-overtake-world-population-by-2021 (zuletzt abgerufen am 20.06.2019)

Sulzbacher in standard.at (26.10.2016), NSA-Lauschstation Königswarte: Jahrelanger Bruch der Neutralität, abrufbar unter: https://derstandard.at/2000046460106/NSA-Lauschstation-Koenigswarte-Jahrzehntelanger-Bruch-der-Neutralitaet (zuletzt abgerufen am 20.06.2019)

telegraph.co.uk (13.07.2015), Caspar Bowden, privacy campaigner – obituary, abrufbar unter: http://www.telegraph.co.uk/news/obituaries/11736359/Caspar-Bowden-privacy-campaigner-obituary.html (zuletzt abgerufen 20.06.2019)

theguardian.com (17.06.2017), Edward Snowden: NSA whistleblower answers reader questions, abrufbar unter: https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower (zuletzt abgerufen am 20.06.2019)

Thiel in faz.net (03.07.2013), NSA-Spionage am Frankfurter Netzknoten? Der bequemere Weg zu den Datenströmen, abrufbar unter: http://www.faz.net/aktuell/feuilleton/nsa-spionage-am-frankfurter-netzknoten-der-bequemere-weg-zu-den-datenstroemen-12269650.html (zuletzt abgerufen am 20.06.2019)

Thorel in zdnet.com (30.06.2000), Frenchelon – France has nothing to envy in Echelon, abrufbar unter: https://www.zdnet.com/article/frenchelon-france-has-nothing-to-envy-in-echelon/ (zuletzt abgerufen am 20.06.2019)

Thorenz in computerwoche.de (09.08.2016), Warum kognitive Systeme wichtig werden, abrufbar unter: https://www.computerwoche.de/a/print/warum-kognitive-systeme-wichtig-werden,3315459 (zuletzt abgerufen am 20.06.2019)

Triebe in faz.net (04.09.2015), Datenspeicherung in Russland : Unbehagen über neues Datenschutzgesetz, abrufbar unter: http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/kreml-will-russische-nutzerdaten-in-russland-speichern-13784269.html (zuletzt abgerufen am 20.06.2019)

U.S. House of Representatives, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (2012), abrufbar unter: https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf (zuletzt abgerufen am 20.06.2019)

Verbraucherzentrale NRW (20.12.2017), Digitaler Sprachassistent: Alexa reagiert auch ungefragt: https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/digitaler-sprachassistent-alexa-reagiert-auch-ungefragt-21363 (zuletzt abgerufen am 20.06.2019)

Weber-Lamberdière in focus.de (07.07.2013), Die langen Ohren Frankreichs: Wie uns die Grande Nation groß ausspioniert, abrufbar unter: https://www.focus.de/politik/ausland/tid-32242/spezialgebiet-wirtschaftsspionage-die-langen-ohren-frankreichs-wie-uns-die-grande-nation-gross-ausspioniert_aid_1036856.html (zuletzt abgerufen am 20.06.2019)

Wenzel in Frankfurter Rundschau (29.05.2018), Der Geheimdienst liest mit, abrufbar unter: http://www.fr.de/kultur/netz-tv-kritik-medien/netz/de-cix-der-geheimdienst-liest-mit-a-1514929 (zuletzt abgerufen am 20.06.2019)

Wiegand, Einführung einer Enterprise Search Lösung und Erweiterung dieser um Aspekte einer Search Based Application (2012), Diplomarbeit Otto von Guericke Universität Magdeburg Fakultät für Informatik, Betreuer Prof. Dr. rer. Pol. Habil. Hans-Knud Arndt, 26 ff, abrufbar unter: http://bauhaus.cs.uni-magdeburg.de:8080/miscms.nsf/FEA8C8150500AA14C125744 9004F79A9/4C9BAAB3F99F05EAC1257A06004FAB37/$FILE/Diplomarbeit%20Christoph%20Wiegand.pdf (zuletzt abgerufen am 20.06.2019).

Wikipedia.de, Verdienstorden vom Deutschen Adler, abrufbar unter: https://de.wikipedia.org/wiki/Verdienstorden_vom_Deutschen_Adler (zuletzt abgerufen am 20.06.2019).

Wikipedia.de, Frenchelon, abrufbar unter: https://en.wikipedia.org/wiki/Frenchelon (zuletzt abgerufen am 20.06.2019)

Wilkens in heise.de (12.10.2017), Datenschutzpanne mit Google Home Mini: Einschaltknopf wird deaktiviert: https://www.heise.de/newsticker/meldung/Datenschutzpanne-mit-Google-Home-Mini-Einschaltknopf-wird-deaktiviert-3858861.html (zuletzt abgerufen am 20.06.2019)

Wissenschaftliche Dienste Deutscher Bundestag, WD 2 – 3000 – 208/15, 3 ff; abrufbar unter: https://www.bundestag.de/blob/424386/be4e65c12abf5f41c6afb9621f407639/wd-2-208-15-pdf-data.pdf (zuletzt abgerufen am 20.06.2019)

Wortham in NewYorkTimes (29.04.2010), Apple Buys a Start-Up for Its Voice Technology, abrufbar unter: http://www.nytimes.com/2010/04/29/technology/29apple.html (zuletzt abgerufen am 20.06.2019)

Wurzel in tagesschau.de (28.02.2018), iCloud zieht nach China, abrufbar: https://www.tagesschau.de/ausland/icloud-china-101.html (zuletzt abgerufen am 20.06.2019)

Wybitul, § 32 BDSG: Bundesarbeitsgericht klärt wichtige Fragen des Beschäftigtendatenschutzes, abrufbar unter: http://hoganlovells-blog.de/2017/09/03/%c2%a7-32-bdsg-bundesarbeitsgericht-klaert-wichtige-fragen-des-beschaeftigtendatenschutzes/# (zuletzt abgerufen am 20.06.2019)

Y. Hofstetter, U. Schäfer und B. Baginski, Öffentliche Diskussion: „Licht und Schatten der Digitalisierung“ (veröffentlicht am 23.06.2017): https://www.youtube.com/watch?v=fBYpp2AyLRs (zuletzt abgerufen am 20.06.2019)

zeit.de (31. Mai 2017), Menschenrechte: Amnesty wirft Frankreich Missbrauch des Ausnahmezustands vor, abrufbar unter: http://www.zeit.de/news/2017-05/31/menschenrechte-amnesty-wirft-frankreich-missbrauch-des-ausnahmezustands-vor-31015005 (zuletzt abgerufen am 20.06.2019)