

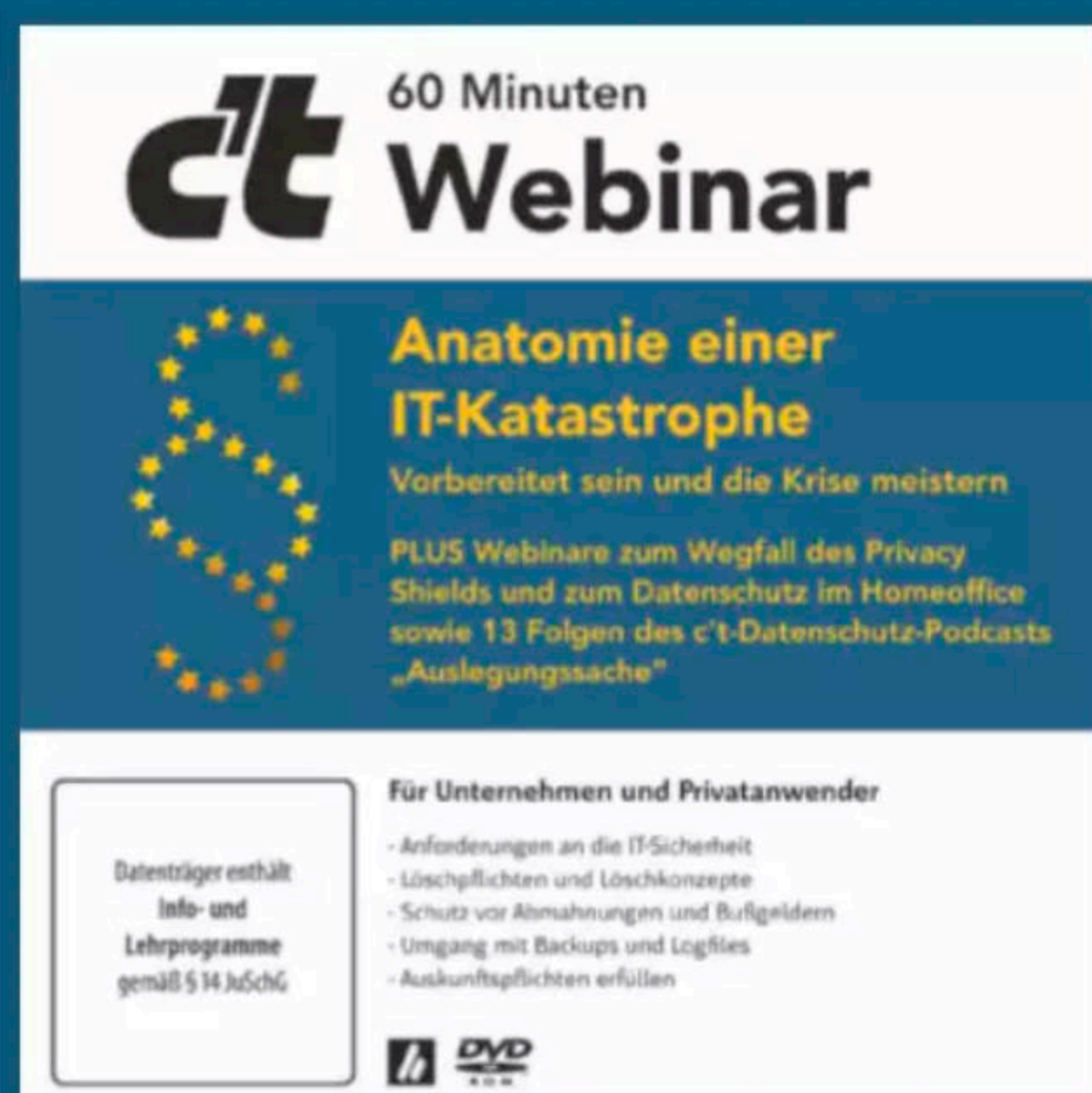
AUF DVD
und zum Download

Webinare, Podcasts und Vorlagen

c't DSGVO

Was 2021 wirklich wichtig wird

- **Aus der Praxis:** 180 Seiten Ratgeber von Fachjuristen
- Was Unternehmen, Vereine und Selbstständige wissen müssen
- Mit vielen FAQs, Anleitungen, Checklisten und Mustern
- Die 10 Datenschutz-Gebote des Homeoffice PLUS Webinar



€ 19,90
CH CHF 33.50
AT € 20,90
LUX € 22,90





**WIR MACHEN
KEINE WERBUNG.
WIR MACHEN EUCH
EIN ANGEBOT.**



ct.de/angebot

Jetzt gleich bestellen:

 ct.de/angebot

 +49 541/80 009 120

 leserservice@heise.de

ICH KAUF MIR DIE c't NICHT. ICH ABONNIER SIE.

Ich möchte c't 3 Monate lang mit 35 % Neukunden-Rabatt testen.
Ich lese 6 Ausgaben als Heft oder digital in der App, als PDF oder direkt im Browser.

**Als Willkommensgeschenk erhalte ich eine Prämie nach Wahl,
z. B. einen RC-Quadrocopter.**



Editorial

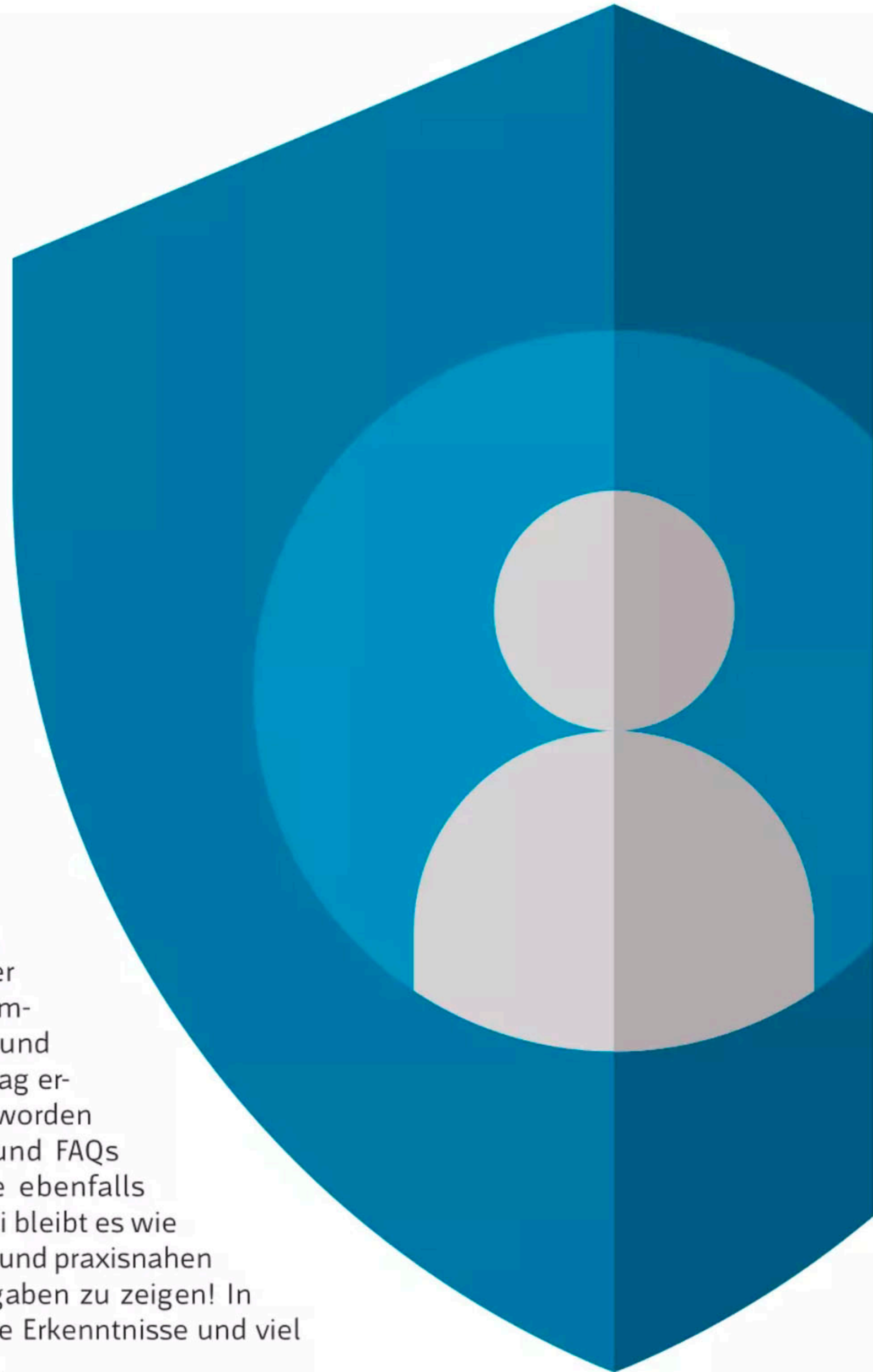
Liebe Leserin, lieber Leser,

im Mai 2021 findet die DSGVO bereits seit drei Jahren Anwendung. Eine ganze Menge Unwägbarkeiten der Anfangszeit liegen bereits hinter uns. So können wir inzwischen immerhin beruhigt feststellen, dass die vielfach erwarteten Massenabmahnungen ausgeblieben sind. In anderen Bereichen ist das Datenschutzrecht aber inzwischen scharf gestellt. Dies gilt vor allem für die Bußgelder, die inzwischen auch zweistellige Millionenhöhe erreichen. Außerdem bringen neue Entwicklungen wie die Pandemie auch für das Recht neue Entwicklungen, etwa die Anforderungen des Datenschutzes an das Homeoffice oder an die Mitarbeiterüberwachung.

Auch mit der nunmehr dritten Auflage unseres Sonderhefts wollen Ihnen die Autoren wieder ihre Erfahrungen aus Theorie und Praxis umfassend und mit viel Herzblut vermitteln und Ihnen damit den datenschutzrechtlichen Alltag erleichtern. Das Magazin ist wieder dicker geworden und wir haben neue Artikel, Checklisten und FAQs aufgenommen. Auf der DVD erwarten Sie ebenfalls neue Webinare, Vorträge und Podcasts. Dabei bleibt es wie bisher unser Ziel, Ihnen einen verständlichen und praxisnahen Weg durch den Urwald der juristischen Vorgaben zu zeigen! In diesem Sinne wünschen wir Ihnen viele gute Erkenntnisse und viel Spaß bei der Arbeit mit unserem Sonderheft.



Joerg Heidrich & Nicolas Maekeler



Inhalt

DSGVO-BASICS

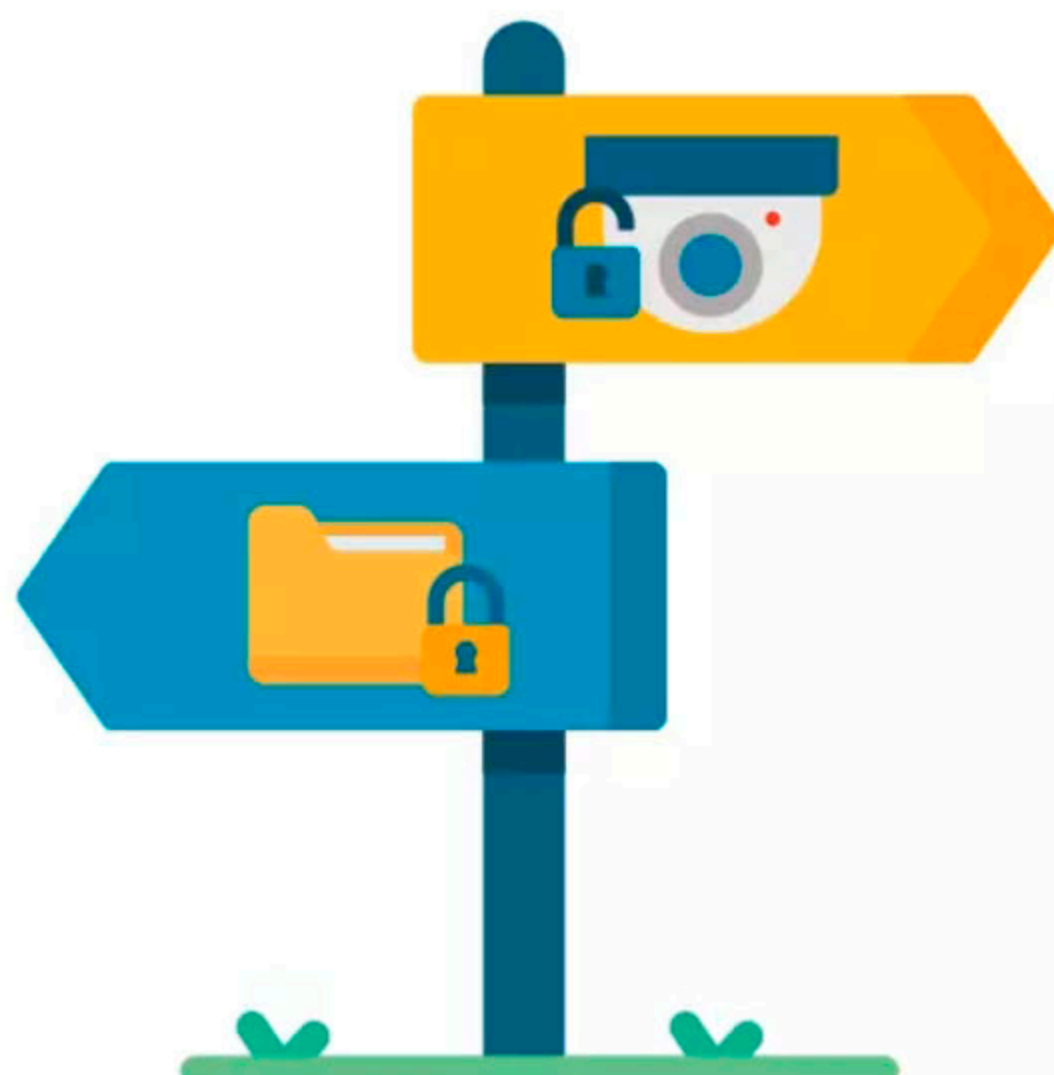
Die Datenschutz-Grundverordnung hat sich in den vergangenen zwei Jahren als Dauerbegleiter etabliert. Alle Regelungen leiten sich aus einigen zentralen Grundsätzen ab.

- 8 Was war, was wird?
- 10 Das sollten Sie wissen
- 12 Gilt die DSGVO auch für mich?
- 16 Grundsätze des Datenschutzrechts

DSGVO FÜR BÜRGER

Ein wesentliches Ziel der Datenschutz-Grundverordnung ist der Schutz des Einzelnen bei der Verarbeitung personenbezogener Daten. Betroffenen gewährt sie daher weitgehende Schutz- und Auskunftsrechte.

- 22 Mehr Rechte für Bürger
- 24 Das Recht auf Auskunft
- 28 Musterantwort für Auskunftersuchen
- 32 Das Recht auf Vergessenwerden
- 34 Folgen für Vereine



PFLICHTEN FÜR UNTERNEHMEN

Die DSGVO bringt nach wie vor für Unternehmen eine Fülle an Pflichten mit sich. Grundsätzlich gelten diese vom Einzelunternehmer bis zum global tätigen Konzern gleichermaßen, mit bislang nur einer Ausnahme.

- 38 Mehr Pflichten für Unternehmer
- 42 Verarbeitungsverzeichnisse
- 46 Datenschutzerklärung
- 50 TOMs dokumentieren
- 54 Datenweitergabe im Unternehmen
- 56 Auftragsverarbeitung
- 60 Sanktionen & Schadensersatz
- 62 Bußgelder: Eine Übersicht
- 70 Abmahnungen
- 72 Schadensersatzansprüche
- 74 Datenschutzbeauftragte
- 78 Auskunftspflichten für Unternehmen
- 82 Rechtmäßige Videoüberwachung
- 86 Online-Gewinnspiele
- 88 Gesundheitsdaten schützen
- 92 Mitarbeiterüberwachung

DATENSCHUTZ UND CORONA

2020 hat Corona den Alltag vieler Menschen grundlegend verändert. Das Homeoffice wurde für Viele zum normalen Arbeitsplatz und Videokonferenzen zum Standard. Was bedeutet das für den Datenschutz?

- 98 Datenschutz und Corona
- 102 Homeoffice & Datenschutz
- 106 Kontrollen am Arbeitsplatz



DATENEXPORT INS AUSLAND

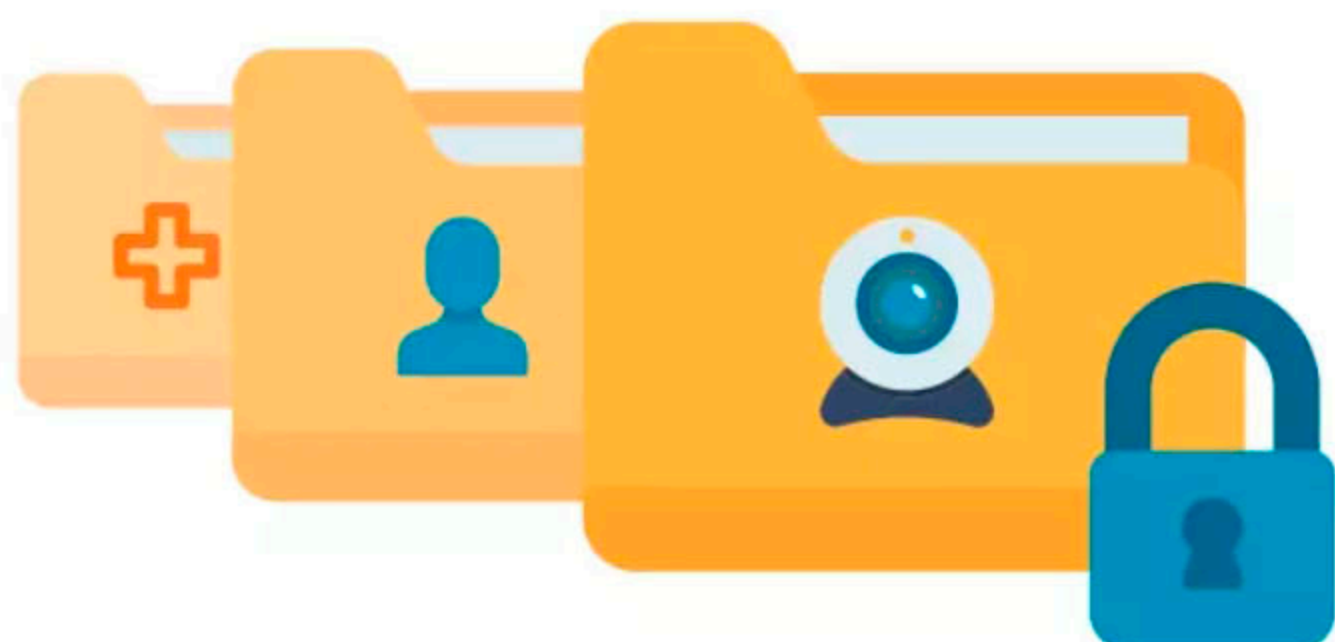
Das Privacy Shield-Abkommen zwischen der EU und den USA gilt nicht mehr, Großbritannien ist aus der EU ausgetreten. Was müssen Unternehmen bei einem Datenaustausch mit ausländischen Partnern beachten?

- 108** Daten ins Ausland übertragen
- 112** Das Ende des Privacy Shield
- 116** Alternativen zum Privacy Shield
- 122** Der Brexit und seine Folgen

TECHNISCHER DATENSCHUTZ

Mit der DSGVO ist die IT-Sicherheit nun elementarer Bestandteil des Datenschutzes. Vernachlässigt man die Pflichten in der technischen Praxis beim Umgang mit personenbezogenen Daten, drohen auch hierfür hohe Bußgelder.

- 124** Ohne IT-Sicherheit kein Datenschutz
- 128** Risiken richtig abschätzen
- 132** Cloud Computing beim Dienstleister
- 136** Daten rechtssicher löschen
- 140** Backup und Archivierung
- 144** Meldepflichten bei Datenpannen



DATENSCHUTZ FÜR WEBSEITEN

Betreiber einer Website müssen ihren Internetauftritt datenschutz-konform gestalten und wissen, welche Informationen weder fehlen noch falsch sein dürfen.

- 148** DSGVO für Website-Betreiber
- 152** Facebook & Datenschutz
- 154** E-Mail-Marketing
- 158** Cookies

RECHTSSICHER FOTOGRAFIEREN

Ob auf Websites oder in Firmenzeitschriften und Flyern: Welche Fotos dürfen Sie unter welchen Voraussetzungen machen und veröffentlichen und welche Anforderungen stellt die DSGVO sonst noch an Fotografen.

- 164** DSGVO für Fotografen
- 168** Rechtssicher fotografieren
- 174** Event-Fotografie

ZUM HEFT

- 3** Editorial
- 6** Impressum
- 7** Autoren
- 176** DVD und Rabattaktion

IMPRESSUM

Redaktion

Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.ct-special.de

Leserbriefe und Fragen zum Heft: sonderhefte@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@ct.de oder xxx@ct.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Jobst-H. Kehrhahn (keh)
(verantwortlich für den Textteil)

Konzeption: Joerg Heidrich (joh), Nicolas Maekeler (nim)

Koordination: Ann-Sophie Eikermann (ase), Jobst-H. Kehrhahn (keh), Angela Meyer (anm)

Redaktion: Jobst-H. Kehrhahn (keh), Angela Meyer (anm)

Mitarbeiter dieser Ausgabe: Nick Akinci, Joerg Heidrich (joh), Nicolas Maekeler, Niklas Mühleis, Brian Scheuch

Assistenz: Susanne Cölle (suc), Tim Rittmeier (tir), Christopher Tränkmann (cht), Martin Triadan (mat)

DTP-Produktion: Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Sarah Hiller, Kirsten Last, Steffi Martens, Marei Stade, Matthias Timm, Ricardo Ulbricht, Ninett Wagner

Fotografie: Andreas Wodrich, Melissa Ramson

Produktion, Xpublisher-Technik: Christine Kreye (Ltg.), Melanie Becker, Anna Hager, Kevin Harte, Pascal Wissner

Titel: Steffi Martens

Bildquelle: www.flaticon.com, www.freepik.com, www.stock.adobe.com

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Dr. Alfons Schröder

Mitglieder der Geschäftsleitung: Beate Gerold, Jörg Mühle

Verlagsleiter: Dr. Alfons Schröder

Anzeigenleitung: Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: André Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3-11, 86650 Wemding

Vertrieb Einzelverkauf:
VU Verlagsunion KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1800
E-Mail: info@verlagsunion.de

Einzelpreis: € 19,90; Schweiz CHF 33.50;
Österreich € 20,90; Luxemburg € 22,90

Erstverkaufstag: 26.01.2021

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlags in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen in c't erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher:
www.xpublisher.com

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2021 by
Heise Medien GmbH & Co. KG

Autoren

Das c't DSGVO stammt aus der Feder von Juristen, die sich auf IT-Recht sowie Internet- und Datenschutzrecht spezialisiert haben. Die Erfahrungen, die sie während ihrer täglichen Arbeit als Rechtsanwälte und Datenschutzbeauftragte seit Inkrafttreten der DSGVO sammeln konnten, sind als Praxisleitfaden in diesem Sonderheft zusammengefasst.



Nick Akinci ist Rechtsanwalt und Partner der Kanzlei Heidrich Rechtsanwälte in Hannover. Bereits während seines Studiums setzte er seine Schwerpunkte auf die Gebiete des Datenschutz- und IT-Rechts sowie des geistigen Ei-

gentums. Zudem hat Akinci zwei Semester an der School of Law der University of Nottingham studiert und anschließend den Grad des Magister Legum Europae (MLE) erworben. Akinci publizierte bereits mehrfach in den Zeitschriften iX und c't und schreibt regelmäßig für die Fachzeitschrift IT-Rechtsberater (ITRB) des Otto Schmidt Verlages.

Joerg Heidrich ist Justiziar und Datenschutzbeauftragter des Heise Verlags in Hannover. Bereits seit 1997 beschäftigt er sich mit den Problemen des Internet- und Datenschutzrechts. Er ist Fachanwalt für IT-Recht, zertifizierter Datenschutzauditor (TÜV) und zertifizierter Datenschutzbeauftragter (TÜV). Heidrich ist Autor zahlreicher Fachbeiträge, unter ande-

rem in den Zeitschriften c't und iX, und Referent zu rechtlichen Aspekten des Datenschutzes sowie Lehrbeauftragter an der Hochschule für Musik, Theater und Medien Hannover.



Nicolas Maekeler ist Syndikusrechtsanwalt und Konzerndatenschutzbeauftragter der Concordia Versicherungen. Daneben ist der hannoversche Jurist als niedergelassener Rechtsanwalt vorrangig in Bereichen des IT- und Da-

tenschutzrechts tätig. Als freier Autor, unter anderem für die Magazine c't, iX sowie heise online, verfasst Maekeler regelmäßig Fachbeiträge zu aktuellen Rechtsthemen der IT-Branche. Er ist zertifizierter Datenschutzbeauftragter (TÜV) gemäß DSGVO und BDSG-neu.

Niklas Mühleis ist Rechtsreferendar beim Land Niedersachsen und wissenschaftlicher Mitarbeiter in der Kanzlei Heidrich Rechtsanwälte in Hannover. Im Anschluss an das erste juristische Staatsexamen vertiefte er seine Kenntnisse in den Bereichen des geistigen Eigentums und des Datenschutzes. Hierzu absolvierte er einen Master of Laws und studierte

unter anderem an der Strathclyde University in Glasgow. Mühleis schreibt Artikel für die Zeitschrift c't, den Blog netzrechtliches.org und das Mittelstandswiki.



Brian Scheuch ist Rechtsanwalt und Partner der Kanzlei Heidrich Rechtsanwälte. Er absolvierte sein Studium der Rechtswissenschaften an den Universitäten Leipzig und Hannover. Sein Schwerpunkt

lag dabei auf den Gebieten IT-Recht, Datenschutzrecht und Urheberrecht. Als Autor schreibt er regelmäßig für die Zeitschrift c't, den Newsticker heise online sowie für die Fachzeitschrift IT-Rechtsberater (itr) des Otto Schmidt Verlages.

Was war, was wird?

2021

Gut zweieinhalb Jahre nach Inkrafttreten der DSGVO hat sich der Pulvernebel der Anfangszeit gelichtet. Trotzdem war die DSGVO weiterhin Thema, man denke nur an die Corona-App oder den Streit um die Nutzung von Videokonferenzplattformen. Was war 2020 wichtig und was wird uns dieses Jahr in Sachen Datenschutz beschäftigen? Ein Überblick.

Von Joerg Heidrich

Das Jahr 2020 wird als das Jahr der Corona-Pandemie in die Geschichte der Menschheit eingehen. Im Datenschutz wurde Mitte des Jahres öffentlich besonders heftig diskutiert, wie man mit den hochgradig sensiblen Informationen in der Corona-App umgehen soll und darf. Überraschenderweise hat man sich dabei auf eine höchst datenschutzfreundliche Version geeinigt, was sicherlich auch sehr zu dem vergleichsweise hohen Verbreitungsgrad der App in Deutschland beigetragen hat.

Datenschutz in Pandemie-Zeiten

Dem ebenso wichtigen Thema Datenschutz im Homeoffice haben wir ein eigenes Kapitel inklusive einer eigenen FAQ gewidmet. Für viele Beschäftigte existenziell ist die Frage nach der Gesundheitskontrolle am Arbeitsplatz (siehe Seite 106). Höchst umstritten ist auch, welcher der vielen Anbieter von Videokonferenzen eigentlich gemäß DSGVO rechtskonform ist (mehr dazu ab Seite 98).

Besonders relevant ist nicht nur im Homeoffice die Frage nach der Überwachung von Mitarbeitern. Die sensiblen Interessen der Beschäftigten kollidieren hier bisweilen mit Pflichten des Arbeitgebers, etwa aus dem Bereich IT-Sicherheit, Compliance oder Betrugsverbeugung. Jedoch lässt

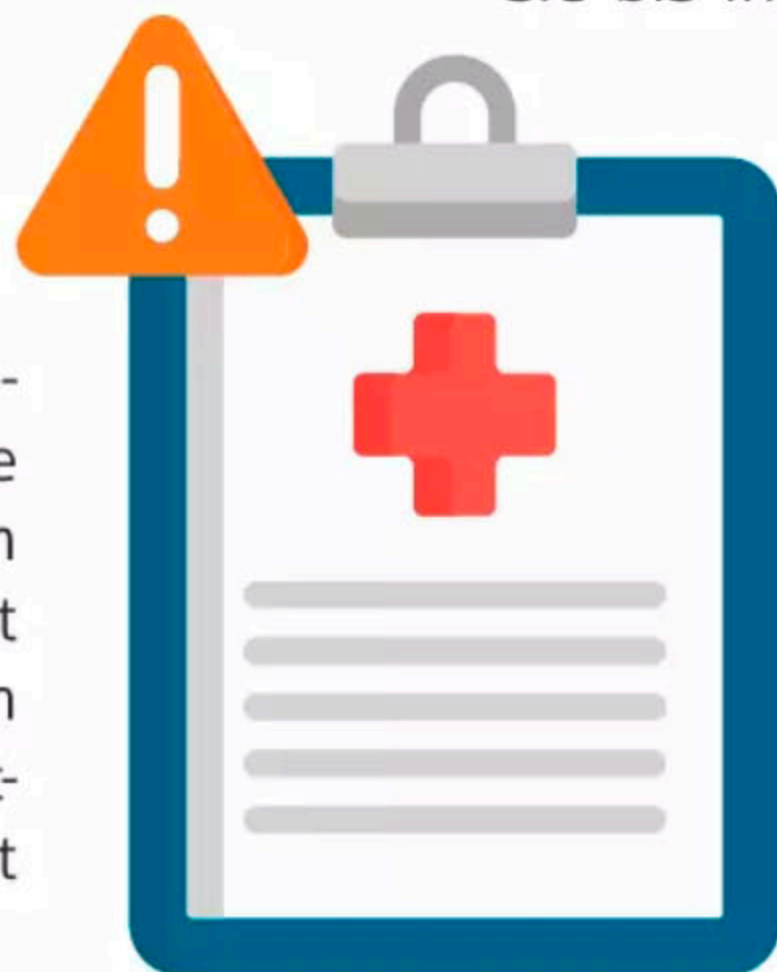
das hiesige Recht, im Gegensatz etwa zu dem der USA, eine Überwachung meist nur sehr eingeschränkt zu. Details dazu finden Sie ab Seite 92.

Teure Bußgelder

So kommt das bislang höchste der hierzulande verhängten Bußgelder auch aus dem Bereich der Mitarbeiterüberwachung. Betroffen waren mehrere hundert Beschäftigte beim deutschen Kundencenter des Bekleidungsunternehmens Hennes & Mauritz (H&M) in Nürnberg. Ihre Vorgesetzten überwachten sie bis in privateste Lebensumstände hinein und speicherten die Ergebnisse dieser Überwachung inklusive Krankheitssymptomen und Diagnosen dauerhaft.

Diese Totalüberwachung brachte H&M 2020 nicht nur den „Big Brother Award“ in der Kategorie Arbeitswelt ein. Anfang Oktober 2020 verhängte der Hamburgische Beauftragte für Datenschutz Johannes Caspar ein Bußgeld in Höhe von 35.258.707,95 Euro – die höchste bislang in Deutschland für Datenschutzverstöße geforderte Summe.

Doch das war nicht das einzige hohe Bußgeld, welches seit Beginn der DSGVO für Aufsehen sorgte. Ein Überblick über die Grundlagen solcher Geldstrafen findet sich ab Seite 60, gefolgt von einer Liste der wichtigsten Bußgelder (siehe Seite 62).



IT-Sicherheit als Bestandteil der DSGVO

Sehr hohe Bußgelder für Versäumnisse bei der IT-Sicherheit zeigen deutlich, dass diese nunmehr elementarer Bestandteil des Datenschutzes ist. Dieses gilt insbesondere für Versäumnisse, die zu Hackerangriffen oder Datenverlust führen. Den von der DSGVO geforderten technischen Maßnahmen haben wir ebenfalls ein eigenes Kapitel gewidmet mit Themen wie Risikoanalysen (Seite 128), Löschkonzepte (Seite 136) oder Backup-Strategien (Seite 140).

Bei Datenpannen bestehen bereits für vergleichsweise geringfügige Fehler wie das Versenden einer E-Mail an die falsche Person oder den Verlust eines Smartphones oder eines USB-Sticks sehr kurzfristige Meldepflichten. Über katastrophale Datenpannen oder Angriffe auf die eigene Infrastruktur muss die jeweilig zuständige Landesdatenschutzbehörde innerhalb von nur 72 Stunden nicht nur informiert werden. Auch die voraussichtlichen Auswirkungen der Datenpanne müssen ebenso dargelegt werden wie die ergriffenen Gegenmaßnahmen. Was dabei als „erste Hilfe“ zu beachten ist, erfahren Sie ab Seite 144.

Cookie-Banner überall!

Eine der von eigentlich allen Seiten eher ungeliebten Auswirkungen der DSGVO ist die Einführung der Cookie-Banner, die inzwischen eher Consent-Management-Systeme sind. Die Anforderungen, die hier von den Behörden an die Betreiber von Online-Angeboten gestellt werden, sind hoch, die Verbraucher zu Recht kritisch. Hinzu kommen Branchenstandards für Online-Werbung, was die Komplexität solcher Systeme noch einmal erhöht. Was bei Aufbau und Betrieb derartiger Banner wichtig ist, erläutern wir ausführlich in einem Artikel und einer umfangreichen FAQ (siehe Seite 158, 162).

Datentransfer in die USA

Die folgenschwerste Gerichtsentscheidung des Jahres 2020 war unzweifelhaft das Schrems-II-Urteil



des Europäischen Gerichtshofs (EuGH). Dieser erklärte quasi über Nacht die allerwichtigste Rechtsgrundlage für den Verkehr von Daten über den Atlantik für unwirksam. Die Folgen sind nicht nur für jedes Unternehmen, sondern auch für Verbraucher enorm.

Was zukünftig bei der Übermittlung personenbezogener Daten in die USA, aber auch in andere Drittstaaten zu beachten ist, erklären wir ebenfalls in einem eigenen Kapitel ab Seite 108. Dabei ist auch eine gewisse Kreativität gefragt, denn neben vertraglichen Vereinbarungen fordern die Gerichte und die Datenschutzbehörden auch zusätzliche technische und organisatorische Maßnahmen, um die Daten der Europäer vor dem Zugriff allzu neugieriger amerikanischer Stellen zu schützen (mehr dazu ab Seite 116).

Unangenehme Folgen: Der Brexit!

Ganz ähnliche Themen werden sich aller Voraussicht nach 2021 hinsichtlich des Datenexports in das Vereinigte Königreich stellen. Hier hat man mit der EU noch einmal einen Aufschub bis Mitte 2021 erreicht. Findet bis dahin keine Einigung zwischen den beiden Parteien statt, so droht UK ein „unsicherer Drittstaat“ zu werden, für den dann hinsichtlich des Datentransfers die gleichen Anforderungen gelten wie hinsichtlich der USA.

Und Vieles mehr!

Das ist nur ein Ausschnitt aus den Themen unseres 180 Seiten umfassenden Magazins, das natürlich auch die datenschutzrechtlichen Basics ausführlich beschreibt ebenso wie die Rechte der Bürger und die Anforderungen an die Vereine. Ebenso finden Sie alle wichtigen Infos über die Anforderungen an Unternehmen, hinsichtlich der Gestaltung von Websites oder was beim Fotografieren zu beachten ist.

Geballte Informationen zu den Themen US-Transfer, Datenschutz im Homeoffice und Anforderungen der DSGVO an die IT-Sicherheit liefern Ihnen die drei Heise-Webinare, die wir auf der DVD zu diesem Sonderheft beigelegt haben (siehe Seite 176).

(anm) **ct**



DSGVO

Das sollten Sie wissen

Mit der DSGVO hat sich im Datenschutz vieles geändert, vieles aber auch nicht. Nach über zwei Jahren der Anwendung zeichnet sich nun klarer ab, worauf man im Alltag unbedingt achten muss.

Von Nick Akinci

Mit dem Erscheinen dieses Ratgebers liegen die ersten zweieinhalb Jahre mit der europäischen Datenschutz-Grundverordnung (DSGVO) hinter uns. Noch immer werden viele strittige Details zur Auslegung der Verordnung heftig diskutiert, da erst nach und nach wegweisende Gerichtsurteile ergehen, die sich mit der Auslegung der Normen beschäftigen. Trotzdem haben wir in der praktischen Umsetzung bereits viel dazugelernt und können für das Jahr 2021 besser einschätzen, was wichtig wird und was nicht.

Was Sie über die DSGVO erfahren

Das vorliegende Magazin vermittelt Unternehmen wie Privatpersonen das wichtigste Wissen über die DSGVO in einfacher und strukturierter Form und dient gleichzeitig als Nachschlagewerk für konkrete Probleme. Dabei beleuchten wir die Rechte der Bürger, die Pflichten von Unternehmen und die techni-

schen Aspekte des Datenschutzes. Darüber hinaus geben wir Ihnen Lösungen an die Hand, die den rechtssicheren Umgang mit personenbezogenen Daten vereinfachen. Dabei haben wir stets alle aktuellen Entwicklungen berücksichtigt.

Was ist eigentlich die DSGVO?

Bei der DSGVO handelt es sich um eine vom europäischen Gesetzgeber erlassene Verordnung. Zwar war diese bereits am 25. Mai 2016 in Kraft getreten – wirksam wurden die neuen Regelungen jedoch erst zwei Jahre später, am 25. Mai 2018. Im Unterschied zu seinem Vorgänger, der europäischen Datenschutz-Richtlinie aus dem Jahre 1995, ist eine EU-Verordnung direkt in allen Mitgliedsstaaten der Europäischen Union anwendbar. Daher kann sich nun beispielsweise jeder Bürger direkt auf die Rechte berufen, die ihm nach der DSGVO zustehen, und muss nicht erst auf eine nationalstaatliche Um-

setzung warten. Vereinzelt enthält die Verordnung jedoch auch Öffnungsklauseln, die dem nationalen Gesetzgeber die Möglichkeit geben, bestimmte Details in eigenen Gesetzen zu regeln. Solche länderspezifischen Vorschriften sind in der Bundesrepublik im neuen Bundesdatenschutzgesetz (BDSG-neu) zu finden, das ebenfalls am 25. Mai 2018 wirksam wurde.

Was war vor der DSGVO?

Aufgrund der großen Spielräume, die die Datenschutz-Richtlinie den Gesetzgebern in den einzelnen europäischen Ländern bei der Umsetzung einräumte, bestanden teils gravierende Unterschiede hinsichtlich des Datenschutzniveaus. Unternehmen flüchteten regelmäßig vor strengeren Datenschutzregimen, indem sie ihren Hauptgeschäftssitz in Länder verlegten, in denen die Anforderungen an den Datenschutz besonders niedrig waren, beziehungsweise in denen Rechtsbrüche selten verfolgt wurden. So unterhielten beispielsweise Social-Media-Größen wie Facebook, Twitter und LinkedIn ihre europäische Niederlassung in Irland, wo die zentrale Aufsichtsbehörde gerade einmal 30 Mitarbeiter vorhielt, um die Rechte von Millionen von europäischen Nutzern zu schützen.

Die DSGVO vereinheitlicht nun das Datenschutzrecht im Sinne einer Vollharmonisierung europaweit und sorgt damit im Idealfall dafür, dass in der gesamten Europäischen Union ein einheitliches Datenschutzniveau herrscht. Dabei wird der Datenschutz auf ein hohes Niveau angehoben, das in etwa dem entspricht, das in Deutschland schon seit längerer Zeit herrscht. Abgesehen von der Erhöhung des Datenschutzniveaus in vielen Ländern bietet die Verordnung aber auch den großen Vorteil, dass sowohl für Unternehmen als auch für Privatpersonen und Verbraucher europaweit einheitliche Regeln gelten, womit eine enorm große Transparenz erreicht wird.

Die wichtigsten Neuerungen auf den Punkt gebracht

Eine der vielleicht wichtigsten Neuerungen, die die DSGVO mit sich bringt, sind die deutlich gestiegenen und nunmehr abschließend geregelten Informationspflichten bei der Datenverarbeitung. So

sind die von der Verarbeitung betroffenen Personen beispielsweise darüber zu informieren, welche Daten zu welchem Zweck verarbeitet und wie lange diese gespeichert werden. Selbstverständlich muss aber nicht jeder, der irgendwie Daten verarbeitet, hierüber informieren. Über den Anwendungsbereich der DSGVO erfahren Sie mehr im nachfolgenden Artikel (siehe S. 12) „Gilt die DSGVO auch für mich?“. Wichtige Begrifflichkeiten erläutern wir im Artikel „Grundsätze des Datenschutzrechts“ ab Seite 16.

Auch die qualitativen Anforderungen an die Informationspflichten wurden deutlich angehoben. Die Verordnung legt hier großen Wert auf Verständlichkeit und Transparenz. Was dies bedeutet, erklären wir im Kapitel „Pflichten für Unternehmen“ ab Seite 46.

Mit der DSGVO legt der Gesetzgeber weiterhin erstmals auch einen Schwerpunkt auf das Thema technischer Datenschutz. Mit den nun eingeführten Begriffen *Privacy by Design* und *Privacy by Default* widmet sich die Verordnung auch der technischen Umsetzung von datenschutzrelevanten Vorhaben und Projekten. Mehr hierzu erfahren Sie ab Seite 124.

Bei den Bürgerrechten hält die DSGVO ebenfalls einige Neuerungen bereit. So führt die Verordnung zum Beispiel das Recht auf Datenübertragbarkeit und das Recht auf Vergessenwerden ein. Ihre erweiterten Rechte lernen Sie ab Seite 38 kennen.

Eine deutliche Veränderung haben schließlich noch die Sanktionen erfahren, die verhängt werden können, um Datenschutzverstöße zu ahnden. Nachdem Bußgelder nach den bisherigen Regelungen maximal 300.000 Euro pro Einzelfall betragen durften, sind nun Bußgelder in Höhe von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes eines Unternehmens möglich, je nachdem, was höher ist. Details zu Bußgeldern, Abmahnungen und Schadensersatz stellen wir Ihnen im Artikel ab Seite 60 vor.

(keh) **ct**



Gesetzestexte

ct.de/wmu6

Gilt die DSGVO auch für mich?



Nicht jede Datenverarbeitung ist ein Fall für die Regelungen der DSGVO. Das Gesetz gilt nur für bestimmte Anwendungsbereiche und Personenkreise.

Von Nick Akinci

Die Frage, ob man die gesetzlichen Vorgaben der DSGVO zu beachten hat, hängt maßgeblich von zwei Voraussetzungen ab. Werden überhaupt personenbezogene Daten verarbeitet? Nur dann ist der sachliche Anwendungsbereich der Verordnung betroffen. Zum anderen muss der persönliche Anwendungsbereich gelten, das heißt: Man muss zum Kreis der (juristischen) Personen gehören, an die sich die gesetzlichen Bestimmungen richten.

Personenbezogene Daten

Die DSGVO definiert personenbezogene Daten in Artikel 4 als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“. Damit ist gemeint, dass die infrage stehende Information einer bestimmten natürlichen Person zugeordnet werden kann. Dies lässt sich am besten anhand von ein paar Beispielen erklären: siehe rechte Spalte. Weitere Beispiele für personenbezogene Daten finden Sie im Kasten auf der nächsten Seite.

Datenverarbeitung

Damit die DSGVO Anwendung findet, muss es sich gemäß Artikel 2 um eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten handeln. Darüber hinaus sind auch nichtautomatisierte Verarbeitungsvorgänge betroffen, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Vor- & Nachname

Die Kombination aus Vor- und Nachnamen lässt sich – je nach Kontext – in den allermeisten Fällen einer bestimmten Person zuordnen und stellt daher ein personenbezogenes Datum dar.

E-Mail-Adresse

Eine E-Mail-Adresse stellt für sich genommen nicht zwingend ein personenbezogenes Datum dar.

Dies ist nur dann der Fall, wenn die Adresse selbst Aufschluss über den Adressinhaber gibt, wie etwa bei jens.mueller@maildienst.com.

Die E-Mail-Adresse info@unternehmensname.de ist hingegen keiner bestimmten Person zuordenbar.

Aussage

Die Information „Jens Müller liest gerne Romane“ ist ebenso als personenbezogenes Datum einzuordnen, wie die Information „Jens Müller ist am 15.04.2018 Vater geworden“.

Als automatisiert können letzten Endes alle computerbasierten Datenverarbeitungsvorgänge begriffen werden. Außerhalb des digitalen Bereichs – also nicht automatisiert – werden aber auch analoge Datensammlungen erfasst, die in einem Dateisystem gespeichert sind. Darunter fallen all diejenigen Datensammlungen, die strukturiert und nach bestimmten Kriterien zugänglich sind.

Datensammlungen

Werden Visitenkarten in einer Rollkartei abgelegt und alphabetisch sortiert, dürfte das Merkmal des Dateisystems erfüllt sein.

Liegen die Visitenkarten nur „lose“ und ohne Sortierung in der Schublade, so kann nicht von einem Dateisystem gesprochen werden.

Sind die Kontaktdaten zusätzlich auf dem Computer – sei es nur in einer E-Mail-Signatur – gespeichert, so liegt eine automatisierte Verarbeitung vor.

Persönlich betroffen

Die Verordnung gilt vom Grundsatz her erst einmal für jeden, das heißt sowohl für Einzelpersonen, Unternehmen und sonstige Organisationen. Es gibt aber auch einige Ausnahmen hiervon.

Die wichtigste Ausnahme ist das Haushaltsprivileg: Handelt eine Privatperson im rein persönlichen oder familiären Bereich, so muss die DSGVO nicht beachtet werden. Das Speichern der E-Mail-Adressen von Freunden auf dem heimischen Computer ist daher selbstverständlich nicht der DSGVO unterworfen.

Im Übrigen ist die Grenze des persönlichen und familiären Bereichs jedoch nur schwer abzustecken. Er endet aber jedenfalls dort, wo ein Bezug zur beruflichen oder wirtschaftlichen Tätigkeit der verarbeitenden Person besteht. Darüber hinaus hat der Europäische Gerichtshof (EuGH) entschieden, dass eine Videoüberwachungskamera an einem Privatgrundstück, die auch den öffentlichen Bereich – wie den

Gehweg – erfasst, dem Datenschutz unterfällt (EuGH, Urteil vom 11.12.2014, Az.: C-212/13). Weiterhin soll laut dem EuGH die Haushaltsausnahme auch dann nicht greifen, wenn personenbezogene Daten im Internet so veröffentlicht werden, dass sie für eine unbegrenzte Anzahl von Personen zugänglich sind (EuGH, Urteil vom 14.02.2019, Az.: C-345/17). Das bedeutet jedoch nicht, dass die DSGVO im Internet grundsätzlich Anwendung findet.

Da der Gesetzgeber mit dem Haushaltsprivileg auch die Nutzung von sozialen Netzwerken im Auge hatte, gilt dieses jedenfalls auch für das Posten von personenbezogenen Daten in geschlossenen Nutzergruppen beispielsweise bei Facebook.

In Artikel 2 der DSGVO finden sich weitere Ausnahmen wie die Datenverarbeitung durch die Strafverfolgungsbehörden, auf die hier aber nicht näher eingegangen werden soll.

- Telefonnummer, E-Mail Adresse, IP-Adresse
- KFZ-Kennzeichen
- Kontonummer
- Bild einer Person
- Unterschrift
- Werturteile (z.B. Zeugnisse)
- Positionsdaten
- Matrikelnummer
- Kaufverhalten
- Aufzeichnung von Arbeitszeiten



Beispiele: personenbezogene Daten



Datenverarbeitung

? Was versteht man eigentlich unter „Verarbeitung“ von Daten?

! Ganz egal, was Sie mit personenbezogenen Daten machen, es wird sich (fast) immer um eine Verarbeitung im Sinne der DSGVO handeln. Ob Sie die Daten erheben, speichern, ändern, nutzen oder übermitteln – all dies fällt unter den Begriff der Verarbeitung. Auch das Löschen oder Vernichten von Daten ist hierunter zu verstehen. Unter der Nennung weiterer Beispiele wird in Art. 4 DSGVO definiert: Eine Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten.

Nicht nur für Unternehmen

? Fallen auch einzelne Selbstständige, Vereine oder Stiftungen in den Anwendungsbereich der DSGVO?

! Ja. Die DSGVO macht hier keine Unterschiede, sondern gilt einheitlich für Einzelpersonen und alle Formen von Organisationen. Sie alle müssen die gleichen Pflichten erfüllen, ob einzelne Selbstständige, kleine Unternehmen oder Großkonzerne. Für Selbstständige und kleinere Organisationen hält sich aber der Aufwand, um den Datenschutzbestimmungen gerecht zu werden, regelmäßig in Grenzen. Der Grund: Es werden ohnehin weniger Daten verarbeitet und die Strukturen sind meist einfacher als in größeren Unternehmen. Eine Privilegierung kleinerer Unternehmen sieht das neue europäische Datenschutzrecht nicht vor.



IP-Adressen

? Sind IP-Adressen personenbezogene Daten?

! Eine IP-Adresse kann man zwar für sich genommen nicht einer bestimmten Person zuordnen, da sich zum einen unmittelbar aus der Ziffernfolge nichts ableiten lässt und zum anderen IP-Adressen meist ständig neu vergeben werden. Die Strafverfolgungsbehörden zum Beispiel haben aber die Möglichkeit, über den Access-Provider herauszufinden, welchem Internetanschluss die IP-Adresse zum Zeitpunkt des Zugriffs zugeordnet war und wer Inhaber dieses Anschlusses ist. In der höchstgerichtlichen Rechtsprechung ist daher anerkannt, dass auch eine IP-Adresse ein personenbezogenes Datum darstellt. In der DSGVO ist dies nunmehr auch konkret geregelt. IP-Adressen gelten als „Online-Kennung“ und sind, so wie Cookie-Kennungen auch, als personenbezogen anzusehen.

Pseudonym oder anonym

? Was sind die Unterschiede von pseudonymisierten & anonymisierten Daten?

! Unter anonymisierten Daten versteht man Angaben über eine Person, die so verändert wurden, dass diese keiner bestimmten Person mehr zugeordnet werden können. Eine IP-Adresse lässt sich zum Beispiel dadurch anonymisieren, dass die letzten drei Ziffern gelöscht werden, da ohne diese kein Rückschluss mehr auf den Anschluss und die dahinterstehende Person möglich ist.

Die Pseudonymisierung hat zwar ebenfalls das Ziel, dass die Daten keiner bestimmten Person mehr zugeordnet werden können, sie kann aber – im Gegensatz zur Anonymisierung – theoretisch wieder rückgängig gemacht werden. Eine Pseudonymisierung liegt beispielsweise vor, wenn einem Kunden anstelle seines Namens und seiner Adresse eine Ziffernfolge (ID) zugewiesen wird und der eigentliche Datensatz davon getrennt aufbewahrt wird. Im Gegensatz zu anonymen Daten sind beim Vorliegen pseudonymer Daten die Vorschriften der DSGVO zu beachten. (keh) **ct**

NEU
im heise shop

[illegible]

14,90 € >

Awareness: Es mangelt an Gefahrenbewusstsein

Risikofaktor Mensch

shop.heise.de/ix-sicherheit20 ➤

➤ Generell portofreie Lieferung für Heiße Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

Grundsätze des Datenschutzrechts

Einigen grundlegenden Prinzipien zum Umgang mit personenbezogenen Daten begegnet man im Datenschutzrecht immer wieder. Auf ihnen bauen alle gesetzlichen Regelungen auf.

Von Nick Akinci

Um die DSGVO und die darin enthaltenen Anforderungen an den Datenschutz (besser) zu verstehen, ist es hilfreich, zunächst die grundlegenden Prinzipien des Datenschutzrechts kennenzulernen. Diese sind zentral in Artikel 5 der DSGVO geregelt. In diesem Artikel finden sich Grundsätze wie das Verbot mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz, der Grundsatz der Datenminimierung sowie die beiden eng miteinander verknüpften Prinzipien Privacy by Design und Privacy by Default. Darüber hinaus ist es auch wichtig zu unterscheiden, welche Arten von personenbezogenen Daten es gibt.

Verbot mit Erlaubnisvorbehalt

Der Grundsatz des Verbots mit Erlaubnisvorbehalt ist der zentrale Grundsatz des Datenschutzrechts. Er galt bereits vor Inkrafttreten der DSGVO und besagt: Jegliche Verarbeitung von personenbezogenen Daten ist grundsätzlich erst einmal verboten, es sei denn, das Gesetz erlaubt dies ausdrücklich. Dies mag vielleicht zunächst überraschen, ist jedoch sinnvoll angesichts des Ziels des Datenschutzes, die Persönlichkeitsrechte des Einzelnen zu schützen. Jede Datenverarbeitung muss daher auf eine Rechtsgrundlage gestützt werden, also eine gesetzliche Regelung, die es unter gewissen Voraussetzungen explizit erlaubt, dass personenbezogene Daten verarbeitet werden dürfen. Eine Auflistung der wichtigsten Rechtsgrundlagen findet sich in Artikel 6 der DSGVO – jedoch existieren auch weitere in- und außerhalb der DSGVO.

Rechtsgrundlagen für die Erlaubnis

Insbesondere rund um den 25. Mai 2018 las man vielfach davon, dass unter der DSGVO fortan immer eine Einwilligung für beabsichtigte Datenverarbeitungen einzuholen sei. Dies ist schlicht falsch. Zwar bildet die Einwilligung eine der drei wichtigsten Rechtsgrundlagen der DSGVO. Daneben lassen sich Verarbeitungen aber insbesondere auf die Erfüllung eines mit dem Betroffenen geschlossenen Vertrags und auf die berechtigten Interessen der datenverarbeitenden Stelle stützen.

Zunächst darf der Verantwortliche im Rahmen von Vertragsverhältnissen, die zur Durchführung dieser Verträge erforderlichen Datenverarbeitungen vornehmen. Datenschutzrechtlich unproblematisch ist daher insbesondere die Speicherung des Namens und der Anschrift eines Vertragspartners. Beim Betrieb eines Online-Shops darf man deshalb die E-Mail-Adresse und die Zahlungsdaten des Kunden auf dieser Rechtsgrundlage speichern. Ein anderes Ergebnis dürfte auch dem gesunden Menschenverstand widersprechen, da es in der Natur einer Online-Bestellung liegt, dass diese Daten benötigt werden. Eindeutig nicht zur Erfüllung des Vertrags erforderlich wäre dagegen beispielsweise die Verwendung dieser Daten zu Werbezwecken.

Sind die infrage stehenden Datenverarbeitungen nicht zur Erfüllung eines Vertrages erforderlich, so stellt die Einwilligung der Betroffenen die wichtigste Rechtsgrundlage für den Verantwortlichen dar, da die Datenverarbeitung dem Willen des Betroffenen entspricht und die Voraussetzungen wenig Ausle-

gungsspielraum bieten. Trotzdem ist die Einholung einer Einwilligung des Betroffenen nicht trivial. Diese muss insbesondere freiwillig, das heißt ohne äußeren Zwang erfolgen.

Dieses Erfordernis mündet zum einen im Kopplungsverbot: Der Datenerhebende darf eine bestimmte Leistung nicht von der Einwilligung des Betroffenen abhängig machen. Ein Online-Shop, der einen Kauf nur dann zulässt, wenn der Kunde der Weitergabe seiner Daten an Dritte zustimmt, würde daher rechtswidrig handeln.

Das Merkmal der Freiwilligkeit muss aber auch dann genauer betrachtet werden, wenn die Einwilligung im Rahmen eines Über-/Unterordnungsverhältnisses eingeholt werden soll, das heißt, wenn

ein besonders großer wirtschaftlicher oder sozialer Unterschied zwischen den Betroffenen und dem Verantwortlichen besteht.

Bei der Einwilligung muss der Verantwortliche darüber hinaus im Zweifel durch entsprechende Dokumentation nachweisen können, dass sie tatsächlich eingeholt wurde. Bei Online-Einwilligungen, beispielsweise bei Newsletter-Abos, macht es daher Sinn, mit einem Double-Opt-In-Verfahren zu arbeiten: Setzt der Kunde beziehungsweise Nutzer das „Einwilligungshäkchen“, wird er in einer nachfolgenden E-Mail nochmals zur Bestätigung seiner Einwilligung aufgefordert. Im Kasten unten wird das Double-Opt-In-Verfahren anhand des [heise.de-Newsletters](https://www.heise.de/Newsletters) verdeutlicht.

Online-Einwilligung als Double-Opt-In

1. Erstes Opt-In auf der Website

Ich willige ein, dass mich Heise Medien per E-Mail über die von ihr angebotenen Zeitschriften, Online-Angebote, Produkte des heise Shops, Veranstaltungen und Software-Downloads informiert. Meine Daten werden ausschließlich zu diesem Zweck genutzt. Eine Weitergabe an Dritte erfolgt nicht. Ich kann die Einwilligung jederzeit per E-Mail an datenservice@heise.de, per Brief an Heise Medien GmbH & Co. KG, Vertrieb & Marketing, Karl-Wiechert-Allee 10, 30625 Hannover oder durch Nutzung des in den E-Mails enthaltenen Abmeldelinks widerrufen. Es gilt die [Datenschutzerklärung](#) von Heise Medien.

Anmelden

2. Hinweis auf die Bestätigungs-E-Mail



Ihre Anmeldung für den Newsletter heise online Top-Newsletter aktivieren Sie bitte über den Link in Ihrer Bestätigungs-E-Mail.

Zur Startseite

3. Zweites Opt-In in der Bestätigungs-E-Mail

Guten Tag,

Sie haben auf unserer Website <http://www.heise.de/> den E-Mail-Newsletter **heise online Top-Newsletter** angefordert.

Newsletter Bestellung bestätigen

Die Einholung einer Einwilligung ist jedoch nicht immer praktikabel und teilweise sogar unmöglich. So kann zum Beispiel der Betreiber von öffentlichen U-Bahn-Stationen unmöglich die Einwilligung aller Fahrgäste einholen, diese filmen zu dürfen.

Ein weiteres Problem stellt das Erfordernis der informierten Einwilligung dar. Der Betroffene muss zum Zeitpunkt der Abgabe der Einwilligung ausreichend über die Datenverarbeitungen, denen er zustimmen soll, informiert sein. Er soll vollständig im Bilde darüber sein, was mit seinen Daten geschieht, um auf dieser Grundlage seine Entscheidung treffen zu können. Vage Angaben wie etwa „Ihre Daten werden zur Bereitstellung unseres Dienstes verarbeitet“ reichen nicht aus. Insbesondere bei komplexen Online-Diensten wie Social-Media-Plattformen ist eine informierte Einwilligung oft kaum möglich. Die Datenverarbeitungsstrukturen solcher Dienste sind in der Regel so komplex, dass sie vom Nutzer nicht oder nur unter großem Aufwand erfasst werden können.

In solchen Konstellationen können Datenverarbeitungen mitunter auf die berechtigten Interessen des Datenerhebenden gestützt werden. Voraussetzung ist aber nicht nur, dass die Interessen des Verantwortlichen berechtigt, also in gewisser Weise schützenswert sind. Es muss weiterhin eine gründliche Abwägung mit den schutzwürdigen Interessen und Rechten der Betroffenen vorgenommen werden. Hat diese Abwägung zum Ergebnis, dass die Interessen der Betroffenen nicht überwiegen, so kann die Datenverarbeitung auf die berechtigten Interessen gestützt werden und ist damit rechtmäßig.

Diese Abwägung ist in den meisten Fällen jedoch alles andere als trivial und kann daher große Unsicherheiten mit sich bringen. In der Regel sollte daher das Ergebnis der Abwägung durch einen Rechtsanwalt überprüft werden. Bei manchen Szenarien sind sich Juristen jedoch darüber einig, dass das berechtigte Interesse der datenverarbeitenden Stelle in der Regel überwiegen dürfte. Zum Beispiel steht es den Rechten und Interessen der Betroffenen in der Regel nicht entgegen, wenn Kundendaten nach der Erhebung innerhalb eines Konzerns an andere konzernangehörige Unternehmen weitergegeben werden. Weiterhin dürften die Betroffeneninteressen auch dann nicht überwiegen, wenn diese im öffentlichen Raum – etwa vor einem Bargeldautomaten – von einer Videokamera erfasst werden, die dazu dient, Straftäter abzuschrecken oder diese gegebenenfalls zu verfolgen.

Zweckbindungsgrundsatz

Der Zweckbindungsgrundsatz dürfte, neben dem eingangs erläuterten Grundsatz des Verbots mit Erlaubnisvorbehalt, das zweitwichtigste Grundprinzip des Datenschutzes darstellen. Auch dieser Grundsatz war bereits lange vor Inkrafttreten der DSGVO fest im Datenschutzrecht verankert. Er besagt, dass man die Zwecke der Verarbeitung bereits vor deren Beginn festlegen muss. Eine nachträgliche Verarbeitung zu anderen Zwecken als dem ursprünglich festgelegten ist unrechtmäßig. So dürfen eben beispielsweise IP-Adressen, die aus Gründen der IT-Sicherheit im Rahmen von Logfiles erhoben wurden, nicht für Werbung genutzt werden.

Damit wird beabsichtigt, dass der Betroffene stets Kenntnis darüber hat, was mit den ihn betreffenden Daten geschieht. Eng mit dem Zweckbindungsgrundsatz verknüpft ist daher auch die Pflicht des Datenverarbeitenden, den Betroffenen bereits vor Beginn der geplanten Verarbeitungen über die damit verfolgten Zwecke zu informieren. Wie Sie Ihre Informationspflichten mit der Datenschutzerklärung erfüllen können, erfahren Sie ab Seite 46.

Der Zweckbindungsgrundsatz ist besonders im Zusammenhang mit Big-Data-Prozessen immer wieder heftig diskutiert worden. Big-Data-Prozessen ist es immanent, dass der ursprüngliche Erhebungszweck nachträglich geändert wird, wenn Daten aus verschiedenen Quellen zusammengeführt und analysiert werden. Unter Juristen wird jedoch teils die Meinung vertreten, dass Big-Data-Prozesse jedenfalls dann rechtmäßig sein können, wenn die dadurch aggregierten Datensätze keinen Personenbezug mehr aufweisen und gewährleistet wird, dass dieser auch nachträglich nicht mehr hergestellt werden kann.

Grundsatz der Datenminimierung

Ein weiterer zentraler Grundsatz des Datenschutzrechts ist die Datenminimierung. Der Gesetzgeber spricht in Artikel 5 davon, dass die Datenverarbeitungen „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“ sein sollen. Die Einhaltung des Datenminimierungsgrundsatzes gewährleistet man auf verschiedene Arten und Weisen.

Zunächst sollte bereits bei der Erhebung der Daten darauf geachtet werden, dass man ausschließlich die tatsächlich für die Verarbeitungs-



zwecke notwendigen Daten abfragt. Ein simples Beispiel hierfür ist das Kontaktformular auf einer Website: Wird die Anfrage vom Website-Betreiber ohnehin per E-Mail beantwortet, braucht er Daten wie die Telefonnummer oder die Anschrift des Anfragenden nicht zur Verwirklichung des (jedenfalls zunächst) ausschließlichen Erhebungszwecks „Bearbeitung und Beantwortung der Anfrage“.

Nach der Erhebung von personenbezogenen Daten gewährleistet man die Datenminimierung insbesondere durch Anonymisierung oder Pseudonymisierung. So sollte man zum Beispiel bei Analysetools zur Reichweitenmessung im Onlinebereich stets die erhobene IP-Adresse kürzen und damit anonymisieren. Ein Pseudonymisierungsverfahren macht dagegen Sinn, wenn man die Klardaten nicht für alle geplanten Zwecke benötigt. Ein gängiges Beispiel hierfür ist die Erstellung von Käuferprofilen durch größere Unternehmen, um gezielt Werbung auszusteuern. Hier müssen die Klardaten der einzelnen Käufer, beispielsweise Name und Anschrift, zunächst durch eine pseudonyme ID ersetzt werden, bevor sie mit anderen Daten, etwa Alter und Postleitzahl, zu einem Profildatensatz zusammengefügt werden.

Dem Grundsatz der Datenminimierung entspringt auch das Prinzip der Speicherbegrenzung, wonach Daten nicht länger verarbeitet werden sollen als unbedingt für den Zweck erforderlich. Sollte in dem oben erwähnten Beispiel einer Anfrage über das Kontaktformular diese abschließend beantwortet sein und außer der Beantwortung der Anfrage keine Verarbeitungsgrundlage bestehen, so sollten die in diesem Rahmen erhobenen personenbezogenen Daten umgehend gelöscht werden.

Privacy by Design und Privacy by Default

Der Grundsatz *Privacy by Design* kann übersetzt werden als „Datenschutz durch Technikgestaltung“. Gemeint ist damit, dass man bei der Entwicklung von Produkten oder der Vorbereitung von Projekten den Datenschutz bereits bei der Planung berücksichtigt. Beispielsweise sollte man bei größeren Datenbank-Projekten von vorn herein technisch sicherstellen, dass Daten im Bedarfsfall restlos und unter geringem Aufwand gelöscht werden können. *Privacy by Default* meint hingegen die Implementierung datenschutzfreundlicher Voreinstellungen und ist daher eng mit dem Grundsatz der Datenminimierung verknüpft. Durch solche Voreinstellungen kann man zum Beispiel Nutzer von Online-Diensten schützen,

die technisch nicht so versiert sind. So sollte in Browsern möglichst voreingestellt sein, dass Cookies, die das Nutzerverhalten tracken, geblockt werden. Ebenso sollte bei sozialen Netzwerken voreingestellt sein, dass dort eingestellte Inhalte nicht öffentlich, sondern vorzugsweise nur für „Freunde“ sichtbar sind.

Besonders sensible Daten

Ein weiteres wichtiges Prinzip ist die Unterscheidung zwischen normalen personenbezogenen Daten und solchen, die besonders sensibel und damit auch besonders schützenswert sind.

Dabei handelt es sich um Daten, die der Intimsphäre der Betroffenen zuzuordnen sind. Die DSGVO spricht in Artikel 9 von „besonderen Kategorien personenbezogener Daten“ und nennt als solche „Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.“ Der besondere Schutz dieser Informationen ist deshalb notwendig, weil diese ein hohes Risiko für die Persönlichkeitsrechte der Betroffenen darstellen. Besonders sensible Daten können die Grundlage von Diskriminierung bilden.

In gewissen Bereichen ist offensichtlich, dass es sich um sensible Daten handelt, beispielsweise bei einer Patientenakte oder der Angabe von sexuellen Vorlieben. Oftmals fällt aber erst bei genauerem Hinsehen auf, dass bestimmte Dokumente oder Datensätze auch sensible Informationen enthalten oder enthalten können. So kann zum Beispiel eine einfache Lohnabrechnung Auskunft über die Religionszugehörigkeit einer Person geben, wenn dort die Abführung von Kirchensteuer vermerkt ist. Ebenso könnte die Abbuchung eines Vereinsbeitrags auf dem Kontoauszug die politische Gesinnung einer Person erkennen lassen, wenn der Verein entsprechend bekannt ist.

Im Bereich dieser besonderen Art von Daten sind daher vor allem die Anforderungen an die Rechtsgrundlagen wesentlich höher. Die Verarbeitung kann hier nicht auf berechtigte Interessen oder die Durchführung eines Vertrages gestützt werden.

Des Weiteren steigen auch die Anforderungen an die Datensicherheit. Es gilt die Faustformel: Je sensibler ein Datum, desto höher sind die Anforderungen an die zu treffenden Sicherheitsmaßnahmen. (keh) 

23. - 25.
FEBRUAR**2021**

Interessante redaktionelle Keynotes
und Partner-Vorträge

Virtuelle Fachausstellung

Interaktive Breakout-Sessions

Diverse Networking-Optionen

sec-it.heise.de

 Heise Medien

Unsere Partner



Der digitale Treffpunkt für Security-Experten

KEYNOTE:

Avant-Garde InfoSec // Dr. Melanie Rieback

INTERAKTIVE VORTRÄGE:

Einstiegsmöglichkeiten in die Cybersicherheit für KMUs // Viktor Rechel

Anleitung zum Emotet-Selbsttest // Martin Junghans

Cyber-Versicherung: Risikogruppe IT-Betriebe? // Tobias Wenhart

„Behind the Hype: Buzzwords kritisch hinterfragt“ // Stefan Strobel

„Experten-FAQ“ mit Sidekick // Olaf Pursche und Tobias Schrödel

PODIUMSDISKUSSION:

zum Thema Hackback // Andreas Könen, Manuel Atug, Tobias Haar

HEISE SHOW SPEZIAL:

Computer-Forensik – Fakten und Fiktion //

Martin Wundram und Krimiautor Constantin Gillies

Preis: 249,00 € (inkl. MwSt.)

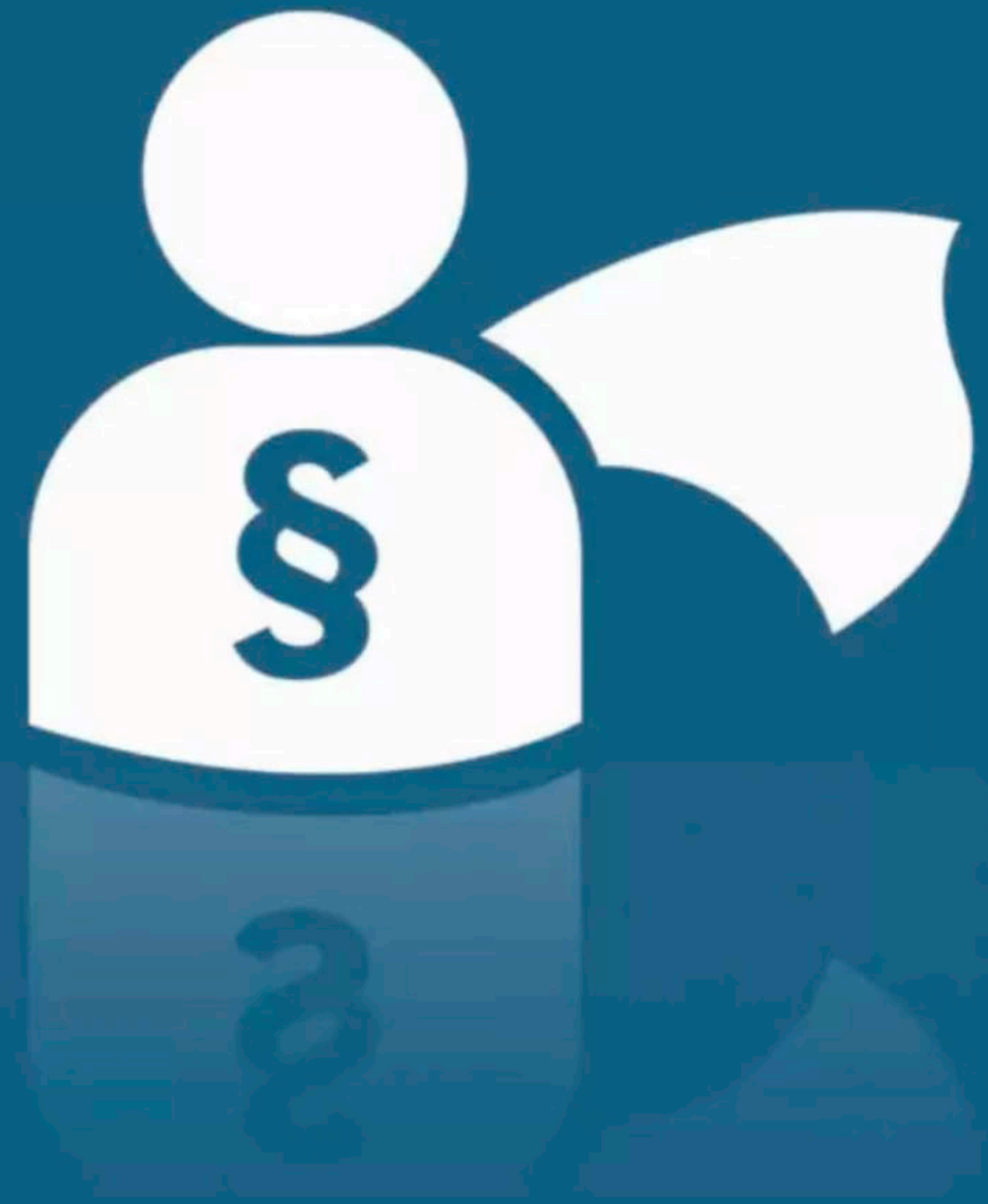
© Gorodenkoff



Mehr Rechte für Bürger

Ein wesentliches Ziel der Datenschutzgrundverordnung ist der Schutz des Einzelnen bei der Verarbeitung personenbezogener Daten. Um diesen zu verbessern, bietet die DSGVO den Bürgerinnen und Bürgern zahlreiche Rechte gegenüber Datenverarbeitern.

Von Niklas Mühleis



Datenschutz bedeutet in erster Linie nicht den Schutz von Daten, sondern es geht um die Stärkung der Persönlichkeitsrechte des Betroffenen. Dies will die DSGVO erreichen durch mehr Pflichten für Unternehmen und mehr Rechte für Bürger.

Transparenz und Verständlichkeit

Zunächst stehen die Gebote der Transparenz und der Verständlichkeit über allem anderen. Verbraucher sollen nachvollziehen können, wer mit ihren Daten hantiert und was mit ihnen geschieht. Die Verantwortlichen für die Datenverarbeitung sind laut Artikel 12 der DSGVO dazu verpflichtet, Nutzer in einer transparenten, verständlichen und leicht zugänglichen Form über die Verarbeitung ihrer Daten zu informieren. Verantwortliche sind beispielsweise Unternehmen, Vereine und andere Organisationen. Diese Informationen dürfen also nicht in einem undurchdringlichen Wust sonstiger Hinweise versteckt oder in komplizierte Schachtel- und Negativsätze gepackt sein, deren Sinn sich kaum erschließen lässt. Ausdrücklich von der Verordnung gefordert ist eine klare und einfache Sprache.

Hier zeigt sich einer der großen Haken der DSGVO. Betroffene sollen umfassend informiert werden, dies jedoch in verständlicher Form. Die Verständlichkeit findet meist schon beim Besuch jeder x-beliebigen Website ihr Ende. Endlose Datenschutzerklärungen, mehrstufig verschachtelte Cookie-Banner

und bewusst trocken gehaltene juristische Belehrungen sind die Realität.

Die Verordnung selbst ist ebenfalls alles andere als einsteigerfreundlich und dürfte in der Regel selbst ambitionierten Jurastudenten noch einiges abverlangen. Auch ergibt sich der vollständige Sinn einzelner Vorschriften erst, nachdem man die Erwägungsgründe der DSGVO zu Rate gezogen hat. Diese sind eine Art Selbstkommentierung des Gesetzgebers, um einzelne Vorschriften näher zu erläutern. Auch wenn sich mittlerweile vielfach frei verfügbare Texte zur Erläuterung der Datenschutzgrundverordnung im Web finden lassen, ist Datenschutz alles andere als einsteigerfreundlich.

Das Recht auf Auskunft und Löschung

Der Nutzer kann nun bei jeder Stelle, die seine Daten verarbeitet, gem. Art. 15 DSGVO kostenfrei Auskunft über Art und Umfang der gespeicherten Daten, die Verarbeitungszwecke, die Beteiligten der Datenverarbeitung und noch vieles weiteres verlangen. Mehr zu den Auskunftsrechten und wie diese geltend gemacht werden können, erfahren Sie ab Seite 24.

Darüber hinaus haben Verbraucher aufgrund der DSGVO europaweit mehr Rechte bezüglich der Löschung ihrer Daten. Entfällt beispielsweise der Zweck der Verarbeitung, können sie auf Grundlage des Rechts auf Vergessenwerden die Löschung ihrer

Daten verlangen. Einfacher ist es auch, Datenspuren im Internet löschen zu lassen (siehe Seite 32).

Umzug gesammelter Daten

Die Datenportabilität, also die Möglichkeit, mit den gesammelten Daten von einem Anbieter zum anderen umzuziehen, ist der geheime Herzenswunsch vieler Internetnutzer – ob beim Wechsel von einem E-Mail-Service zum anderen oder zwischen Versicherungen, Telefonanbietern oder sozialen Netzwerken wie Facebook und Twitter. In all diesen Fällen hilft Artikel 20 DSGVO: Hiernach ist es Diensteanbietern gestattet, die gesammelten Daten dem Verbraucher zur Verfügung zu stellen oder direkt an den anderen Dienst zu versenden. Damit sollen Nutzer nicht durch komplizierte Wechselmodalitäten möglichst lange an den eigenen Dienst gebunden werden (Lock-in-Effekt).

Die zu versendenden Daten müssen darüber hinaus ein gängiges und interoperables Format haben, das auch vom neuen Diensteanbieter verarbeitet werden kann. Hieraus resultieren für die Diensteanbieter neue Herausforderungen. Die zu übertragenden Daten müssen sowohl auf anderen Systemen kompatibel sein als auch über eine ausreichende Verschlüsselung verfügen, um die Sicherheit der Daten beim Transfer zu gewährleisten.

Umgesetzt ist dies nach wie vor nicht überall. Prinzipiell müssten zum Beispiel auch Musik-Streaming-Anbieter den neuen Umzugsservice für personenbezogene Daten ermöglichen, sodass Nutzer ihre persönlichen Playlists mitnehmen können. In der Praxis lassen sich die Daten zwar herunterladen, jedoch nicht zum Konkurrenzunternehmen übertragen. Es fehlt an gemeinsamen Standards, interoperablen Systemen und offensichtlich auch am Willen der Streaming-Anbieter.

Privacy by Design und Privacy by Default

Die DSGVO verpflichtet Unternehmen, ihre Angebote von vornherein so zu gestalten, dass Datenschutz-Grundsätze wirksam umgesetzt werden, ohne für den Benutzer unnötig umständlich zu sein. Die verpflichtenden Vorgaben des Artikels 25 DSGVO für die Prinzipien *Privacy by Design* und *Privacy by Default* zielen zugleich darauf, dass nur noch das absolut notwendige Minimum an Daten erhoben und die Sicherheit maximiert wird (siehe Seite 16).

Privacy by Design verlangt hierfür, die Sicherheit von Daten bereits bei der Entwicklung von Technologien zu berücksichtigen. Beispiele für die Umsetzung dieser Vorgabe sind die Verwendung von Verschlüsselungstechnologien bei der Datenübertragung sowie die konsequente Pseudonymisierung von Daten.

Privacy by Default verpflichtet Datenverarbeiter dazu, in Programmen, Apps und anderen Anwendungen die datenschutzfreundlichsten Einstellungen vorausgewählt anzubieten. Hier war das Gegenteil lange Zeit Standard. Das bekannteste Beispiel dafür ist das soziale Netzwerk Facebook. Mit jedem Update seiner Nutzungsbedingungen musste man erneut die Verwendung seiner Nutzerdaten anpassen. Hier hat Facebook aufgrund der DSGVO schon etwas nachgebessert.

Beide Prinzipien lassen sich derzeit sehr gut umgesetzt auf den meisten Websites beobachten. Die dortigen Cookie-Einstellungen müssen von Beginn an auf die datensparsamste Variante, also nur die Erhebung der essenziellen Cookies gesetzt sein. Mehr zu der Thematik „Cookies“ finden Sie auf der Seite 158.

Hohe Strafen bei fehlender Umsetzung

Nicht alle Rechte sind neu, die mit der DSGVO gekommen sind. Viele Verbraucher stellen sich daher zu Recht die Frage, wie sie gegen Unternehmen vorgehen können, die sich beispielsweise weigern, Auskunft über die gesammelten Daten zu geben oder bei einem geplanten Datentransfer zu kooperieren. Hier sind die immensen Strafzahlungen, die zu den gravierendsten Änderungen in der Datenschutzgrundverordnung gehören, ein wirksamer Hebel zur Durchsetzung der Rechte.

Jeder mutmaßliche Verstoß gegen den Datenschutz kann fortan bei der nächsten Datenschutzbehörde gemeldet werden. Unabhängig vom Sitz des Datenverarbeiters kann sie Ermittlungen aufnehmen und bei vorliegenden Datenschutzverletzungen empfindliche Bußgelder verhängen. Hiervon wurde in den letzten 12 Monaten in Deutschland, aber auch in einigen anderen EU-Ländern, reichlich Gebrauch gemacht, mit zum Teil spektakulär hohen Bußgeldern. Außerdem haben Betroffene unter bestimmten Umständen ein Anrecht auf Schadensersatz (siehe auch Seite 60). (keh) **ct**



Infoseite aus
Verbrauchersicht

[ct.de/wm6k](https://www.ct.de/wm6k)

Das Recht auf Auskunft

Die Verbraucher sind die großen Gewinner des europäischen Datenschutzes. Mit der DSGVO haben sie exzellente Möglichkeiten, Auskunft über die Verarbeitung ihrer Daten von Unternehmen, Behörden und Vereinen in ganz Europa zu verlangen.

Von Niklas Mühleis

Nicht jedes Recht, das mit der Datenschutz-Grundverordnung (DSGVO) gekommen ist, war wirklich neu. So konnte man in Deutschland nach der alten Fassung des Bundesdatenschutzgesetzes (BDSG-alt) bereits Auskunft über die Datenverarbeitung verlangen. Dieses Recht war jedoch gegenüber der nun geltenden Regelung deutlich eingeschränkter und nur bei Institutionen mit Sitz in Deutschland möglich.

Wer beispielsweise von Unternehmen mit Sitz in einem anderen EU-Mitgliedsstaat Auskunft über die Art und Weise der Verarbeitung seiner Daten verlangte, hatte aufgrund der uneinheitlichen Gesetzeslage große Mühe, an die gewünschten Informationen zu gelangen.

Datensparsamkeit oder Big Data?

Das mit der Verordnung eingeführte Auskunftsrecht nach Artikel 15 DSGVO ist zu deutlich mehr in der Lage als Verbraucher mit ein paar zusätzlichen Informationen auszustatten. Vielmehr stellt dieses Recht das wirksamste Werkzeug gegen die Datensammelwut großer Unternehmen dar. Um den Ansatz der Datenmaximierung zu verstehen, muss zunächst jedoch ein Schritt zurückgegangen werden.

Anfang dieses Jahrzehnts wurde das massenhafte Speichern von personenbezogenen Daten (siehe Seite 12) – bekannt unter dem Begriff Big Data – zum neuen Trend auserkoren. Die Idee war: Wenn man von einer ausreichend großen Anzahl an Personen

möglichst viele Daten speichert und diese anschließend auswertet, so lassen sich das Konsumverhalten, Vorlieben und politische Entscheidungen vorhersagen und sogar beeinflussen. Dass dies kein

Cambridge Analytica

Das britische Datenanalyse-Unternehmen Cambridge Analytica nutzte einen Exploit in der App-Struktur Facebooks aus, um an die Daten von bis zu 87 Millionen Facebook-Nutzern zu gelangen. Diese Daten wiederum spielten eine große Rolle im Social-Media-Wahlkampf des republikanischen Präsidentschaftskandidaten Donald Trump im Jahr 2016. Wie groß der Anteil von Cambridge Analytica an dessen Sieg ist, lässt sich nicht mehr nachvollziehen. Dass der Wahlkampf in den sozialen Netzwerken von Trump gewonnen wurde, ist jedoch unbestritten.



weit hergeholtes Science-Fiction-Szenario ist, zeigen Datenskandale wie der um Cambridge Analytica (siehe Kasten auf der linken Seite).

Das Erfolgsgeheimnis von Big Data besteht also in der Speicherung und Auswertung von möglichst vielen Nutzerdaten. Die DSGVO hingegen will das genaue Gegenteil bezwecken und schreibt Datenverarbeitern die größtmögliche Sparsamkeit bei der Erhebung von Daten vor.

Grundsatz der Datensparsamkeit

Mit dem Auskunftsrecht aus der DSGVO besteht die Möglichkeit, aktiv zu überprüfen, ob der Grundsatz

der Datensparsamkeit (siehe Seite 16) und viele andere Vorschriften eingehalten werden. Denn jeder Betroffene kann erfragen, welche Kategorien personenbezogener Daten gespeichert und verarbeitet werden, also beispielsweise der Name, die Anschrift oder das Geburtsdatum, und sich diese Daten kostenfrei als Kopie zur Verfügung stellen lassen. Ein Augenmerk sollte dabei stets auf die besonderen Kategorien personenbezogener Daten gelegt werden. Diese umschreiben äußerst sensible Daten wie medizinische Befunde, die sexuelle Orientierung oder die Zugehörigkeit zu Religionsgemeinschaften. Diese Daten dürfen nur unter sehr engen Voraussetzungen gespeichert und verarbeitet werden.

Doch nicht nur die Einhaltung der Datensparsamkeit lässt sich mit dem Auskunftsrecht überprüfen. Datenverarbeiter müssen auch Auskünfte erteilen, die einen Einblick in die Einhaltung vieler gesetzlicher Pflichten aus der DSGVO gewähren. Dazu gehört unter anderem, wer personenbezogene Daten bislang empfangen hat und in Zukunft noch empfangen wird, die geplante Dauer der Speicherung der Daten sowie deren Herkunft.

Personenbezogene Daten dürfen nur von dazu berechtigten Bearbeitern empfangen werden. Daten sämtlichen Personen innerhalb derselben Institution zur Verfügung zu stellen, würde einen Verstoß gegen das Gebot der Datenminimierung darstellen. Bei dem Rückgriff auf externe Datenverarbeiter schreibt die DSGVO den Abschluss eines Vertrages über die Auftragsverarbeitung vor (siehe Seite 56).

Zuletzt muss für die Betroffenen die Herkunft der Daten nachvollziehbar sein, da für jede Erhebung oder Speicherung von Daten eine Einwilligung oder anderweitige Rechtfertigung vorliegen muss (siehe Seite 16).

Zweck der Verarbeitung

Darüber hinaus ermöglicht das Auskunftsrecht tiefe Einblicke in den geschäftlichen Betrieb der Datenverarbeiter und lässt damit auch Rückschlüsse auf das Verantwortungsbewusstsein beim Umgang mit personenbezogenen Daten zu. Verbraucher können sich daher auch über die Zwecke der Verarbeitung (siehe Seite 16) ihrer Daten informieren lassen. Online-Shops müssen dementsprechend ihren Kunden Auskunft erteilen, ob sie deren Daten lediglich zur Abwicklung von Bestellungen nutzen oder ob sie diese beispielsweise automatisiert auswerten. Bei der Verwendung von automatisierten Entschei-

Datenschutzrechtliche Selbstauskunft nach DSGVO

Betr: Name, Adresse, sonstige Identifikationsmöglichkeit (z. B. Kundennummer, verwendete E-Mail-Adresse)

Sehr geehrte Damen und Herren,

nach **Art. 15 DSGVO** habe ich das Recht, von Ihnen eine Bestätigung darüber zu verlangen, ob Sie personenbezogene Daten über meine Person gespeichert haben. Sofern dies der Fall ist, so habe ich ein Recht auf Auskunft über diese Daten.

1. Auskunft über meine bei Ihnen gespeicherten Daten

Ich darf Sie in diesem Fall bitten, mir gemäß Art. 15 Abs. 1 DSGVO folgende Informationen mitzuteilen:

- Welche Daten über meine Person konkret bei Ihnen gespeichert oder verarbeitet werden (z.B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).
- Weiterhin wollen Sie mich bitte über die Verarbeitungszwecke meiner Daten ebenso informieren wie über
- die Kategorien personenbezogener Daten, die bezüglich meiner Person verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, die meine Daten bereits erhalten haben oder künftig noch erhalten werden;
- die geplante Dauer für die Speicherung meiner Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen meiner Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung meiner Daten, ebenso wie über mein Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DSGVO und mein Beschwerderecht bei der zuständigen Aufsichtsbehörde.
- Sofern die Daten nicht bei mir erhoben werden, fordere ich Sie auf, mir

Beispiel für eine datenschutzrechtliche Selbstauskunft

dungsfindungen, unter anderem dem Profiling, müssen Datenverarbeiter Informationen über die verwendete Logik und die angestrebte Auswirkung zur Verfügung stellen. Wenn Online-Kaufhäuser wie Amazon ihre Kunden bestimmten Konsumgruppen zuordnen, um Kaufvorschläge zu unterbreiten und damit künftige Kaufentscheidungen zu beeinflussen, muss dies transparent gemacht werden.

Auch dürfen Kundendaten nicht ohne Weiteres an Geschäftspartner weitergegeben werden. Ebenso widerspricht das unerlaubte Weiterreichen von E-Mail-Adressen zum Zweck der Newsletter-Versendung der DSGVO (siehe Seite 154).

Eine weitere Pflicht der DSGVO für Datenverarbeiter betrifft die Speicherung der Daten. Sobald der Zweck der Datenverarbeitung erfüllt wurde und die weitere Speicherung nicht durch gesetzliche Pflichten vorgeschrieben wird, müssen die Daten unverzüglich gelöscht werden (siehe Seite 32).

Weiterleitung personenbezogener Daten in Drittstaaten

Transparent muss nun auch die Weiterleitung von personenbezogenen Daten in Drittstaaten oder an internationale Organisationen sein (siehe auch Seite 54). Unter Drittstaaten sind hierbei sämtliche Staaten außerhalb der Europäischen Union zu verstehen, die demzufolge nicht von der Datenschutz-Grundverordnung betroffen sind. Weil in den Drittstaaten

zumeist ein geringeres Datenschutzniveau existiert, müssen Datenverarbeiter benennen, wohin sie Daten weiterleiten, und Datenschutzgarantien von dem Empfänger der Daten einholen. Erlaubt ist die Übermittlung an Datenverarbeiter in Drittstaaten nur dann, wenn nahezu das gleiche Niveau an Datenschutz beibehalten wird. Damit unternimmt die DSGVO den Versuch, für die Daten von EU-Bürgern einen Schutz über das Territorium der EU hinaus durchzusetzen. Selbstverständlich müssen die Betroffenen auch über diese Garantien informiert werden.

Vorformulierte Musterbriefe

Dieses Gesamtpaket an Auskunftsrechten ist selbst für Juristen nicht leicht zu durchblicken. Damit Verbraucher dennoch ihr Auskunftsrecht wirksam durchsetzen können, sollten sie auf vorformulierte Musterbriefe zurückgreifen, von denen bereits einige im Netz kursieren. Diese enthalten sämtliche möglichen Auskunftsansprüche. Unter Datenverarbeitern tragen diese Briefe den inoffiziellen Titel „Albtraum-Brief“ („nightmare-letter“), da sie für einen erheblichen Aufwand sorgen und insbesondere in Institutionen, die den internen Datenschutz eher stiefmütterlich behandeln, viel Arbeitszeit binden.

Auch wir haben eine entsprechende Vorlage entwickelt: „Die c't-Fassung von Framstags freundlichem Folterfragebogen“, kurz ct5F (siehe Kasten unten).



Framstags freundlicher Folterfragebogen

Damit Sie Ihre Ansprüche gegen die ungewollte Speicherung Ihrer Daten durchsetzen können, haben wir eine Vorlage entwickelt, mit der Sie Auskunfts- und Löschansprüche geltend machen können. Eine bekannte Vorlage hinsichtlich der Ansprüche aus dem alten Bundesdatenschutzgesetz gab es bislang bereits unter dem Titel „T5F – Thoms Fassung von Framstags freundlichem Folterfragebogen“.

Um diese seit 2001 im Netz erhältliche Vorgabe zu ehren, haben wir unser Dokument „ct5F“ genannt – „Die c't-Fassung von Framstags freundlichem Folterfragebogen“.

Unsere Vorlage steht zum Download und zur nicht-kommerziellen Nutzung frei zur Verfügung (siehe ct.de/wcft). Unseriöse Versender oder Spammer benutzen Ihre Adresse? Foltern Sie sie!



Auskunft über welche Daten möglich?

? Was für Informationen kann ich mit dem Recht auf Auskunft verlangen?

! Mit dem Recht auf Auskunft können Sie Informationen verlangen über die Daten, die von Ihnen gespeichert und verarbeitet werden, die Verarbeitungszwecke, den gegenwärtigen und künftigen Empfängerkreis der Daten, die geplante Dauer der Speicherung sowie die Kriterien der Dauer, die bestehenden Rechte auf Löschung und Berichtigung hinsichtlich der gespeicherten Daten, die Herkunft der Daten, die Verwendung von automatisierter Entscheidungsfindung sowie deren Logik und Zweck und die Übermittlung von Daten in Drittländer oder an internationale Organisationen. Darüber hinaus kann die Vorlage sämtlicher personenbezogener Daten in Kopie verlangt werden.

Formvollendet

? Muss man eine bestimmte Form für ein Auskunftsverlangen einhalten?

! Grundsätzlich wird keine besondere Form für ein Auskunftsverlangen vorgeschrieben. Theoretisch kann dieses also auch mündlich an den für die Datenverarbeitung Verantwortlichen gerichtet werden. Jedoch müssen sich die Antragsteller gegebenenfalls identifizieren, um die Gefahr von Fake-Anfragen durch unbefugte Personen zu verhindern. Es empfiehlt sich daher, das Auskunftsersuchen schriftlich per Brief oder via E-Mail einzureichen.

Wartezeit

? Wie lange haben Datenverarbeiter Zeit, um auf mein Auskunftsersuchen zu reagieren?

! Bei einem Auskunftsersuchen sind die verlangten Informationen unverzüglich, also ohne schuldhaftes Zögern, spätestens jedoch nach einem Monat zu erteilen. Diese Frist kann das befragte Unternehmen in komplexen Fällen um zwei Monate verlängern. Dann muss es allerdings den Verbraucher darüber und über die Gründe der Verlängerung informieren. Dies wird in Art. 12 DSGVO geregelt.

Auskunft verweigert

? Gibt es Fälle, in denen die Auskunftserteilung verweigert werden darf?

! Ja, in bestimmten Fällen darf die Auskunftserteilung verweigert werden. Die Schöpfer der DSGVO waren sich durchaus des großen Arbeitsaufwands bewusst, welcher mit der Erteilung von Auskünften einhergeht. Daher kann die Erteilung von Auskünften bei offensichtlich unbegründetem oder exzessivem Auskunftsersuchen verweigert werden. Dies kann bei wiederholtem Auskunftsersuchen vorliegen oder wenn es niemals eine Verbindung zwischen dem Betroffenen und der datenverarbeitenden Stelle gegeben hat.

Rechtsverstöße

? Ich habe Auskunft erhalten und bin der Meinung, dass gegen die Vorgaben der DSGVO verstoßen wird. Was kann ich tun?

! Für viele Datenverarbeiter stellen die strengen Regelungen der DSGVO nach wie vor eine große Schwierigkeit dar. Die Umstellung des Geschäftsbetriebs auf Datensparsamkeit, Speicherfristen und Zugangsbeschränkung ist bei vielen Institutionen noch nicht optimal umgesetzt. Sollten Sie offensichtliche Rechtsverstöße im Umgang mit Ihren Daten entdecken, können Sie kostenlos bei dem Datenschutzbeauftragten Ihres Bundeslandes Beschwerde einreichen. Dies gilt übrigens auch für den Fall, wenn Ihr Auskunftsersuchen nicht oder nicht umfassend beantwortet werden sollte. (keh) **ct**



Vorlage ct5F

ct.de/wcft



Musterantwort für Auskunftersuchen

Die Beantwortung von Auskunftersuchen gemäß Artikel 15 DSGVO bereitete vielen Unternehmen in den letzten Jahren große Schwierigkeiten. Mit dieser kommentierten Musterantwort stellen wir eine Vorlage zur Verfügung, mit welcher Auskunftsanfragen möglichst einfach beantwortet werden können.

Von Niklas Mühleis

Die Datenschutzgrundverordnung wartet mit zahlreichen Pflichten für die Verarbeiter von personenbezogenen Daten auf. Damit die Beantwortung von Auskunftersuchen nicht mehr Zeit als notwendig in Anspruch nimmt, gilt „Vorbereitung ist alles“. Was Sie bereits vor dem ersten Auskunftersuchen sowohl organisatorisch als auch einzelfallbezogen planen und aufziehen können, finden Sie auf der Seite 78. Eine geordnete Vorlage erleichtert die Antwort. Es empfiehlt sich daher, sich an der Struktur des Artikel 15 DSGVO zu orientieren und nicht an der Reihenfolge der Fragen aus dem Auskunftersuchen. Für den Fragesteller ist es egal in welcher Reihenfolge seine Fragen beantwortet werden, während es dem Auskunftserteilenden Sicherheit gibt, stets nach dem gleichen Schema zu arbeiten.

Die Musterantwort Schritt für Schritt

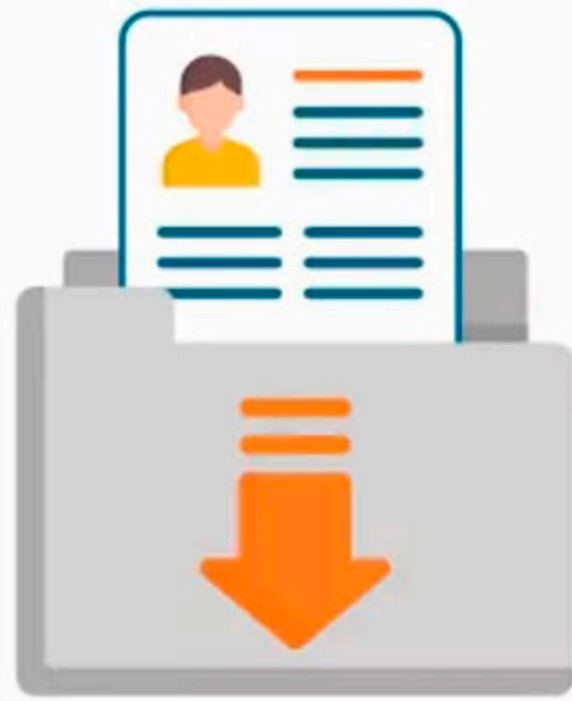
*Sehr geehrte/r [Anrede Ersuchender],
vielen Dank für Ihre Anfrage vom [Datum]. Wir haben*

diese erhalten und können Ihnen hierzu folgendes Ergebnis mitteilen.

Variante 1: Aktuell haben wir keine Daten mit Bezug auf Ihre Person bei uns gespeichert.

Variante 2: Aktuell haben wir Kategorien personenbezogener Daten über Sie gespeichert. Ihr Auskunftersuchen haben wir entsprechend der von Ihnen begehrten Informationen beantwortet.

Der Antwort an den Auskunftersuchenden sollte zunächst ein einleitendes Anschreiben vorangestellt werden. Sollten keine personenbezogenen Daten gespeichert sein, ist die Variante 1 zu wählen, mit der die Beantwortung des Schreibens abgeschlossen ist. Selbst, wenn keine personenbezogenen Daten gespeichert sind, sollte jede Anfrage dennoch beantwortet werden. Für den Fall, dass Daten mit Personenbezug gespeichert wurden, ist Variante 2 zu wählen, mit welcher die eigentliche Beantwortung einzuleiten ist.



a) Bei uns gespeicherte personenbezogene Daten zu Ihrer Person

Im angehängten Dokument befinden sich alle Daten, die wir zum TT.MM.JJJJ von Ihnen in unseren Systemen gespeichert haben.

Achten Sie darauf, dem Antragsteller stets eine vollständige Kopie seiner gespeicherten personenbezogenen Daten zu übersenden. Hierbei kann es sich der Antragsteller aussuchen, ob dies auf dem postalischen oder elektronischen Wege geschehen soll. Grundsätzlich muss zu diesem Zweck jedoch nicht absolut jeder verfügbare Datensatz übermittelt werden. Hier wird beispielsweise von § 34 Bundesdatenschutzgesetz bezüglich der Daten zum Zwecke der Datensicherung und Kontrolle eine Grenze gezogen. Zu beachten ist, dass kein Anspruch auf Übersendung von umfassenden Aktenvorgängen besteht. Es geht stets nur um die personenbezogenen Daten des Antragstellers.

b) Verarbeitungszwecke Ihrer personenbezogenen Daten

Ihre Daten werden je nach System für verschiedene Zwecke gespeichert. Anhand der nachfolgenden Auflistung können Sie alle Systeme, in denen Ihre Daten hinterlegt sind, mit dem jeweiligen Zweck des Systems einsehen.

Listen Sie hier die unterschiedlichen Systeme mit dem jeweiligen Verarbeitungszweck auf, für welche die personenbezogenen Daten hinterlegt sind, wie beispielsweise „Rechnungsabteilung, Vertragserfüllung“.

c) Kategorien Ihrer personenbezogenen Daten

Ihre Daten werden als Kundendaten gespeichert.

Überprüfen Sie, unter welchen Kategorien die Daten in Ihrem System gespeichert werden. Die müssen nicht nur zwangsläufig Kundendaten sein. Andere Möglichkeiten sind Vertragspartner, Dienstleister, Forderungsgegner oder auch Arbeitnehmer.

d) Die Empfänger oder Kategorien von Empfängern, die Ihre Daten erhalten haben oder noch erhalten werden.

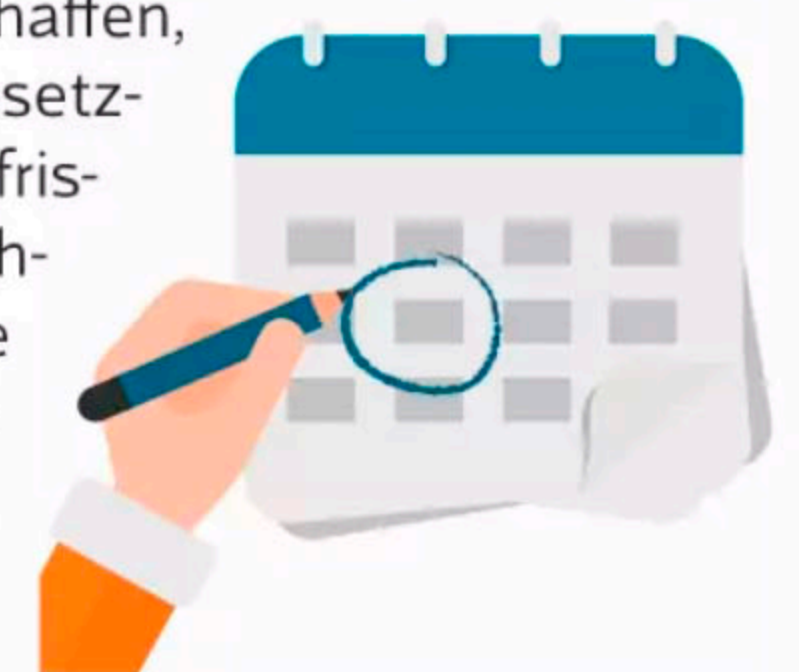
Eine Weitergabe erfolgt an Empfänger, die wir zur Durchführung unserer vertraglichen Pflichten benötigen. Entsprechende Kategorien von Empfängern sind: ...

Hier hat eine vollständige Auflistung von sämtlichen Kategorien von Empfängern, also den Dienstleistern und Auftragsdatenverarbeitern zu erfolgen, welche die personenbezogenen Daten des Antragstellers empfangen haben. Hierzu können beispielsweise gehören: Zahlungsdienstleister, Versand- und Logistikdienstleister, Marketing-Dienstleister.

e) Geplante Dauer für die Speicherung Ihrer Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

Sobald der Zweck für die Speicherung entfällt, werden wir Ihre personenbezogenen Daten löschen oder sperren. Darüber hinaus kann eine Speicherung jedoch erfolgen, wenn dies durch den europäischen oder nationalen Gesetzgeber in EU-Verordnungen, Gesetzen oder sonstigen Vorschriften, denen wir unterliegen, vorgesehen wurde. Das betrifft zum Beispiel Daten, die aus handels- oder steuerrechtlichen Gründen aufbewahrt werden müssen, etwa Rechnungsdaten. Eine Sperrung oder Löschung Ihrer Daten erfolgt dann, wenn eine durch diese Vorschriften vorgeschriebene Speicherfrist abläuft, es sei denn, dass eine Erforderlichkeit zur weiteren Speicherung der Daten für einen Vertragsabschluss oder eine Vertragserfüllung besteht. Daten, die in Zusammenhang mit der Erfüllung von Verträgen stehen, werden von uns auf Grundlage der gesetzlichen Verpflichtungen für zehn Jahre gespeichert. Alle anderen Daten (beispielsweise E-Mail bei E-Mail-Newsletter) speichern wir bis auf Widerruf der Einwilligung.

Die Speicherdauer kann ein schwieriges Terrain darstellen. Zum einen verfolgt die DSGVO das Ziel, dass Daten grundsätzlich so kurz wie möglich gespeichert werden. Zum anderen gibt es zahlreiche nationale und europäische Vorschriften, die eine feste Speicherdauer gesetzlich vorgeben. Es empfiehlt sich daher, Klarheit zu schaffen, welche Daten von gesetzlichen Mindestspeicherfristen betroffen sind. Beachtenswert ist, dass eine nicht widerrufene Einwilligung in die zweckgebundene Datenverarbeitung auch stets



einen Rechtsgrund für die fortlaufende Speicherung von Daten darstellt.

f) Informationen über das Bestehen Ihrer Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung Ihrer Daten, ebenso wie über Ihr Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DSGVO und Ihr Beschwerderecht bei der zuständigen Aufsichtsbehörde



Sofern die jeweiligen gesetzlichen Voraussetzungen vorliegen, besteht auf Ihrer Seite ein Recht auf Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) oder Einschränkung der Verarbeitung Ihrer Daten (Art. 18 DSGVO). Darüber hinaus haben sie gegebenenfalls ein Widerspruchsrecht gegen diese Verarbeitung (Art. 21. DSGVO). Darüber hinaus haben Sie gemäß Art. 77 DSGVO die Möglichkeit, Beschwerde bei der zuständigen Landesdatenschutzbehörde zu erheben. Die für uns zuständige Aufsichtsbehörde ist: ...

Die DSGVO sieht vor, dass betroffene Personen über ihre Rechte aufgrund der Datenverarbeitung zu informieren sind. Darüber hinaus soll ebenfalls Transparenz darüber hergestellt werden, welche Landesdatenschutzbehörde die Aufsicht über den jeweiligen Datenverarbeiter hat.

g) Informationen über die Herkunft Ihrer Daten

Die von uns verwendeten Daten stammen ausschließlich aus Direkterhebungen.

Alternative: Die von uns verwendeten Daten stammen aus Dritterhebungen. Die Direkterhebung fand durch die Firma XYZ im Rahmen einer Newsletter-Anmeldung statt.

Die betroffene Person muss darüber informiert werden, woher die personenbezogenen Daten stammen. Die sogenannte Direkterhebung, also die Herkunft direkt von der betroffenen Person, stellt dabei den Regelfall dar. Die Alternative ist die Dritterhebung, also die Herkunft aus anderen Quellen. Eine solche ist nicht grundsätzlich rechtswidrig, jedoch wird hierfür eine rechtliche Erlaubnis benötigt.

h) Informationen über das Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling gemäß Art. 22 DSGVO

Wir treffen keine Entscheidungen beruhend auf einer automatisierten Verarbeitung, einschließlich Profiling im Sinne von Art. 22 DSGVO.

Alternative: Wir treffen Entscheidungen beruhend auf einer automatisierten Verarbeitung. Hierzu gehört das Bilden von Nutzerprofilen, das Profiling im Sinne von Art. 22 DSGVO.

Sie müssen die betroffene Person darüber informieren, ob personenbezogene Daten automatisiert verarbeitet werden, das sogenannte Profiling. Dies geschieht beispielsweise bei vielen Online-Shops, um den betroffenen Personen zugeschnittene Kaufvorschläge anbieten zu können.

i) Informationen, ob Ihre personenbezogenen Daten an ein Drittland oder an eine internationale Organisation übermittelt wurden und welche geeigneten Garantien gemäß Art. 46 DSGVO im Zusammenhang mit der Übermittlung vorgesehen sind

Eine Übermittlung Ihrer Kundendaten in Drittländer fand nicht statt. Soweit ausnahmsweise eine Übermittlung von technischen Daten, zum Beispiel IP-Adressen, in Drittstaaten erfolgte, so erfolgt diese in die USA und findet Ihre Rechtsgrundlage in den EU-Standardvertragsklauseln.

Eine Übermittlung in Drittländer außerhalb der Europäischen Union ist zulässig, wenn zwischen diesen Staaten und der Europäischen Union eine Vereinbarung zum Datentransfer wie die Standardvertragsklauseln existiert. Bis vor kurzem konnte hier auch noch der „EU-US-Privacy-Shield“ angeführt werden. Durch ein aktuelles Urteil des EuGH vom 16.07.2020 ist dieser nicht mehr anwendbar. Das Anführen der Standardvertragsklauseln darf jedoch keine reine Floskel sein. Diese müssen auch tatsächlich vereinbart worden sein. Einer der häufigsten Fälle für die Datenübertragung in das europäische Ausland ist die Verwendung von sozialen Netzwerken wie Facebook oder die Nutzung eines Hosting Servers außerhalb der Europäischen Union. Mehr zu der Datenübertragung in die Vereinigten Staaten nach dem Fall des Privacy-Shields können Sie auf den Seiten 108-121 lesen. (keh) 



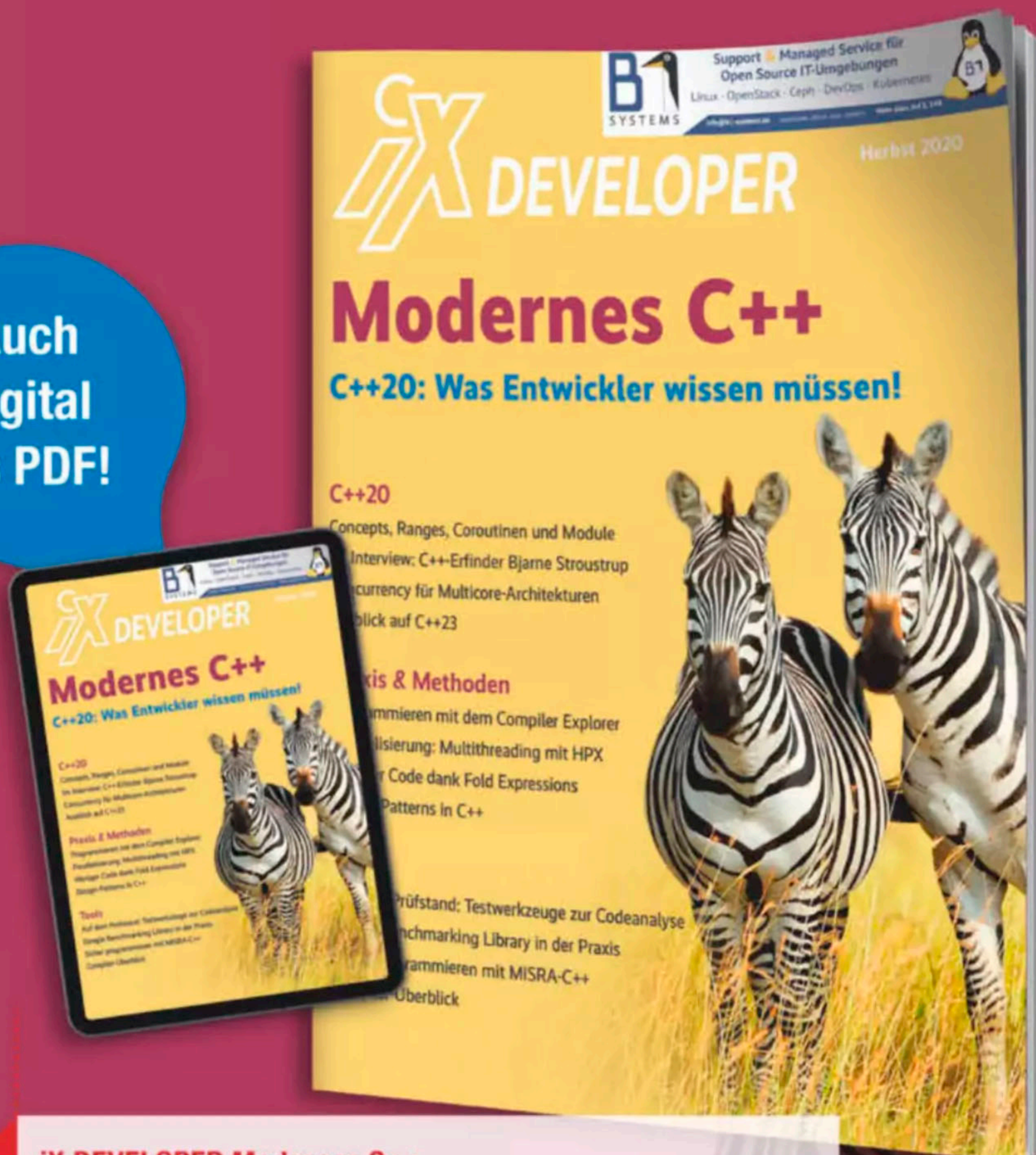
Musterantwort

ct.de/wche

C++20: Was Entwickler wissen müssen!

NEU
im heise shop

Auch
digital
als PDF!



iX DEVELOPER Modernes C++

Noch in diesem Jahr soll **C++20** erscheinen, der neue Standard für C++. Das iX-Sonderheft stellt die **zentralen Features** des Standards vor und liefert einen spannenden Einblick in die **vier großen Neuerungen**. Zusätzlich gibt das Heft eine Übersicht zur Kernsprache, der Bibliothek und Concurrency. iX-Artikel der letzten 2 Jahre zu C++ geben außerdem einen umfassenden Überblick für Entwickler.

shop.heise.de/ix-dev-c++20

Einzelheft
für nur

14,90 € >

 **heise shop**

shop.heise.de/ix-dev-c++20 >

> Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

Das Recht auf Vergessenwerden



Eine der wichtigsten Lektionen über den Umgang mit dem Internet ist: Das Internet vergisst nicht. Artikel 17 der DSGVO will dies ändern.

Von Niklas Mühleis

Mit dem Recht auf Vergessenwerden wurde in Gesetzesform gegossen, was in Grundzügen schon existiert. Bereits im Jahr 2014 entwickelte der Europäische Gerichtshof (EuGH) dieses Recht in seiner „Google Spain“-Entscheidung. Hintergrund war damals die Klage eines Spaniers gegen den spanischen Ableger des Suchmaschinenunternehmens Google. Dieser verlangte von Google, zwei Treffer zu seiner Namenssuche zu löschen, die zu der Website einer Tageszeitung führten, welche unter Nennung seines Namens Angaben zu einer Versteigerung von Grundstücken aus einer Zwangspfändung machte.

Der EuGH gab dem Antragsteller Recht und erfand damit das Recht auf Vergessenwerden. Dieses sollte Suchmaschinenbetreiber dazu verpflichten, personenbezogene Angaben (siehe Seite 12) aus den Suchergebnissen nach einiger Zeit zu löschen, sofern das Interesse der Person an der Löschung der Angaben das wirtschaftliche Interesse des Suchmaschinenbetreibers überwiegt.

Neu geregelte Löschpflichten

Mit dem Recht auf Vergessenwerden der DSGVO wird die Löschung personenbezogener Daten gegenüber der alten Rechtslage deutlich aufgewertet. Suchmaschinenbetreiber können nun verpflichtet werden, einzelne Linksetzungen zu löschen. Ebenso muss sich jeder Datenverarbeiter um die Tilgung personenbezogener Daten kümmern, die über das Internet veröffentlicht sind. Weiterhin kann jede Privatperson von Online-Shops, sozialen Netzwerken, Streaming-Diensten und anderen Datenverarbeitern

die konventionelle Löschung ihrer Daten verlangen. Dies war zwar bereits nach der alten Fassung des Bundesdatenschutzgesetzes unter bestimmten Bedingungen möglich, jedoch lange nicht so umfassend, wie es nun der Fall ist, insbesondere nicht auf europäischer Ebene. Zuvor mussten die betreffenden Unternehmen ihren Sitz innerhalb Deutschlands haben, damit Verbraucher einen Löschungsanspruch aus dem BDSG geltend machen konnten. Bekannte Social-Media-Unternehmen wie Facebook, Twitter und LinkedIn waren davon mit ihren Firmensitzen in Irland nicht betroffen.

Voraussetzungen

Eine Löschung kann immer dann verlangt werden, wenn der Zweck zur Erhebung der Daten wegfällt, die betroffene Person ihre Einwilligung zur Verarbeitung widerruft oder die Datenverarbeitung unrechtmäßig erfolgt ist. Wer sich also bei Facebook abmeldet, muss nicht damit leben, dass der Datenriese die über Jahre gesammelten Daten weiterhin speichert und für die interne Auswertung nutzt.

Gleiches gilt für Online-Kaufhäuser wie Amazon. Für die meisten Kunden sind die personalisierten Kaufempfehlungen ein praktisches Tool, welches das Shopping-Erlebnis bereichert. Andere sehen hinter dem ausgefeilten Algorithmus einen problematischen Datengebrauch. Dieser wertet nicht nur das Konsumverhalten der Nutzer aus, sondern versucht darüber hinaus künftige Kaufentscheidungen vorherzusagen und sogar zu beeinflussen. Auch der Datensammelwut der Online-Shops kann Art. 17 DSGVO enge Grenzen setzen. Selbst für Amazon und Co.

dürfte es schwer zu argumentieren sein, dass die Speicherung der gesamten Kaufhistorie eines Kunden notwendig ist, um den aktuellen Geschäftsbetrieb aufrechtzuerhalten – erst recht, wenn die Kunden ihre Zustimmung zur Datenverarbeitung widerrufen.

Mit dem Recht auf Vergessenwerden wird den Verbrauchern ein wirkungsvolles Werkzeug in die

Hände gegeben, mit dem sie in vielen Bereichen die Kontrolle über ihre Daten zurückerhalten. Wo vorher einmal gegebene Daten in vielen Fällen unbegrenzt lange weiterverwendet werden konnten, kann der unendlichen Speicherung und Verarbeitung nun ein Ende gesetzt werden. Das Internet fängt langsam an, das Vergessen zu lernen.



Wer – wie – was?

? Welche Daten kann ich löschen lassen?

! Grundsätzlich erstreckt sich das Löschungsrecht auf alle personenbezogenen Daten. Neben Angaben wie Name, Adresse, Geburtsdatum und Geschlecht sind dies auch Musikvorlieben, gekaufte Bücher, geschaute Serien oder Bewegungsprotokolle (siehe Seite 12). In aller Regel muss der Datenverarbeiter also alle gespeicherten Daten löschen. Unter Umständen können bestimmte Daten davon jedoch ausgenommen sein, wenn diese für die Erfüllung von vertraglichen oder rechtlichen Pflichten weiterhin benötigt werden (siehe Seite 13). Wer zum Beispiel gerade erst bei Amazon Bestellungen getätigt hat, wird die steuerlichen Datenspeicherfristen abwarten müssen.

Löschen verweigert

? Gibt es Ausnahmen von der Löschungspflicht?

! Ja, wenn die Nutzung der Daten unter das Recht auf freie Meinungsäußerung und Information fällt oder für die Erfüllung rechtlicher Verpflichtungen, für Forschungszwecke oder aus Gründen des

öffentlichen Interesses im Bereich der öffentlichen Gesundheit notwendig ist. Die Löschung darf nur aus einem dieser Gründe verweigert werden. Dies muss entsprechend begründet werden.

Ohne Zeitverzug

? Wie schnell muss gelöscht werden?

! Die Löschung muss unverzüglich, also ohne schuldhaftes Zögern, erfolgen. Dabei muss der für den Datenschutz verantwortlichen Person genügend Zeit eingeräumt werden, die Voraussetzungen für die Löschung zu prüfen und die dafür geeigneten Maßnahmen zu ergreifen. Spätestens jedoch einen Monat nach Eingang des Löschantrags muss die betroffene Person über die erfolgten Handlungen informiert werden.

Antrag auf Auskunftserteilung

? Wie funktioniert ein Löschantrag?

! Um zu erfahren, welche personenbezogenen Daten gespeichert worden sind, empfiehlt es sich, zuerst einen Antrag auf Auskunftserteilung nach Art. 15 DSGVO zu stellen (siehe Seite 24).

Die für die Löschung verantwortliche Person entnimmt man der Datenschutzerklärung auf der Website des betreffenden Unternehmens. Ansonsten muss sie auf Nachfrage mitgeteilt werden. Es gibt keine Formerfordernisse für den Löschantrag, doch es empfiehlt sich, diesen via E-Mail oder per Brief zu stellen. Er sollte so konkret wie möglich formuliert werden und sich direkt auf Artikel 17 der DSGVO beziehen. Benennen Sie die personenbezogenen Daten, die gelöscht werden sollen, um keinerlei Interpretationsspielraum zu lassen. (keh) **ct**

Kurzpapier der DSK:

[ct.de/wehh](https://www.ct.de/wehh)

Folgen für Vereine



Seit dem Inkrafttreten der DSGVO beklagen vor allem Vereine, dass die Regelungen der neuen Datenschutz-Grundverordnung zu hart und nicht umsetzbar sind. Doch trifft die DSGVO die ehrenamtliche Arbeit tatsächlich so hart wie befürchtet?

Von Niklas Mühleis

Der DSGVO hängt der Ruf an, die ehrenamtliche Arbeit erheblich zu erschweren oder sogar unmöglich zu machen. Tatsächlich gab es seit dem Wirksamwerden der DSGVO im Mai 2018 vermehrt Berichte und Meldungen über Vereine, die aus Angst vor Bußgeldern ihre Homepages abgeschaltet oder ihre Tätigkeit eingestellt haben.

Vereinskiller wider Willen

Das war nicht beabsichtigt, kleine ehrenamtliche Vereine sind nicht der Hauptadressat der Regelungen zum Datenschutz. Die Gesetzgeber in Brüssel hatten bei der Ausarbeitung der DSGVO eher große Unternehmen und Behörden im Blick. Dennoch gelten zahlreiche Pflichten der Verordnung auch für Vereine – jedoch in einem eher eingeschränkten Maße.

Keine Panik!

Die Beachtung dieser Pflichten aus der DSGVO sollte kein ernstliches Hindernis bei der täglichen Vereinsarbeit darstellen. Zum einen werden in den allermeisten Vereinen nur sehr wenige personenbezogene Daten (siehe Seite 12) gespeichert und verarbeitet. Dies erleichtert beispielsweise das Führen

der Verzeichnisse enorm und lässt darüber hinaus auch die Anforderungen an die Datensicherung sinken. Zum anderen sind in vielen Vereinen weniger als zehn Personen mit der Verarbeitung von personenbezogenen Daten befasst. In der Folge kann dann auf die Benennung eines Datenschutzbeauftragten verzichtet werden.



Auf die leichte Schulter sollte man den Datenschutz im Verein dennoch nicht nehmen. Auch wenn keine hohen Anforderungen an die Datensicherung gestellt werden, müssen Vereine diese dennoch beachten. Mitgliederlisten dürfen also künftig nicht mehr für jedermann zugänglich offen im Regal aufbewahrt werden, Computer, auf denen personenbezogene Daten gespeichert sind, müssen passwortgesichert sein. Selbst die Büros sollten abgeschlossen werden. Darüber hinaus sollte man die Vereinswebsite mit einer Datenschutzerklärung ausstatten und auch Datenpannen muss man selbstredend bei den zuständigen Aufsichtsbehörden melden.

Hier könnte es unangenehm werden

Manche Pflichten aus der DSGVO lassen sich mit einem überschaubaren Aufwand erfüllen. Beispielsweise muss die Datenschutzerklärung für die Vereinswebsite nur einmalig eingestellt werden. Macht ein Vereinsmitglied sein Recht auf Auskunft aus Art. 15 DSGVO geltend, kann eine solche Auskunftserteilung je nach Umfang der gespeicherten Daten und Art der Verarbeitung viel Zeit binden. Mehr zu dem Recht auf Auskunft finden Sie auf Seite 24.

Eine wichtige Aufgabe ist die Dokumentation von Verarbeitungstätigkeiten in einem entsprechenden Verzeichnis. Welche Angaben hier zu machen sind, erklärt der Artikel auf Seite 42. Die meisten Vereine kommen um diese lästige Aufgabe nicht herum.

Warum das so ist, wird in den nachfolgenden FAQs ausführlich beantwortet.

Den Datenschutz anpacken

Eine pauschale Aussage, was sich für Vereine mit der DSGVO ändert, lässt sich leider nicht treffen. Dennoch lohnt es sich, auch als kleiner Verein das Thema Datenschutz proaktiv anzugehen. Um die Datenschutz-Grundverordnung wurde vor allem in den Anfangsmonaten ihres Inkrafttretens viel Panik verbreitet und daher scheint einiges nach außen schlimmer, als es in Wirklichkeit ist. Die letzten Jahre haben gezeigt, dass die oft befürchteten Zwangsaufösungen von Vereinen meist nicht notwendig sind und die Datenschutzbehörden Vereine auch nicht gezielt auf die Einhaltung der Datenschutzvorschriften überprüfen.



letztlich immer an der Schwere des jeweiligen Verstoßes sowie dem Jahresumsatz der betroffenen Organisation. Adressat eines Bußgeldbescheids ist in der Regel der Verein, denn das Verhalten des Vereinsvorstands und der Mitglieder wird dem Verein zugerechnet. Daneben kommt aber auch eine Haftung des Vorstands oder einzelner Mitglieder in Betracht.

Solange Vereine nicht im Wettbewerb mit anderen Marktteilnehmern stehen, sind jedoch keine Abmahnungen für fehlende Datenschutzerklärungen oder andere Datenschutzverstöße zu befürchten.

Abmahnungen und Bußgelder

? Welche Kosten können auf meinen Verein zukommen, wenn der Datenschutz nicht richtig beachtet wird?

! Die DSGVO bringt nicht nur einen umfangreichen Pflichtenkatalog mit sich, sondern auch die Möglichkeit saftige Bußgelder zu verteilen. Vielen dürfte aus der Berichterstattung der Medien die Summe von 20 Millionen Euro im Gedächtnis geblieben sein. Solche Summen sind jedoch für Großkonzerne vom Schlage Googles, Volkswagen und Facebook gedacht. Der lokale Angelverein ist zwar nicht vor Bußgeldern geschützt, diese dürften jedoch deutlich moderater ausfallen und orientieren sich

Verzeichnis von Verarbeitungstätigkeiten

? Muss mein Verein ein Verzeichnis über die Verarbeitung von Daten führen?

! Das Verzeichnis von Verarbeitungstätigkeiten muss grundsätzlich jeder für die Datenverarbeitung Verantwortliche führen. Nur Vereine, die weniger als 250 Mitglieder haben und personenbezogene Daten nur gelegentlich verarbeiten, sind davon theoretisch ausgenommen. Von einer gelegentlichen Verarbeitung kann jedoch schon nicht mehr die Rede sein, wenn ein Verein seine Mitgliederkartei auf dem Laufenden hält. Außerdem dürfen keine besonderen Datenkategorien, wie Gesund-



heits- oder Religionsdaten, verarbeitet werden.

Von dieser Freistellung profitieren in der Praxis daher nur Vereine, die keine Lohnabrechnung durch-

führen, da hier Gesundheitsdaten zur Feststellung von Krankheitstagen und die Religionszugehörigkeit zur Abführung der Kirchensteuer benötigt werden. Wird eine Datenverarbeitung vorgenommen, die ein Risiko für Rechte und Freiheiten von Personen birgt, ist ein Verarbeitungsverzeichnis ebenfalls Pflicht. Das betrifft beispielsweise Refugee Law Clinics, die eine ehrenamtliche Rechtsberatung für Flüchtlinge anbieten und dementsprechend oftmals mit hochsensiblen Daten arbeiten.

Information der Mitglieder

? Muss ich meine Vereinsmitglieder über die Verarbeitung ihrer Daten informieren?

! Grundsätzlich werden Mitglieder immer informiert, wenn sie nach Auskunft verlangen. Alle seit dem 25.05.2018 neu eintretenden Mitglieder müssen aktiv über die Art und Weise der Datenverarbeitung aufgeklärt werden. Es empfiehlt sich daher, dies direkt mit dem Aufnahmeantrag zu verbinden. Ein Rundbrief an Bestandsmitglieder ist jedoch nicht notwendig, da die Informationspflicht nicht rückwirkend gilt.

Infos online

? Was muss ein Verein bei seiner Website beachten und welche Infos dürfen online abrufbar sein?

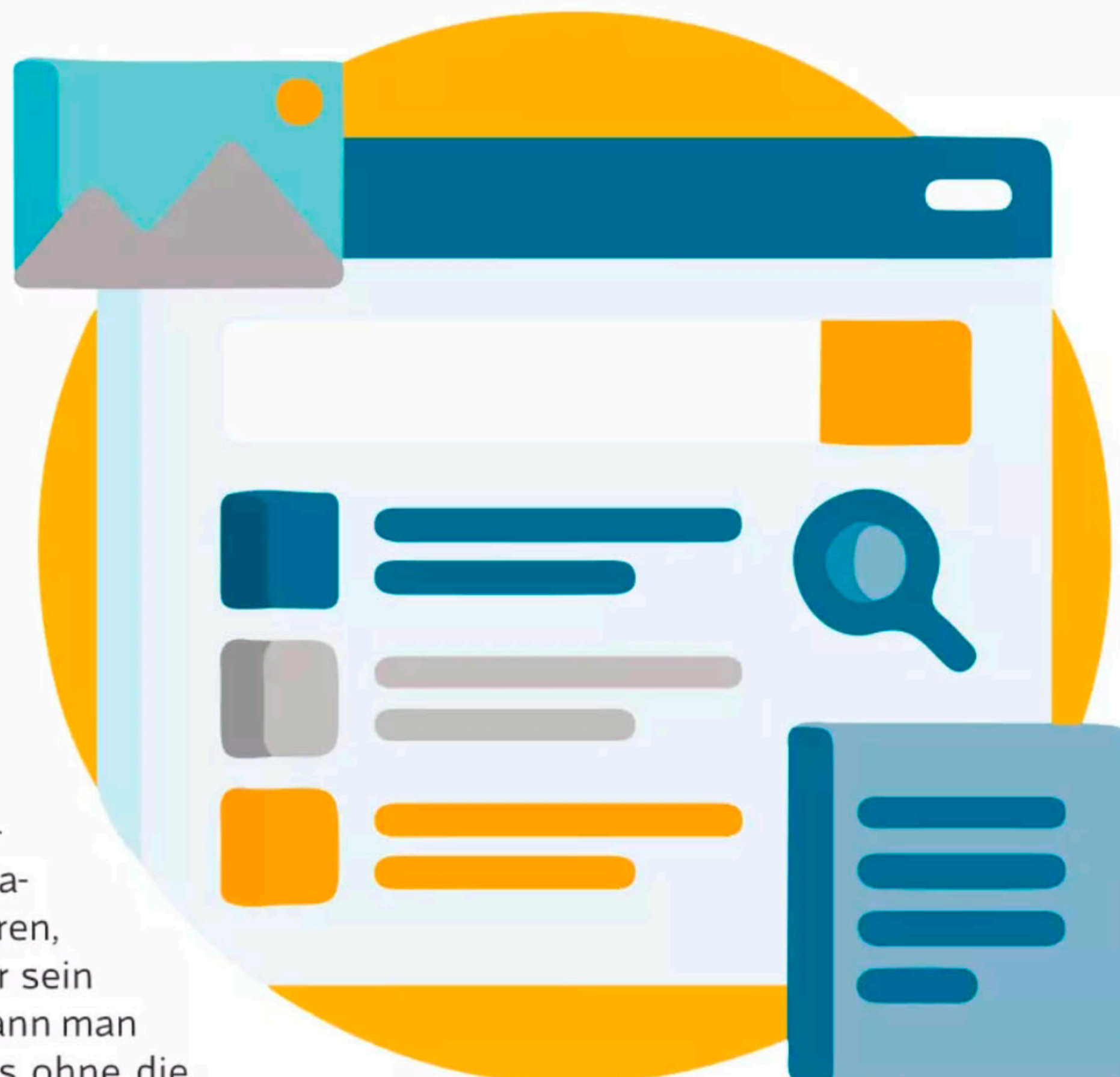
! Vereine, die sich online präsentieren, benötigen eine Datenschutzerklärung auf der Website (siehe Seite 148). Daneben ist auch die heikle Frage zu klären, welche Informationen online verfügbar sein dürfen. Für personenbezogene Daten kann man sich die Faustregel merken, dass nichts ohne die

Einwilligung der Betroffenen geht. Wenn sich der Vereinsvorstand online vorstellen möchte, ist das also unproblematisch. Anders sieht es mit Mitgliederlisten auf der Homepage aus. Hierzu müsste jedes einzelne Mitglied zugestimmt haben. Zudem können Betroffene jederzeit der Verarbeitung ihrer Daten widersprechen. Wenn also ein Mitglied nicht mehr mit Namen und Foto auf der Website des Vereins genannt werden möchte, muss diesem Wunsch nachgekommen werden. Mehr zur Regelung der Fotorechte finden Sie ab Seite 164.

Lösch mich!

? Wann müssen Mitgliederdaten gelöscht werden?

! Wenn Daten nicht mehr benötigt werden, um einen bestimmten Zweck zu erreichen, müssen sie gelöscht werden. Tritt ein Mitglied aus dem Verein aus, besteht in der Regel kein Grund mehr, dessen Daten zu behalten. Folglich ist der Datensatz aus der Mitgliederkartei zu löschen (siehe Seite 22). Ausnahmen bilden solche Daten, die man erst nach Ablauf gesetzlicher Aufbewahrungspflichten – beispielsweise aus steuerrechtlichen Gründen – löschen darf.
(keh) **ct**



DEVELOPER-KONFERENZEN + WORKSHOPS 2021



[Container Conf]

Cloud Native Day: 10.02.2021

Online

betterCode()

Domain-Driven Design: 25.02.2021

Online

» Continuous Lifecycle »

Dev(Sec)Ops Day: 03.03.2021

Online

betterCode()

APIs: 11.03.2021

Online



16. bis 18.03.2021

Hybride Veranstaltung on-site
und online

// heise devSec()

18.03.2021 (Thema folgt)

Online

Veranstalter:



@ heise Developer



dpunkt.verlag

Weitere Informationen unter:

www.heise.de/developer



Mehr Pflichten für Unternehmer

Die DSGVO bringt nach wie vor für Unternehmen eine Fülle an Pflichten mit sich. Grundsätzlich gelten diese vom Einzelunternehmer bis zum global tätigen Konzern gleichermaßen, mit bislang nur einer Ausnahme.

Von Brian Scheuch

Die Datenschutzgrundverordnung behandelt grundsätzlich alle Unternehmer gleich. Eine (teilweise) Privilegierung für Kleinunternehmen wäre zwar wünschenswert gewesen, ist bislang aber nur für die Personengrenze zur Bestellung eines Datenschutzbeauftragten beschlossen worden (siehe Artikel ab Seite 74). Eine weitere Nachbesserung

ist seit dem Inkrafttreten vor zweieinhalb Jahren bisher nicht erfolgt, auch nicht in Hinblick auf die umfangreichen Dokumentationspflichten. Nach wie vor fällt daher auch „der Bäcker von nebenan“ unter die Regelungen der DSGVO, der bei Bestellungen die Kundennamen in eine Liste auf dem Computer einträgt.



Anwendung findet die DSGVO nur dann nicht, wenn die Verarbeitung personenbezogener Daten ausschließlich durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt. Teilweise ist die Abgrenzung zwischen privaten Hobbys und einer Unternehmung jedoch schwierig. Dies gilt beispielsweise für Blogger auf privaten Websites, die ihre laufenden Kosten aber mittels Bannerwerbung finanzieren.

Sobald ein Blogger mit seiner Tätigkeit Umsätze generiert – und seien es auch nur wenige Euro, zum Beispiel durch Google AdSense –, kann er sich nicht mehr auf die Ausnahme des Artikel 2 Abs. 2 DSGVO (private Tätigkeit) berufen. Er ist dann gewerblich tätig und muss sämtliche Pflichten aus der DSGVO erfüllen. Man sollte sich daher vorab genau überlegen, ob man gewerbliche Umsätze generieren will.

Übrigens sind auch Vereine nicht explizit von den Regelungen der DSGVO ausgenommen worden, weshalb sie grundsätzlich dieselben Verpflichtungen haben (siehe Seite 34).

Was ist zunächst zu tun?

Wer die DSGVO nach Jahren noch immer eher stiefmütterlich behandelt hat, also diese noch nicht vollständig oder sogar überhaupt nicht umgesetzt hat, sollte möglichst schnell handeln. Die Meldungen über Bußgelder häufen sich und die ersten empfindlichen Bußgelder in Millionenhöhe sind verhängt worden (siehe S. 62). Die Zeiten in denen die Aufsichtsbehörden nunmehr noch „ein Auge zudrücken“ dürften vorbei sein. Mitunter wurden auch schon erste Verfahren wegen einem unzureichenden Cookie-Banner eingeleitet. Darüber hinaus besteht nach wie vor die Gefahr, abgemahnt zu werden (siehe Seite 70).



Wer bei „null“ anfängt, sollte sich daher zeitnah von „außen nach innen“ vorarbeiten, um potenziellen Abmahnern keinen Ansatz zu bieten und den Aufsichtsbehörden zu signalisieren, dass man das Thema DSGVO angegangen ist. Es zeigt sich nunmehr, dass die Aufsichtsbehörden nunmehr kein „Auge mehr zudrücken“ werden.

DSGVO-konforme Außendarstellung

Zu den datenschutzrelevanten Bereichen, die „nach außen sichtbar sind“, zählt insbesondere die Datenschutzerklärung (Privacy-Policy) auf der Unternehmens-Website. Eine DSGVO-konforme Datenschutzerklärung ist dabei meist deutlich umfangreicher im Vergleich zur alten Rechtslage (siehe Seite 46).

Weiterhin sollte man überall dort auf der Website, wo der Nutzer aktiv personenbezogene Daten an den Website-Betreiber übermittelt, entsprechende Einwilligungserklärungen per Opt-In einholen und dokumentieren. Klassische Beispiele hierfür sind Kontaktformulare und Newsletter-Anmeldeformulare. Übrigens: Auch vor Inkrafttreten der DSGVO war es bei Newslettern bereits erforderlich, den Nutzer über die Widerspruchsmöglichkeit zu informieren. Diese Pflicht hat ihren Ursprung im Wettbewerbsrecht.

Seit der neuesten Rechtsprechung des europäischen Gerichtshofs (EuGH) ist darüber hinaus insbesondere für die Nutzung von Tracking-Cookies eine aktive Einwilligung der Websitebesucher erforderlich (siehe Artikel auf Seite 158).

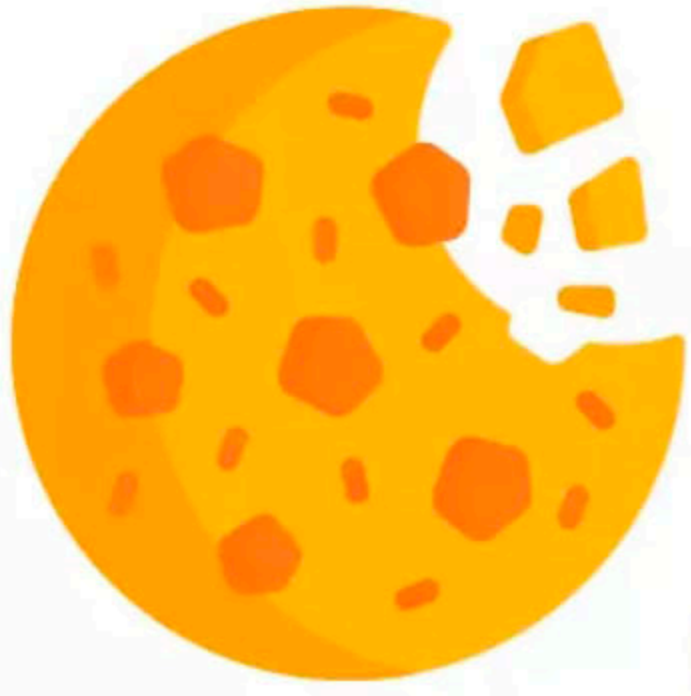
Interne Prozesse anpassen

Ist die Unternehmung nach außen DSGVO-konform gestaltet, folgen die internen Prozesse. Das Wichtigste sind die Anlage und Pflege eines Verzeichnisses über die Verarbeitungstätigkeiten, die Dokumentation der technisch-organisatorischen Maßnahmen (TOM), der Abschluss von Vereinbarungen zur Auftragsverarbeitung (AVV) mit externen Dienstleistern und gegebenenfalls die Bestellung eines Datenschutzbeauftragten.



Fortlaufende Dokumentation

Die Einhaltung der datenschutzrechtlichen Bestimmungen ist kein einmaliges Projekt, sondern ein fortlaufender Prozess. Bereits die Pflege und Anpassung des Verzeichnisses über die Verarbeitungs-



tätigkeiten und der technisch-organisatorischen Maßnahmen dürften Unternehmen fortlaufend beschäftigen.

Anpassung der Prozesse an Rechtsprechung

Auch Gerichtsurteile – insbesondere die höchstgerichtlichen Rechtsprechungen – führen dazu, dass Unternehmen ihre internen Prozesse entsprechend anpassen müssen. Ein Paradebeispiel hierfür ist das oben erwähnte Urteil des europäischen Gerichtshofs zu Tracking-Cookies oder das Urteil des europäischen Gerichtshofs zum Privacy-Shield. Hat man sich vor dem Urteil noch auf das berechtigte Interesse berufen, wird dies nun kaum noch möglich sein. Prozesse rund ums Marketing, Tracking und der Übermittlung personenbezogener Daten in Drittstaaten wie den USA, müssen neu angepasst werden.

Hilfen bei der Umsetzung

Wie Unternehmen ihre Pflichten aus der DSGVO konkret erfüllen und wie sie den Kosten- und Arbeitsaufwand für die Umsetzung möglichst gering halten, erklären die nachfolgenden Artikel.

Am Anfang steht das **Verzeichnis über die Verarbeitungstätigkeiten**. Kennt man sämtliche Verarbeitungsprozesse, kann man die Dokumentation zumeist in Eigenregie vornehmen. Wir stellen ab Seite 42 vor, was es damit auf sich hat, und zeigen beispielhaft, wie es ausgefüllt wird.

Ab Seite 46 erfahren Sie im Detail, wie die **Informationspflichten** konkret zu erfüllen sind, inklusive Erläuterungen zur Einholung von Opt-Ins und einer Checkliste zur Datenschutzerklärung.

Welchen Zweck die **technisch-organisatorischen Maßnahmen (TOMs)** haben, wird ab Seite 50 dargestellt. Die TOMs sind kein „Hexenwerk“: Viele Unternehmen haben bereits notwendige Maßnahmen getroffen, ohne sich dessen bewusst zu sein.

Ab Seite 54 wird in dieser Auflage zusätzlich aufgeführt, ob und unter welchen Voraussetzungen eine **Datenweitergabe**

innerhalb eines Konzerns nach dem „Konzernprivileg“ zulässig ist.

Bei der **Auftragsverarbeitung** ist mit dem Auftragnehmer gegebenenfalls eine entsprechende Vereinbarung zu schließen. Wann Unternehmen dazu verpflichtet sind und welche Punkte dort zwingend zu regeln sind, erläutern wir ab Seite 56.

Wird die DSGVO falsch oder nur unzureichend umgesetzt, drohen **Abmahnungen und Bußgelder** (siehe Seite 60).

Zum Thema **Schadensersatz** hat sich seit Inkrafttreten und der letzten Auflage einiges geändert, weshalb eine entsprechende Anpassung notwendig wurde (siehe Seite 72).

Wann ein unternehmensinterner **Datenschutzbeauftragter** zu bestellen ist, welche Rechte und Pflichten dieser hat und wie seine Benennung zu erfolgen hat, erfahren Sie ab Seite 74.

Zu den Vorgängen, bei denen Unternehmen Pflichten aus der DSGVO beachten müssen, gehören außerdem die **Auskunftserteilung an Betroffene** (siehe Seite 78), die **Datenübermittlung ins Ausland** (siehe Seite 108) sowie die Sonderproblematik der **Videoüberwachung** (siehe Seite 82). (keh) **ct**



Praxishilfen:

ct.de/w2wc

Vorsprung reloaded.

Neue Erfolge entstehen aus dem Wissen der Vergangenheit. Bestellen Sie deshalb jetzt das gesammelte Know-how Ihrer Fachmagazine: Die wichtigsten Informationen und Inspirationen kompakt auf den neuen Archiv-Discs – Vorsprung wie bestellt, einfach online im heise shop.



Bessere Aussichten mit dem Blick zurück:

Fakten, Meinungen, Tests und Hintergrundwissen – das Jahresarchiv 2019 mit allen Beiträgen aus 26 c't-Heften

auf DVD **24,50 €**
auf 32 GByte USB 3.0-Stick **34,50 €**

c't-Know-how XL:

Der Inhalt der letzten 14 Jahre c't, 2005 bis 2019

auf DVD **79,- €**

c't-Know-how XXL:

Alle Artikel von 1983 bis 2019

auf Blu-ray Disc **99,- €**
auf 64 GByte USB 3.0-Stick **139,- €**



Ein Jahr iX-Know-how für IT-Experten:

Nachlesen, vergleichen, absichern – alle iX-Inhalte kompakt.

auf DVD **24,50 €**
auf 32 GByte USB 3.0-Stick **34,50 €**

iX-Know-how XL:

Die Archiv-DVD mit allen Beiträgen von 1994 bis 2019

auf DVD **69,- €**

iX-Know-how XXL:

Alle Beiträge von 1988 bis 2019

auf 64 GByte USB 3.0-Stick **109,- €**

shop.heise.de/ix-archiv



Neues baut auf Altem auf:

Ihr Blick in wichtige Fakten und Hintergrundinfos des Archives 2019 von Deutschlands einzigem Innovationsmagazin.

auf DVD **24,50 €**

Technology Review-Know-how XL:

Alle Artikel von 2003 bis 2019

auf DVD **59,- €**

shop.heise.de/tr-archiv

➤ Bestellen Sie ganz einfach online im heise shop oder per E-Mail: service@shop.heise.de

 **heise shop**

shop.heise.de





Verarbeitungs- verzeichnisse

Verarbeitungsverzeichnisse sind die Basis für die korrekte Umsetzung der DSGVO-Pflichten. Mustervorlagen helfen dabei, sie zu erstellen.

Von Brian Scheuch

Sinn und Zweck

? Was ist ein Verarbeitungsverzeichnis?

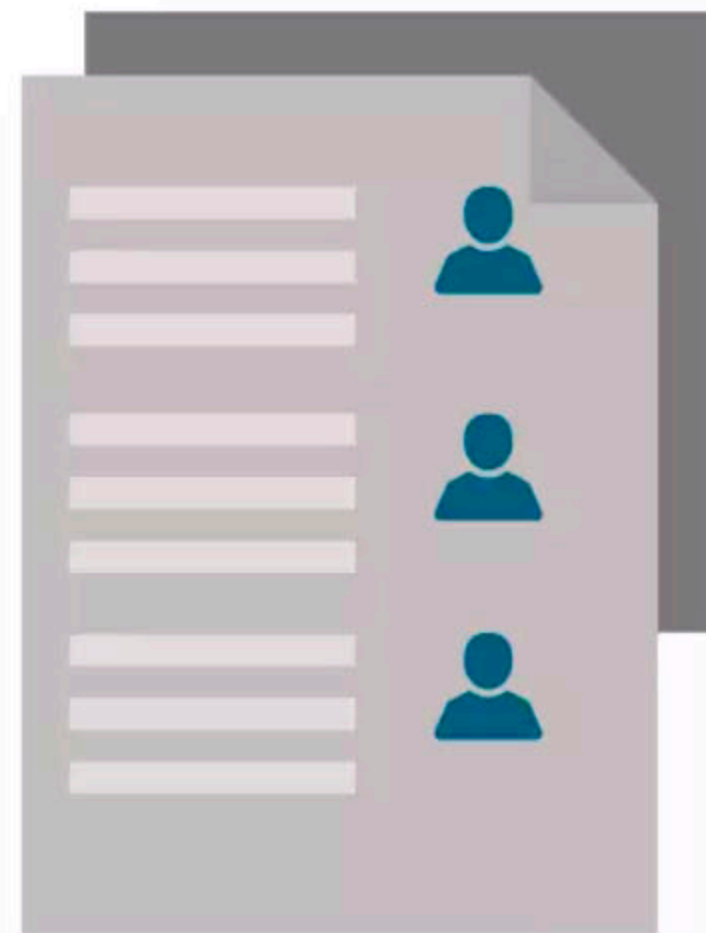
! Mit dem Verzeichnis über die Verarbeitungstätigkeiten dokumentiert das datenverarbeitende Unternehmen zunächst die einzelnen Verarbeitungstätigkeiten fortlaufend. Darin dokumentiert man die Arten der verarbeiteten personenbezogenen Daten, den Kreis der betroffenen Personen, den Zweck der Verarbeitung sowie die Löschfristen. Das Verzeichnis über die Verarbeitungstätigkeiten muss nicht nach außen für Dritte einsehbar sein, jedoch auf Verlangen der Aufsichtsbehörde vorgelegt werden. Einmal angelegt, muss es fortlaufend weitergeführt und aktualisiert werden. Wer über noch keines verfügt, sollte dies schnellstmöglich anfertigen. Je nach unternehmerischer Tätigkeit wird das Verzeichnis so umfangreich, dass man es nicht in wenigen Stunden erstellen kann.

Betroffene Unternehmen

? Wer muss ein Verarbeitungsverzeichnis erstellen?

! Jedes Unternehmen, das von der DSGVO betroffen ist und personenbezogene Daten verarbeitet, muss ein solches Verzeichnis führen. Um

betroffen zu sein, genügt eine Internetpräsenz, bei der man IP-Adressen verarbeitet, die ebenfalls nach dem EuGH als personenbezogene Daten zu qualifizieren sind, oder die Lohnabrechnung bei der Beschäftigung von Mitarbeitern.



Unternehmen, die im Auftrag eines anderen Kunden personenbezogene Daten verarbeiten (Auftragsverarbeiter), müssen ein separates Verarbeitungsverzeichnis für diese Tätigkeit führen. Ist man daher als Auftragsverarbeiter tätig, so ist man verpflichtet, zwei Verarbeitungsverzeichnisse zu führen. Als Auftragsverarbeiter muss man für jeden Auftraggeber separat eine fortlaufende Nummer vergeben sowie die durchzuführenden Tätigkeiten beschreiben.

Korrektter Aufbau

? Wie muss ein Verarbeitungsverzeichnis aufgebaut sein?

! Das Verzeichnis muss alle notwendigen Informationen enthalten. Gemäß Artikel 30 DSGVO gehören zu den notwendigen Informationen auf der ersten Seite des Verzeichnisses:

- Angaben zum Verantwortlichen
- (falls zutreffend) Angaben zum gemeinsamen Verantwortlichen

- (falls zutreffend) Angaben zum Vertreter des Verantwortlichen
- (falls vorhanden) Angaben zur Person des Datenschutzbeauftragten

Sodann müssen zu jeder einzelnen Verarbeitungstätigkeit zwingend folgende Angaben enthalten sein:

- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen
- Beschreibung der Kategorien von personenbezogenen Daten
- Kategorien von Empfängern, denen personenbezogene Daten offengelegt wurden oder noch werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- (falls vorhanden) Angaben zur Übermittlung personenbezogener Daten in Drittstaaten
- Löschfristen

Als Anlage zum Verzeichnis gehört zwingend eine Darstellung der technisch-organisatorischen Maßnahmen (siehe Seite 50).

Die Aufsichtsbehörden haben für das Verarbeitungsverzeichnis ein kostenloses Muster herausgegeben. Alternativ hierzu kann man auch selbst eine Excel-Tabelle anfertigen, die im Anschluss ausgedruckt und unterschrieben wird. Hierbei sollte man jedoch darauf achten, dass innerhalb der Excel-Tabelle mindestens alle Punkte der Musterformulare der Aufsichtsbehörden enthalten sind.

Für einen datenschutzrechtlichen Laien sind diese Formulare nicht ganz selbsterklärend. Nachfolgend wird das Musterverzeichnis daher genauer

beschrieben und beispielhaft Schritt für Schritt ausgefüllt.

Muster-Beispiel

? Wie fülle ich das Verzeichnis aus?

! Das Verzeichnis über die Verarbeitungstätigkeit beginnt immer mit einem Deckblatt (siehe [ct.de/wf9x](https://www.ct.de/wf9x)). Auf dem Deckblatt werden zunächst Angaben zum Verantwortlichen gemacht. Verantwortlicher ist dabei immer das Unternehmen. Bei Einzelunternehmen ist der jeweilige Inhaber Verantwortlicher im Sinne der DSGVO. Handelt es sich um eine GmbH, AG, GbR oder UG, so ist die juristische Person verantwortlich für die Verarbeitung und entsprechend einzutragen.

„Angaben zum ggf. gemeinsam mit diesem Verantwortlichen“ wird dann ausgefüllt, wenn man mit einem anderen Unternehmen Daten zusammen verarbeitet. Dies können entweder Kooperationspartner sein, mit denen man beispielsweise bei Gewinnspielen Daten gemeinsam erhebt oder auch konzernverbundene Unternehmen, mit denen die Daten zusammen erhoben werden. Wenn keine gemeinsame Datenverarbeitung stattfindet, kann dieser Punkt leer gelassen werden.

Die Angaben zum Datenschutzbeauftragten sind dann zu tätigen, wenn ein interner oder externer Datenschutzbeauftragter bestellt wurde. Ab wann ein externer Datenschutzbeauftragter zu bestellen ist, lesen Sie ab Seite 74. Falls keine Pflicht zur Bestellung eines Datenschutzbeauftragten be-

So bleiben Ihre Daten im Netz sicher und privat



Auch als
Heft + PDF
erhältlich mit
22 % Rabatt



> Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

 **heise shop**

shop.heise.de/ct-datenschutz20 >



steht, kann dieses Feld ebenfalls ausgelassen werden.

Nach dem Ausfüllen des Deckblatts geht es nun ans „Eingemachte“. Im nächsten Schritt wird das Musterverzeichnis für jede einzelne Verarbeitungstätigkeit ausgefüllt. Exemplarisch nehmen wir als eine Verarbeitungstätigkeit die „Beschäftigung von Mitarbeitern“. Dies ist entsprechend oben im Feld einzutragen und bekommt eine fortlaufende Nummer, hier exemplarisch die Nummer 1.

Unter „Datum der Einführung“ ist einzutragen, ab wann mit der Verarbeitungstätigkeit begonnen wurde. Dies wäre für die Beschäftigung von Mitarbeitern das Datum, an dem der erste Mitarbeiter eingestellt wurde.

Sodann sind Angaben zur jeweiligen Verantwortlichen Fachabteilung (falls vorhanden) zu machen. Dies ist in der Regel die Personalabteilung oder wenn keine vorhanden ist, die Geschäftsführung.

Unter „Zwecke der Verarbeitung“ wäre beispielsweise die „Durchführung der Arbeitsverträge“ einzutragen. Denn ohne personenbezogene Daten des jeweiligen Mitarbeiters zu erheben und zu verarbeiten, kann weder eine Lohnabrechnung erstellt noch das Gehalt überwiesen werden.

„Betroffene Personen der Verarbeitung“ sind in diesem Fall selbstverständlich die Beschäftigten des verantwortlichen Unternehmens. Bei den Angaben über die „Kategorien der personenbezogenen Daten“ ist eine genaue Analyse der erhobenen Daten erforderlich, um bei der Dokumentation keine Daten zu vergessen. Bei Mitarbeitern werden regelmäßig folgende Kategorien von Daten erhoben:

- Name, Anschrift, Telefonnummer
- Geburtsdatum
- Steuer-/Sozialversicherungsnummer
- Kontonummer

Je nachdem für welche Tätigkeit der jeweilige Mitarbeiter eingesetzt wird, können durchaus auch weitere Kategorien von Daten dazukommen. Bei Sicherheitsunternehmen zum Beispiel wird regelmäßig auch ein polizeiliches Führungszeugnis verlangt.

Augenmerk ist zwingend auf die besonderen Kategorien von personenbezogenen Daten zu legen. Dabei handelt es sich um äußerst sensible Daten wie Her-

kunft, Gewerkschafts- oder Religionszugehörigkeit. Wegen der Abführung der Kirchensteuer wird letztere bei Mitarbeiterdaten immer miterfasst und in der Dokumentation öfters übersehen.

Bei diesen „Besonderen Kategorien“ muss das Schutzniveau bei den technisch-organisatorischen Maßnahmen (TOMs) zwangsläufig höher sein als bei „normalen Daten“, da bei unberechtigtem Zugriff für die betroffene Person erhebliche Schäden drohen können.

Anschließend ist auszufüllen, wer im Unternehmen bei der Verarbeitung Zugriff auf die jeweiligen personenbezogenen Daten hat. Intern ist es zumindest bei Mitarbeiterdaten die Personalabteilung und/oder Geschäftsführung. Bei einer umfangreichen Digitalisierung der Mitarbeiterakten kann aber auch die jeweilige IT-Abteilung Zugriff auf die Daten haben.

Weiterhin ist zu dokumentieren, ob die Daten an externe Empfänger weitergegeben werden und zu welcher Kategorie die externe Stelle gehört. Bei Mitarbeiterdaten könnte dies zum Beispiel eine Lohnbuchhaltung als Auftragsverarbeiter sein. Rechtsanwälte und Steuerberater fallen nach der derzeit überwiegenden Auffassung nicht unter die Auftragsverarbeiter.

Sodann ist einzutragen, ob die externe Stelle in einem Drittland außerhalb der EU sitzt oder eine internationale Organisation Empfänger der Daten ist. Sitzt die Lohnbuchhaltung zum Beispiel in den USA, wäre zusätzlich vor einer Übermittlung zu prüfen, ob die jeweilige Datenweitergabe überhaupt zulässig ist (siehe Seite 108). Grundsätzlich ist eine Übermittlung von personenbezogenen Daten ins Ausland, insbesondere bei sensiblen personenbezogenen Daten, mit Vorsicht zu genießen.

Übermittelt man personenbezogene Daten in ein Drittland oder an eine internationale Organisation, dokumentiert man im nächsten Formularfeld, wie und an wen dies geschieht. Hier ist grundsätzlich Vorsicht geboten, weil häufig Dienstleister mit Sitz in den USA schlicht übersehen werden, beispielsweise bei der Nutzung amerikanischer Clouds wie Dropbox. Man



sollte deshalb unbedingt sämtliche Dienstleister genau überprüfen, ob eine Auslandsübermittlung stattfindet.

In diesen Fällen sind auch „geeignete Garantien“ zu dokumentieren, die in Artikel 46 DSGVO geregelt sind. Dies wäre regelmäßig eine Zertifizierung nach „Privacy-Shield“ oder „EU-Standardvertragsklauseln“. Kooperiert man mit Unternehmen zum Beispiel in den USA, muss zwingend mindestens eines von beiden vorliegen.

Am Ende des Verarbeitungsverzeichnisses sind die Löschfristen zu dokumentieren. Die DSGVO verfolgt unter anderem den Grundsatz der Datensparsamkeit. Personenbezogene Daten dürfen daher grundsätzlich nur so lange aufbewahrt werden, wie diese für den jeweiligen Zweck erforderlich sind. Nicht mehr benötigte Daten sind umgehend zu löschen.

Im Fall von Mitarbeiterdaten bedeutet dies: Die Daten werden nur so lange verarbeitet, wie sich der jeweilige Mitarbeiter im Anstellungsverhältnis befindet. Kündigt der Mitarbeiter, so braucht der Arbeitgeber die Daten grundsätzlich nicht mehr zur Durchführung des Arbeitsverhältnisses.

Dies führt aber nicht automatisch zur Löschung. Bei fast jeder Verarbeitungstätigkeit stehen unter Umständen gesetzliche Aufbewahrungsfristen entgegen. Ein Klassiker sind Aufbewahrungspflichten aus dem Bereich der Steuern. Rechnungen sind 10 Jahre aufzubewahren. Ähnlich verhält es sich mit den Lohnabrechnungen der Mitarbeiter. Eine kom-

plette Löschung darf daher erst nach 10 Jahren erfolgen.

Einen Sonderfall bilden Bewerberdaten. Hier hat man regelmäßig keine Abrechnungen erstellt. Wegen der Datensparsamkeit sind daher Bewerberdaten zwingend zu löschen, sobald entweder die ausgeschriebene Stelle besetzt ist oder der Bewerber eine Absage erhalten hat. Bewerberdaten sollten nicht in einem internen Fachkräftepool gesammelt werden getreu dem Motto „vielleicht brauchen wir den später einmal“. Will man Bewerberdaten länger speichern als für den Bewerbungsprozess erforderlich, so muss man eine Einwilligung der betroffenen Person einholen.

Die Vorgehensweise und die Fristen unterscheiden sich bei der Verarbeitung von Bewerberdaten deutlich von der Verarbeitung normaler Mitarbeiterdaten. Den Umgang mit ihnen dokumentiert man daher als separate Verarbeitungstätigkeit „Bewerbungen“ nach dem oben genannten Schema ebenso wie alle weiteren Verarbeitungen personenbezogener Daten, die man bei der systematischen Überprüfung aller Vorgänge gefunden hat.

Fügt man dann noch die geforderte Darstellung der technisch-organisatorischen Maßnahmen hinzu, kann das Verarbeitungsverzeichnis recht umfangreich ausfallen. Viele Verarbeitungsprozesse sind einem im Alltag gar nicht bewusst. Hier hilft ein sorgfältig zusammengestelltes Verarbeitungsverzeichnis, da es dem Unternehmen regelmäßig vor Augen führt, wo und welche Daten verarbeitet werden. (anm) **ct**

**Musterverzeichnis
und Übersicht Auf-
bewahrungsfristen:**

ct.de/wf9x

Datenschutzkonform ins Jahr 2021 mit dem audatis MANAGER Datenschutzmanagement-Software & E-Learning

Der audatis MANAGER führt Sie sicher durch die EU-Datenschutz-Grundverordnung (DS-GVO) und das Bundesdatenschutzgesetz (BDSG). Mit unserer Datenschutzmanagement-Software bekommen Sie den Datenschutz in den Griff. Mit seinen zahlreichen Funktionen ermöglicht es der audatis MANAGER auf einfache, aber effektive Weise, alle gesetzlichen Ansprüche zu erfüllen und die Mitarbeiter mit E-Learnings zu sensibilisieren.

Testen Sie den audatis MANAGER 30 Tage kostenlos unter:
<https://www.audatis-manager.de/dsgvo2021/>



webbasiert



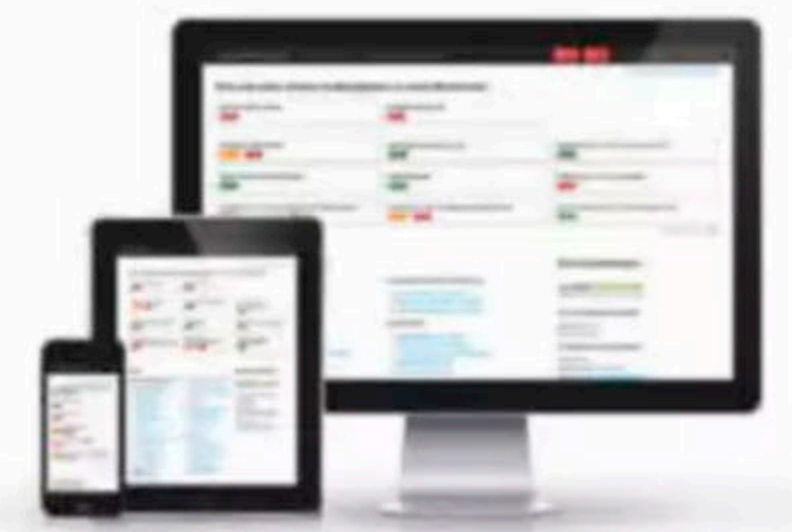
einfach



dokumentenorientiert



mandantenfähig



audatis[®] MANAGER
Datenschutzmanagement einfach online

Datenschutz- erklärung

Jeder kennt sie, doch kaum einer macht sich die Mühe, sie zu lesen: die Datenschutzerklärung. Trotzdem gehört der auch Privacy Policy genannte Text für Unternehmen zum datenschutzrechtlichen Standard-Repertoire. Wer hier schlampt, begeht einen der offensichtlichsten Datenschutzverstöße.



Von Nick Akinci

Jedes Unternehmen muss unabhängig von seiner Größe alle Betroffenen darüber informieren, wie es ihre personenbezogenen Daten verarbeitet. Hierzu ist es gängige Praxis, auf der Unternehmenswebsite eine Datenschutzerklärung zu veröffentlichen. Die DSGVO schlägt diese Vorgehensweise in den Erwägungsgründen auch ausdrücklich vor.

Im Internet findet sich eine Fülle an Musterdatenschutzerklärungen, die vermeintlich alles abdecken, was in den Datenschutzhinweisen enthalten sein muss. Ebenfalls erfreuen sich Datenschutzerklärungs-Generatoren großer Beliebtheit. Der Nutzer wird dabei meist aufgefordert, bestimmte Informationen über seine Website, wie das Vorhandensein eines Kontaktformulars oder von Tracking-Software, in eine Maske einzugeben. Am Ende erhält er – so wird es versprochen – eine auf seine Belange abgestimmte individuelle Datenschutzerklärung.

Hier ist jedoch Vorsicht geboten. Jede Website ist anders aufgebaut und kann Besonderheiten aufweisen, die in den Mustererklärungen nicht oder falsch dargestellt werden. Außerdem wird regelmäßig vergessen, dass im Zweifel nicht nur über die

auf der Website stattfindenden Datenverarbeitungen zu informieren ist (siehe Seite 148), sondern auch über alle sonstigen datenschutzrelevanten Vorgänge im Unternehmen. In bestimmten Fällen kann es sinnvoll sein, die Betroffenen in einer abschließenden Datenschutzerklärung umfassend gleich über alle im Unternehmen und auf der Website stattfindenden Datenverarbeitungsvorgänge zu informieren. Sucht man Unterstützung bei der Erstellung der Datenschutzerklärung, kann es daher ratsam sein, einen auf Datenschutzrecht spezialisierten Juristen zu Rate zu ziehen.



Zentrale Regelung

Für den Fall, dass personenbezogene Daten bei der betroffenen Person erhoben werden, regelt die DSGVO die Informationspflichten zentral und abschließend in Artikel 13. Die Vorschrift unterscheidet dabei zwischen Pflichtinformationen auf der einen Seite (Abs. 1) und „weiteren Informationen“ auf der anderen (Abs. 2). Letztere sind dem Betroffenen nur dann mitzuteilen, wenn sie „notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten“. Aufgrund des großen Interpretationsspiel-

raums, den diese Formulierung zulässt, wird es jedoch schwierig oder gar unmöglich sein, diese Unterscheidung rechtssicher zu treffen. Es ist daher dringend angeraten, auch diese weiteren Informationen zu vermitteln, weshalb im Folgenden nicht zwischen den beiden Kategorien unterschieden wird.

In zeitlicher Hinsicht müssen die Betroffenen bereits ab dem Zeitpunkt der Erhebung informiert werden. Auf die Erfüllung von Informationspflichten kann man nur verzichten, „wenn und soweit die betroffene Person bereits über die Information verfügt“.

Verantwortlicher und Datenschutzbeauftragter

Zunächst sind dem Betroffenen der Name und die Kontaktdaten des datenschutzrechtlich Verantwortlichen mitzuteilen. Dies ist in der Regel das Unternehmen, in dem die Datenverarbeitungen stattfinden. Es sollte hierzumindest der Unternehmensname inklusive der Rechtsform beziehungsweise der Name des Einzelunternehmers, die Anschrift und eine E-Mail-Adresse genannt werden.

Ist im Unternehmen ein Datenschutzbeauftragter vorhanden, so sind ebenso dessen Kontaktdaten aufzuführen. Dieser muss jedoch nicht namentlich benannt werden – es reicht aus, wenn eine E-Mail-Adresse genannt wird, unter welcher der Datenschutzbeauftragte direkt erreichbar ist.

Rechtsgrundlage und Verarbeitungszwecke

Weiterhin ist dem Betroffenen mitzuteilen, zu welchen Zwecken die einzelnen Datenverarbeitungen stattfinden. Der Betroffene soll wissen können, wozu seine Daten verarbeitet werden, um sich ein Bild darüber verschaffen zu können, was mit den ihn betreffenden Informationen geschieht.

Eine weitere wesentliche Pflicht besteht in der Nennung der Rechtsgrundlage für die Datenverarbeitung(en). Als wichtigste Rechtsgrundlagen sind bereits im Artikel ab Seite 16 die Verarbeitung zur Erfüllung eines Vertrages mit dem Betroffenen, die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten und die Einwilligung des Betroffenen genannt worden. Die Rechtsgrundlage muss dabei für jeden einzelnen Datenverarbeitungsvorgang präzise benannt werden.

Beruft sich das Unternehmen zur Nutzung von Informationen auf eigene berechnete Interessen,

hat es nicht nur die entsprechende Rechtsgrundlage anzugeben, sondern auch die Interessen, die es mit der Verarbeitung verfolgt. Im Falle der vorübergehenden Speicherung von IP-Adressen wäre das berechnete Interesse etwa die Betriebssicherheit der Website.

Weitergabe der Daten

Bei der Weitergabe von personenbezogenen Daten an unternehmensexterne Dritte ist der Betroffene über die Empfänger der erhobenen Daten zu benachrichtigen. Nutzt beispielsweise der Betreiber eines Online-Shops einen externen Zahlungsdienstleister für die Abwicklung der Bezahlung der Waren, so ist der Käufer darüber zu informieren, dass der Dienstleister die erforderlichen Zahlungsdaten erhält.

Außerdem ist auch darüber zu informieren, ob der Verarbeitende die Daten an Server im Nicht-EU-Ausland übermitteln will. Ist dies der Fall, so muss weiterhin darüber informiert werden, worauf sich die Drittstaatenübermittlung stützt. Grundlage kann etwa ein Angemessenheitsbeschluss der EU-Kommission sein. Der für die USA bisher bestehende Angemessenheitsbeschluss, welcher auf dem sog. Privacy-Shield-Abkommen beruhte, ist nunmehr aufgrund des Urteils des EuGH vom 16. Juli 2020, Az.: C-311/18 unwirksam, sodass ein Verweis hierauf nunmehr nicht mehr ausreicht. Mehr zum Thema Privacy Shield und den Grundlagen, auf die eine Drittstaatenübermittlung gestützt werden kann, lesen Sie ab Seite 108.



Speicherdauer und Betroffenenrechte

Darüber hinaus soll der Nutzer erfahren, wie lange Daten über ihn gespeichert werden. Es gilt die Faustregel: Benötigt man die Daten nicht mehr, sind sie zu löschen. Die aus Sicherheitsgründen nötige Nutzer-IP-Adresse sollte man beispielsweise nicht länger als 14 Tage speichern. Kann man keinen festen

Zeitraum angeben, sind die Kriterien für die Speicherdauer zu nennen.

Der Betroffene muss weiterhin auch über alle ihm nach der DSGVO zustehenden Rechte „belehrt“ werden, die umfassend im dritten Kapitel der DSGVO geregelt sind. Details zu den Betroffenenrechten finden Sie ab Seite 22. Dabei ist es grundsätzlich ausreichend, schlicht auf das Bestehen der verschiedenen Rechte hinzuweisen. So ist es zum Beispiel beim Beschwerderecht nicht notwendig, dass auch die zuständige Datenschutzbehörde benannt wird. Beim Widerspruchsrecht gilt die Besonderheit, dass die Information darüber von den anderen getrennt zu erfolgen hat. Eine optische Hervorhebung durch Rahmung oder Fettdruck sollte hierbei aber ausreichend sein.

Verständlichkeit steht an erster Stelle

Für alle vorgenannten Informationspflichten gilt der Grundsatz, dass die Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher

Form in einer klaren und einfachen Sprache zu übermitteln“ sind. Der Link zur Datenschutzerklärung sollte gut sichtbar auf der Startseite des Webauftritts stehen.

Im Text sollten juristische Fachbegriffe vermieden oder zumindest erklärt werden. Der Text muss in Deutsch und – je nach Kundenkreis – auch in weiteren Sprachen abgefasst sein. Das bedeutet, dass beispielsweise ein deutscher Online-Shop, der neben der deutschen auch in englischer Sprache verfügbar ist und einen Versand in das Vereinigte Königreich anbietet, sowohl eine deutsche, als auch eine englische Version der Datenschutzerklärung zum Abruf bereithalten muss.

Bezüglich des Textumfangs muss die Datenschutzerklärung in der Praxis mitunter einen Spagat zwischen umfassender Information und Verständlichkeit meistern. Je nachdem, welche und wie viele Datenverarbeitungen im Unternehmen stattfinden, kann sie schnell mehrere Seiten lang werden. Der Text sollte bei einer besonders umfangreichen Datenschutzerklärung klar und übersichtlich gegliedert sein. Es bietet sich dann auch an, Details aus dem

Mindestangaben

- 
- ✓ Name und Kontaktdaten des Unternehmens als verantwortliche Stelle
 - ✓ alle Zwecke, zu denen personenbezogene Daten verarbeitet werden
 - ✓ Rechtsgrundlagen für die Datenverarbeitung
 - ✓ Speicherdauer
 - ✓ Betroffenenrechte

Einzelfallbezogene Informationspflichten

- 
- ✓ Kontaktdaten des Datenschutzbeauftragten
 - ✓ berechnete Interessen, die mit der Datenverarbeitung verfolgt werden
 - ✓ Empfänger (Dritte), an die erhobene Daten übermittelt werden
 - ✓ Absicht, die Daten ins Nicht-EU-Ausland zu übertragen, und das Vorhandensein oder Fehlen eines Datenschutzabkommens mit dem Zielland
 - ✓ Verpflichtung zur Bereitstellung der Daten und Folgen der Nichtbereitstellung
 - ✓ Bestehen einer automatisierten Entscheidungsfindung

Checkliste für die Datenschutzerklärung

Haupttext ausgliedern und über Links für interessierte Kunden und Nutzer an separater Stelle vorzuhalten.

Eine Verletzung der Informationspflichten kann mit empfindlichen Geldbußen geahndet werden. Als Obergrenze legt die DSGVO 20 Millionen Euro respektive vier Prozent des gesamten weltweit erzielten Jahresumsatzes fest, je nachdem was höher ist. Es ist jedoch davon auszugehen, dass die Aufsichtsbehörden diesen Spielraum bei Verstößen gegen die Informationspflichten nicht voll ausschöpfen werden, da hierdurch in der Regel keine nennenswerten Schäden entstehen.

Informationspflichten ernst nehmen

Weiterhin drohen bei Verstößen unter Umständen Abmahnungen von Konkurrenten oder „Abmahnvereinen“. Es ist noch immer umstritten, ob eine fehlende oder unzureichende Datenschutzerklärung als Wettbewerbsverstoß durch Mitbewerber

abgemahnt werden kann. Einige Gerichte haben eine Abmahnbarkeit jedoch bejaht. Allerdings kann hinsichtlich des Kostenrisikos, welches mit derartigen Abmahnungen einhergeht, in gewisser Weise Entwarnung gegeben werden. Das „Gesetz zur Stärkung des fairen Wettbewerbs“, welches am 02.12.2020 in Kraft getreten ist, sieht vor, dass Abmahner in solchen Fällen die Abmahnkosten von Unternehmen und gewerblich tätigen Vereinen, die in der Regel weniger als 250 Mitarbeiter beschäftigen, nicht erstattet verlangen können.

Unternehmen sollten daher genau prüfen, ob und wie sie personenbezogene Daten verarbeiten. Bei der Anpassung der Datenschutzerklärung kann man sich direkt am Gesetzestext orientieren, da Art. 13 der DSGVO die Informationspflichten nunmehr zentral katalogisiert aufführt. Darüber hinaus können die auf der linken Seite abgebildeten Checklisten dabei helfen, die Datenschutzerklärung zu vervollständigen. (keh) 

Informationspflichten:

[ct.de/wcgy](https://www.ct.de/wcgy)

 Minds Mastering Machines

DIE **ONLINE-KONFERENZ** FÜR
MACHINE LEARNING UND KI

Im Frühjahr 2021 werden wir die Minds Mastering Machines als **Online-Veranstaltung** an mehreren Tagen durchführen. Details zur Ausrichtung finden sich auf der Website, und wer auf dem Laufenden bleiben möchte, sollte den Newsletter abonnieren:

www.m3-konferenz.de/newsletter.php

Im Call for Proposals suchen die Veranstalter ab sofort Vorträge für 2021:

www.m3-konferenz.de/call_for_proposals.php

Veranstalter



 heise Developer

 dpunkt.verlag



TOMs dokumentieren

Wer personenbezogene Daten verarbeiten will, muss sich genau überlegen, wie er dies tut, und die zu ihrem Schutz getroffenen Maßnahmen dokumentieren.

Von Brian Scheuch

Sinn und Zweck der TOMs

? Wozu dient die Dokumentation der technisch-organisatorischen Maßnahmen?

! Um ein dem jeweiligen Risiko angemessenes Schutzniveau zu gewährleisten, ergreift jedes datenverarbeitende Unternehmen technisch-organisatorische Maßnahmen (TOMs, siehe auch Seite 124). Was konkret unternommen wird, um den Schutz personenbezogener Daten zu gewährleisten, muss das Unternehmen dokumentieren und regelmäßig überprüfen, ob der Schutz noch angemessen ist. Diese Dokumentation der TOMs ist in der Regel kein Hexenwerk. Viele Punkte sollten für die meisten Unternehmen bereits Selbstverständlichkeiten sein – spätestens seit dem 25.05.2018.

Die TOMs selbst bestehen aus zwei Komponenten: Zu den technischen Maßnahmen zählen zum Beispiel abschließbare Büroräume, Backups oder Sicherungen der IT-Infrastruktur. Unter organisatorische Maßnahmen fällt alles, was dem Schutz der Daten abseits der Technik dient, beispielsweise Sensibilisierung und Schulung von Mitarbeitern.

Die Anforderungen an die TOMs steigen, je mehr personenbezogene Daten verarbeitet werden oder je sensibler die personenbezogenen Daten sind.

Wer noch nicht angefangen hat, die TOMs zu dokumentieren, sollte dies nachholen. Die Höhe des notwendigen Schutzniveaus klärt man zuvor mit der Erstellung des Verarbeitungsverzeichnisses (siehe Seite 42).

Am richtigen Ort

? Wo sind die TOMs zu dokumentieren?

! Artikel 30 Abs. 1 lit. g) DSGVO verlangt, dass im Verarbeitungsverzeichnis wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO zu erfolgen hat. Die Aufsichtsbehörden vertreten die Auffassung, dass die TOMs zwingender Bestandteil des Verzeichnisses sind. Diese werden in der Regel als Anlage zum Verzeichnis dokumentiert.

Die TOMs sind ferner auch zwingender Bestandteil bei der Auftragsverarbeitung (siehe Seite 56). Artikel 28 Abs. 3 lit. c) DSGVO verlangt, dass der Auftragsverarbeiter alle in Art. 32 DSGVO erforderlichen Maßnahmen ergreift. Dazu gehören auch die TOMs, die wie beim Verarbeitungsverzeichnis als Anlage dokumentiert werden.

Zwingende Bestandteile

? Was muss dokumentiert werden?

! Bei der Dokumentation der technisch-organisatorischen Maßnahmen sind gemäß Art. 32 Abs. 1 DSGVO zwingend folgende Punkte zu darstellen:

- Pseudonymisierung und Verschlüsselung von personenbezogenen Daten
- Sicherstellung der Vertraulichkeit
- Sicherstellung der Integrität
- Sicherstellung der Verfügbarkeit
- Sicherstellung der Belastbarkeit
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Kein unbefugter Zugriff

? Was versteht man unter Vertraulichkeit?

! Unter Vertraulichkeit werden in den TOMs alle Maßnahmen aufgelistet, die sicherstellen sollen, dass personenbezogene Daten ausschließlich einem bestimmten Empfängerkreis zugänglich sind. Dazu gehören regelmäßig:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffsberechtigung
- Trennungskontrolle
- weitere Maßnahmen

Unter Zutrittskontrolle werden alle Maßnahmen aufgelistet, die erforderlich sind, damit unberechtigte Dritte keinen Zugang zu Datenverarbeitungsanlagen des jeweiligen Unternehmens erhalten. Zu den klassischen Maßnahmen bei der Zutrittskontrolle gehören:

- abschließbare Geschäftsräume (Schließsystem mit Sicherheits-schlössern, Zugangscode etc.)
- Alarmanlagen
- abschließbare Büroräume der einzelnen Fachabteilungen
- Schlüsselregelung bei Beschäftigten
- Empfangskontrolle (Besucherempfang)

Die Maßnahmen müssen, wie eingangs erwähnt, geeignet sein und im angemessenen Verhältnis zu der Verarbeitungstätigkeit und der Größe des Unternehmens stehen. Es kann beispielsweise von einem 2-Mann-Unternehmen regelmäßig nicht verlangt werden, aus seinen Geschäftsräumen einen „Hochsicherheitstrakt“ zu machen oder alle personenbezogenen Daten in einem mehrere Tonnen schweren Safe zu lagern.

Das Sicherheitsniveau muss jedoch dann steigen, wenn besonders sensible personenbezogene Daten verarbeitet werden oder überdurchschnittlich viele. Dann reicht eine Sicherung mittels einfachen Schlosses kaum aus.

Bei der Zugangskontrolle werden alle technischen und organisatorischen Maßnahmen dokumentiert, die geeignet sind, die Nutzung der Datenverarbeitungssysteme, klassischerweise der Computer, durch Unbefugte zu verhindern. Auch hierbei handelt es sich um Maßnahmen, die fast jedes Unternehmen ohnehin schon umsetzt, wie:

- Login mit Benutzername und Passwort
- Firewalls
- Antivirenprogramm
- Verwendung von sicheren Passwörtern (Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen)
- automatische Desktop-Sperre bei Abwesenheit
- abschließbare Computer-Gehäuse
- Verschlüsselung der Festplatten
- VPN bei Remote-Tätigkeiten

Separate Logins und Passwörter, eine aktuelle Firewall sowie ein Antivirenprogramm sind das unbedingte Minimum und sollten von jedem Unternehmen umgesetzt werden. Gerade diese Anforderungen sind auch für jedes Unternehmen bezahlbar, wenn nicht sogar kostenlos erfüllbar.

Bei der Zugriffskontrolle listet man alle Maßnahmen auf, die den Zugriff auf personenbezogene Daten ausschließlich nur auf die jeweils Berechtigten beschränken. Dies bedeutet insbesondere bei größeren Unternehmen, dass beispielsweise nur die Personalabteilung und / oder die Geschäftsführung auf Personalakten zugreifen können und andere Abteilungen nicht einmal Einblick in solche Daten haben. Um dies sicherzustellen, gehört zur Zugriffskontrolle insbesondere

auch das sichere Löschen von Daten, damit diese nicht von Unberechtigten aus dem Mülleimer „gefischt“ werden. Zu den klassischen Maßnahmen zählen daher:

- zuverlässig umsetzbare Berechtigungskonzepte
- Beschränkung der Anzahl der Administratoren auf ein Minimum
- Aktenschredder (mind. Kreuzschnitt)



- richtiges Löschen oder Vernichten von Datenträgern (spezielle Löschrprogramme oder zertifizierte Vernichtung der nicht mehr benötigten Datenträger)

Auch hier gilt: Ein Aktenschredder ist das unbedingte Minimum, auch für kleine Unternehmen.

Das Unternehmen muss ferner durch geeignete Maßnahmen sicherstellen, dass eine Trennungskontrolle stattfindet. Diese soll sicherstellen, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden.

Ein häufiger Anwendungsfall wäre beispielsweise ein Online-Shop, der personenbezogene Daten einerseits für Newsletter verarbeitet und andererseits für die Versendung von gekauften Artikeln.

Klassische Maßnahmen zur Trennung der Datenverarbeitungen sind:

- physikalische Trennung von Datenbanken oder der Datenträger
- Festlegung von unterschiedlichen Datenbankrechten

Unter dem Punkt Weitere Maßnahmen werden anderweitige Maßnahmen zum Schutz der personenbezogenen Daten dokumentiert, wie beispielsweise Anonymisierung und Pseudonymisierung von personenbezogenen Daten. Aber auch Sensibilisierung und Schulung der Mitarbeiter sind ebenso wichtige organisatorische Maßnahmen. An ihnen sollte man nicht sparen, damit Mitarbeiter sicher wissen, was sie im Rahmen der DSGVO dürfen und was nicht.

Unverfälschte Daten

? Was versteht man unter Integrität?

! Unter dem Punkt Integrität ist zu dokumentieren, wie man zu verhindern sucht, dass Daten verfälscht werden können. Die zwei wesentlichen Punkte hierzu sind:

- Weitergabekontrolle
- Eingabekontrolle

Bei der Weitergabekontrolle listet das Unternehmen alle Maßnahmen auf, die gewährleisten sollen, dass personenbezogene Daten während des Transports von unbefugten Dritten nicht gelesen, kopiert, ver-

ändert oder gelöscht werden können. Klassische Maßnahmen wären:

- Verschlüsselungen der Daten (E-Mails, Festplatten)
- Einsatz von VPN
- verschlüsselte Verbindungen (z. B. https)
- sichere Transportbehälter
- Sorgfalt bei der Auswahl von externen Dienstleistern

Hierbei ist anzumerken, dass auf einer Website, die personenbezogene Daten mittels Kontaktformular erhebt, mindestens eine SSL-Verschlüsselung (https) absolute Pflicht ist.

Die Eingabekontrolle soll festhalten, von wem die Daten in ein Datenverarbeitungssystem aufgenommen, verändert oder entfernt worden sind. Die Protokollierung soll gewährleisten, dass man überprüfen kann, dass Daten nicht von Unberechtigten verfälscht worden sind. Klassische Maßnahmen sind:

- Log-Daten bei der Änderung von personenbezogenen Daten
- Nachvollziehbarkeit der Änderung, Löschung und Eingabe
- Einführung eines Berechtigungskonzeptes

Sicher aufbewahren

? Was versteht man unter Verfügbarkeit?

! Wenn personenbezogene Daten verarbeitet werden, muss das datenverarbeitende Unternehmen Maßnahmen treffen, die sicherstellen, dass personenbezogene Daten nicht einfach „abhandenkommen“ oder zufällig zerstört werden. Geeignete Maßnahmen können sein:

- Backups
- Feuer- und Rauchmeldeanlagen
- Sprinkleranlage
- Überwachung und Klimatisierung des Serverraumes
- Spiegelung der Festplatten
- Notfallplan

Grundsätzlich kann von jedem Unternehmen verlangt werden, Backups zu erstellen, die es ermöglichen, die Daten wiederherzustellen – woran aber jedes Unternehmen ohnehin ein Interesse hat. Kol-

lidieren kann diese Forderung jedoch mit dem neu eingeführten „Recht auf Vergessenwerden“. Bei der Planung der Backups muss gleich von vornherein geklärt werden, wie man vorgeht, wenn die betroffene Person eine Löschung begehrt.

Belastbare IT

? Was ist mit dem Punkt „Belastbarkeit“ gemeint?

! Die Belastbarkeit ist streng genommen ein Unterpunkt der Verfügbarkeit. Um eine entsprechende Verfügbarkeit der Daten zu gewährleisten, müssen die Datenverarbeitungsanlagen auch entsprechend belastbar sein. Es müssen demnach geeignete Maßnahmen getroffen werden wie:

- Firewalls (Hard- und Software)
- regelmäßige Stresstests der EDV-Systeme
- sorgfältige Auswahl von IT-Dienstleistern

Regelmäßige Kontrolle



? Wie dokumentiert man die Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der TOMs?

! Im letzten Punkt stellt man die Maßnahmen dar, die die regelmäßige Überprüfung, Bewertung und Evaluierung der TOMs gewährleisten sollen.

Ebenso wie das Verarbeitungsverzeichnis ist die Dokumentation der technisch-organisatorischen Maßnahmen kein einmaliges Projekt. Es muss regelmäßig überprüft werden, ob die festgelegten TOMs noch ein geeignetes Schutzniveau gewährleisten, insbesondere, wenn weitere Verarbeitungsprozesse hinzukommen. Folgende Maßnahmen können dafür getroffen werden:

- regelmäßige Prüfintervalle der EDV
- Prüfung der TOMs insgesamt durch Datenschutzbeauftragten oder Geschäftsführung
- Datenschutzmanagement Software
- Zertifizierungen
- Schulungen und Sensibilisierung der Mitarbeiter
- Datenschutzfolgenabschätzung für einzelne Prozesse (keh) **ct**

Früher war alles besser!



Willkommen in der Welt der Classic Games, wo Computer- und Videospiele viel Kreativität und Spielspaß versprochen – und bis heute halten. Wir stellen Spiele, deren Entwickler und Plattformen vor. Bei Retro Gamer finden Sie Screenshots, Fakten, Tipps und mehr zu den Hits von damals.



Testen Sie 2x Retro Gamer mit 30 % Rabatt!

Lesen Sie 2 Ausgaben für nur 18,- Euro* statt 25,80 Euro* im Handel.

*Preis in Deutschland.

Jetzt bestellen und vom Test-Angebot profitieren:
www.emedia.de/rg-mini

Telefon: [0541] 800 09 126
[werktags von 8-20 Uhr, samstags von 10-16 Uhr],
E-Mail: rg-abo@emedia.de
eMedia Leserservice, Postfach 24 69, 49014 Osnabrück

Datenweitergabe im Unternehmen



Werden personenbezogene Daten innerhalb desselben Unternehmens oder innerhalb eines großen Konzerns weitergegeben, können die Hürden niedriger sein als bei einer Übermittlung an Dritte. Dieser Beitrag zeigt, wann dies der Fall ist und was bei einer solchen Übermittlung zu beachten ist.

Von Nick Akinci

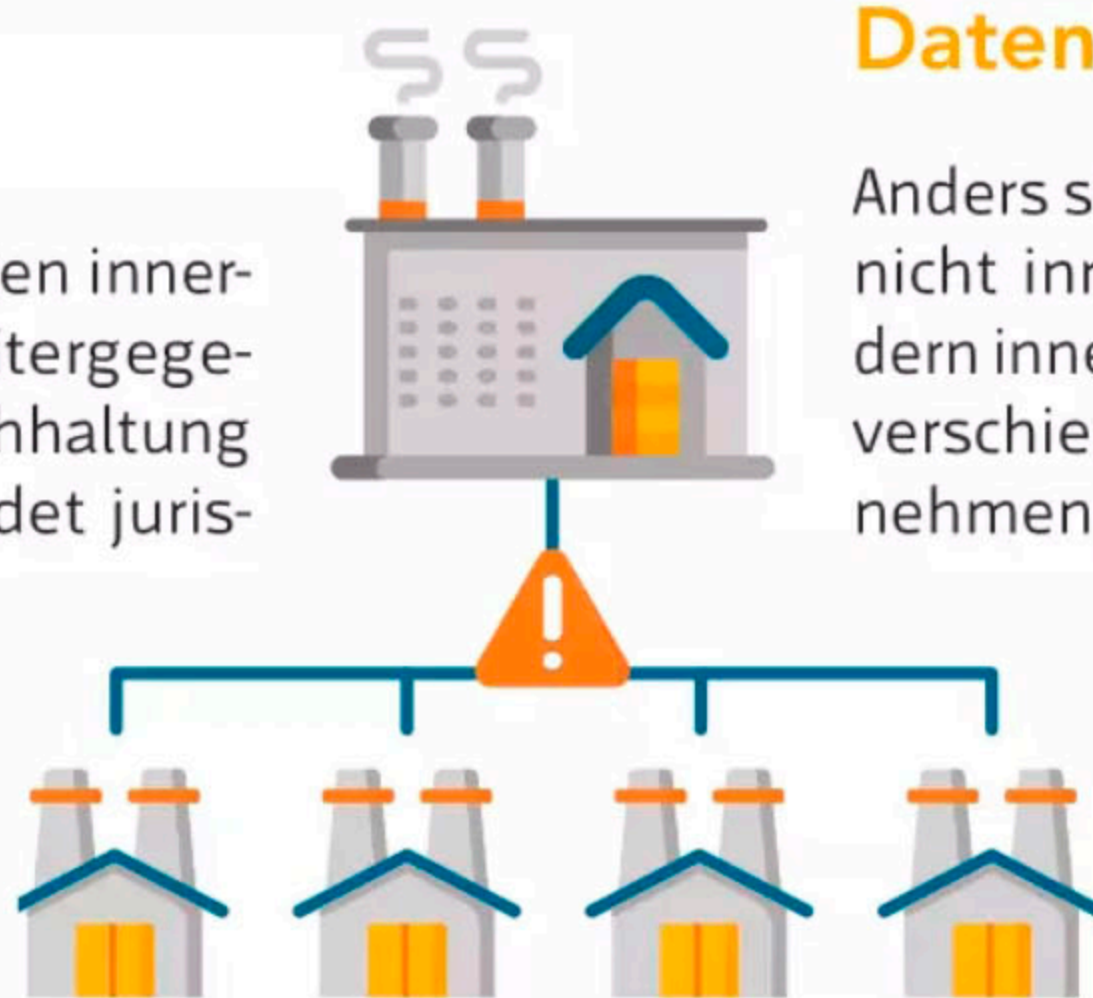
Die Weitergabe von personenbezogenen Daten ist eines der sensibelsten Themen im Bereich des Datenschutzes, da jede Datenübertragung den Kreis derer, die Zugriff auf die betreffenden Daten nehmen können, potentiell vergrößert. In der Regel liegt es im Interesse des Betroffenen, dass seine Daten nur so wenig Empfängern wie möglich offenbart werden. Dies gilt umso mehr, je sensibler diese Daten sind.

keit gebieten es, dass nur die Personen innerhalb eines Unternehmens Zugriff auf die Daten haben sollten, die sich notwendigerweise mit den Daten befassen müssen, um den mit der Verarbeitung verfolgten Zweck zu erreichen. Zum Beispiel muss die Personalabteilung eines Unternehmens selbstverständlich Zugriff auf Bewerberdaten haben – in der Marketingabteilung hätten diese Daten jedoch nichts zu suchen.

Datenweitergabe im Unternehmen

Werden personenbezogene Daten innerhalb eines Unternehmens weitergegeben, zum Beispiel von der Buchhaltung an die Rechtsabteilung, so findet juristisch betrachtet keine Weitergabe an einen Dritten statt. Datenschutzrechtlich ist das Unternehmen als Ganzes die datenverarbeitende Stelle.

Das bedeutet jedoch nicht, dass personenbezogene Daten innerhalb eines Unternehmens „wild herumgereicht“ werden dürfen. Die in der DSGVO verankerten Grundsätze der Datenminimierung und Vertraulich-



Datenweitergabe im Konzern

Anders sieht es aus, wenn der Datentransfer nicht innerhalb eines Unternehmens, sondern innerhalb eines Konzerns zwischen zwei verschiedenen konzernangehörigen Unternehmen stattfindet. Da es sich in diesem Fall um zwei verschiedene juristische Personen handelt, ist das empfangende Unternehmen zunächst einmal als „Dritter“ im Sinne des Datenschutzrechts zu werten.

Um die Übermittlung innerhalb eines solchen Unternehmensverbunds zu erleichtern, hält der Datenschutz hier allerdings Vereinfachungen für „Unternehmensgruppen“ bereit. Die DSGVO definiert in Art. 4 Nr. 19

den Begriff der Unternehmensgruppe als „eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht“. Diese Definition ähnelt der Definition des Konzerns in § 18 des deutschen Aktiengesetzes (AktG) so stark, dass man davon ausgehen kann, dass ein Konzern in aller Regel dem datenschutzrechtlichen Begriff der Unternehmensgruppe unterfallen wird.

Wie für jede Verarbeitungstätigkeit, braucht es auch für die Weitergabe von Daten stets einer Rechtsgrundlage. Eine Einwilligung der Betroffenen ist bei der konzerninternen Datenweitergabe in der Regel wenig sinnvoll. Viel zu umständlich wäre es, jeden Kunden oder Geschäftspartner um seine Zustimmung zur Weitergabe an die verbundenen Unternehmen zu bitten. Wenn es um Beschäftigendaten geht, kann sich jedoch die Einholung einer Einwilligung der Arbeitnehmer in Form einer (Konzern-) Betriebsvereinbarung anbieten.

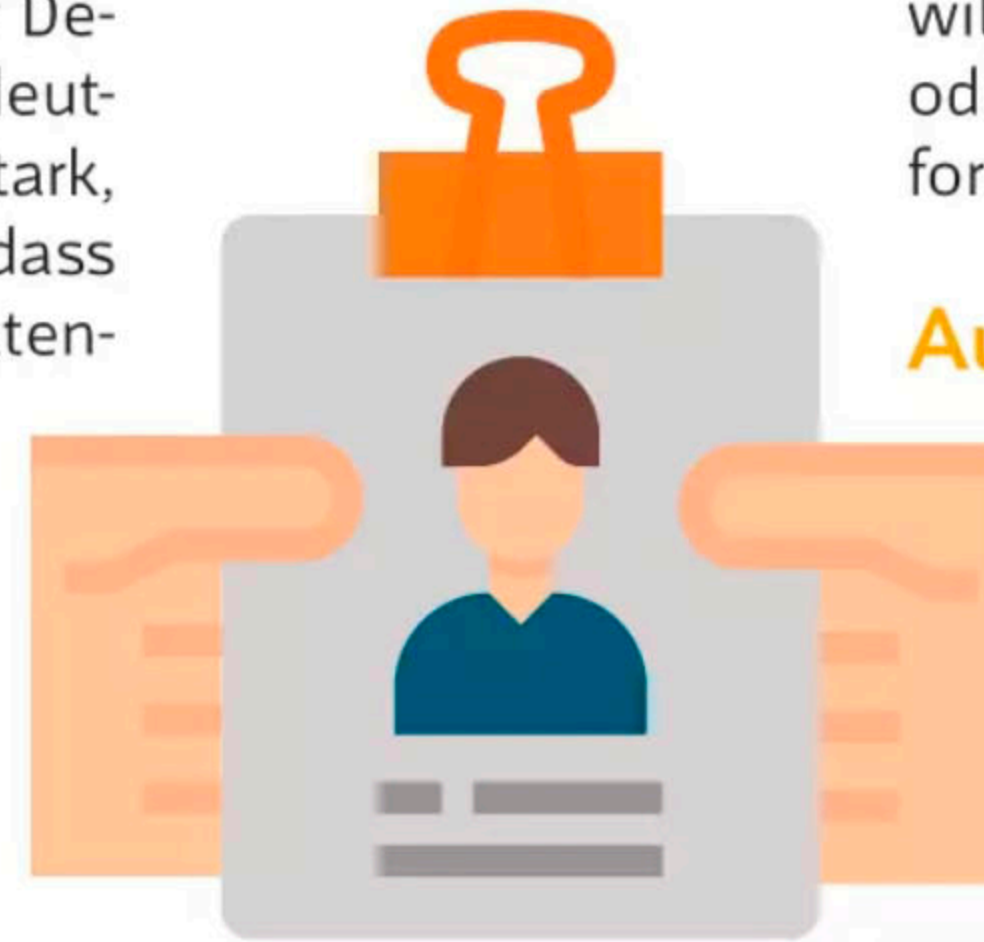
Berechtigte Interessen

Möglich wäre allerdings, dass die Datenweitergabe auf den Erlaubnistatbestand des berechtigten Interesses nach Art. 6 Abs. 1 S. 1 Buchst. f) DSGVO gestützt werden kann. Hier hilft der 48. Erwägungsgrund der Verordnung. Dieser besagt, dass Unternehmen, welche einer Unternehmensgruppe beziehungsweise einem Konzern angehören, ein berechtigtes Interesse an der Übertragung von personenbezogenen Daten an verbundene Unternehmen für konzerninterne Verwaltungszwecke haben können. Juristen sprechen in diesem Zusammenhang vom kleinen Konzernprivileg.

Dies bedeutet jedoch nicht, dass die konzerninterne Weitergabe von personenbezogenen Daten stets erlaubt ist. In der Regel jedoch überwiegen die Interessen des Konzerns, wenn die Datenweitergabe internen Verwaltungszwecken dient. Letzten Endes sollte aber stets für jeden Einzelfall geprüft werden, ob nicht doch die Interessen der Betroffenen überwiegen.

Auf berechtigte Interessen kann man sich jedoch nicht stützen,

wenn es um die Weitergabe besonders sensibler Daten im Sinne des Art. 9 DSGVO, beispielsweise Gesundheitsdaten, geht. Hier ist zwingend eine Einwilligung des jeweiligen Betroffenen oder eine andere Rechtsgrundlage erforderlich.



Auftragsverarbeitung und Auslandsbezug

Eine weitere Möglichkeit der rechtskonformen Datenweitergabe innerhalb eines Konzerns ist die Auftragsverarbeitung. Konzerne können sich beispielsweise dieses Instruments bedienen,

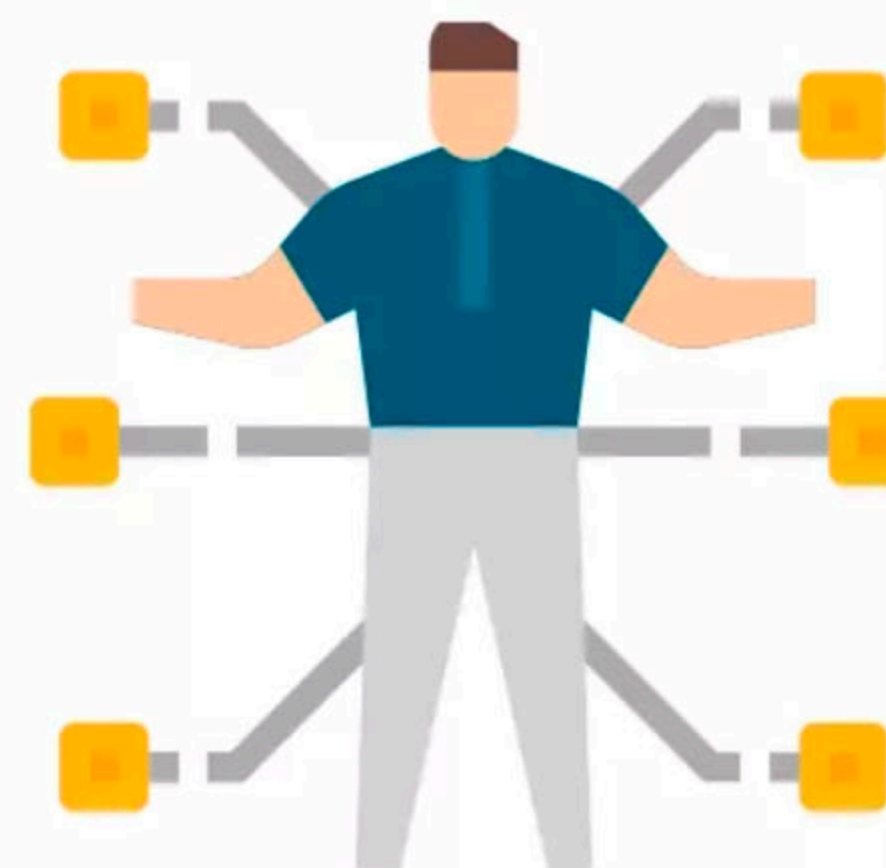
wenn zumindest unsicher ist, ob die Weitergabe (noch) auf berechtigte Interessen gestützt werden kann. Diese Vorgehensweise kann jedoch je nach Größe und Struktur des Konzerns zu einem sehr hohen Aufwand führen. Denn Voraussetzung ist, dass zwischen den verbundenen Unternehmen Vereinbarungen zur Auftragsdatenvereinbarung (AVV) geschlossen werden. In diesen Verträgen müssen die Arten und Zwecke der Datenweitergabe und -verwendung genau geregelt werden.

Weitere Voraussetzungen müssen – unabhängig von der Frage der Rechtsgrundlage – beachtet werden, wenn sich das verbundene Unternehmen in einem Drittstaat befindet. In diesem Fall sind die Anforderungen des fünften Kapitels der DSGVO zu beachten. Genaueres hierüber erfahren Sie ab Seite 108.

Fazit

Während die Weitergabe von personenbezogenen Daten innerhalb desselben Unternehmens weitestgehend unproblematisch ist, ist bei der konzerninternen Datenweitergabe an verbundene Unternehmen

stets eine Rechtsgrundlage erforderlich. Da die Instrumente der Einwilligung und der Auftragsverarbeitung oftmals aufwändig und teils unpraktikabel sind, sollte zunächst immer geprüft werden, ob die Datenübertragung auf berechtigte Interessen gestützt werden kann. Bei der Weitergabe von Daten zu Verwaltungszwecken wird dies aufgrund des kleinen Konzernprivilegs in der Regel der Fall sein. (keh) **ct**



Auftragsverarbeitung



Die Zusammenarbeit mit externen Dienstleistern bei der Verarbeitung personenbezogener Daten ist für Unternehmen äußerst relevant. Bei der Auftragsverarbeitung macht die DSGVO klare Vorgaben.

Von Nicolas Maekeler

Viele Geschäftsprozesse erfordern die Weitergabe personenbezogener Daten an Dritte. Wenn etwa eine Agentur mit der Versendung eines E-Mail-Newsletters an die eigenen Kunden beauftragt wird, man sich ausgedienter Festplatten entledigen möchte und sie für die Datenträgervernichtung an einen spezialisierten Dienstleister übergibt oder wenn die Lohn- und Gehaltsabrechnung outgesourct werden soll. Doch die Weitergabe personenbezogener Daten ist natürlich auch in diesen Fällen nicht ohne Weiteres zulässig.

Herr der Daten

Aufgrund des Verbots mit Erlaubnisvorbehalt muss entweder eine Einwilligung des Betroffenen oder eine gesetzliche Erlaubnis vorliegen. Um für die Verarbeitung von Daten durch beauftragte Dienstleister nicht die Einwilligung der Betroffenen einholen zu müssen, haben sich bereits unter dem alten Bundesdatenschutzgesetz (BDSG-alt) Regelungen zur Auftragsdatenverarbeitung etabliert. Sie zeichneten sich dadurch aus, dass die Person oder Stelle, die personenbezogene Daten im Auftrag verarbeitete, nicht mehr als „Dritter“ angesehen wurde. Denn ein Dienstleister unterliegt den Weisungen des Auftraggebers, der als „Herr der Daten“ die alleinige Verfügungsgewalt über die Daten behält.

Der Auftragnehmer agiert dadurch lediglich als verlängerter Arm des Auftraggebers. Nach außen bilden Auftraggeber und Auftragnehmer eine recht-

liche Einheit. Aus Sicht des für die Verarbeitung Verantwortlichen bedarf es daher keines gesonderten Erlaubnistatbestandes für die Weitergabe personenbezogener Daten an seinen Dienstleister.

Andere Begriffe

An diesem Prinzip hat der europäische Gesetzgeber festgehalten, allerdings gibt es signifikante Änderungen gegenüber den Regelungen des BDSG-alt. Zunächst hat man sich an neue Begrifflichkeiten gewöhnen müssen. Anstelle von *Auftraggeber* und *Auftragnehmer* werden die Beteiligten in Art. 28 DSGVO als *Verantwortlicher* und *Auftragsverarbeiter* bezeichnet. Die *Auftragsdatenverarbeitung* wird demgemäß nur noch schlicht Auftragsverarbeitung genannt.

Datenschutz-Zertifikate

Bereits bei der Auswahl geeigneter Auftragsverarbeiter muss der Verantwortliche darauf achten, dass sein neuer Geschäftspartner hinreichende Garantien bietet, dass die Vorschriften der DSGVO eingehalten werden. Zum Nachweis der Erfüllung von Datenschutz-Standards setzt die Verordnung dabei verstärkt auf Zertifikate. Diese haben das Potenzial, bei Auftragsverarbeitungen Klarheit zu schaffen, ob die datenschutzrechtlichen Anforderungen erfüllt werden. Auch die Auftragsverarbeiter profitieren, da deren Kunden sich anhand von Zertifikaten und Gütesiegeln leicht ein Bild von einem bestimmten

Produkt oder einer Dienstleistung bezüglich der Einhaltung der DSGVO machen können.

Firmen außerhalb des EU- beziehungsweise EWR-Auslands kommen als Auftragsverarbeiter ebenfalls in Betracht. Anders als das BDSG-alt sieht die DSGVO nämlich keine räumliche Beschränkung der Auftragsverarbeitung mehr vor. Voraussetzung ist jedoch, dass die Vorgaben zum internationalen Datentransfer eingehalten werden. So muss etwa im Empfangsstaat ein angemessenes Datenschutzniveau gewährleistet sein (siehe Seite 108).

In dem Vertrag zur Auftragsverarbeitung (kurz „AV-Vertrag“) müssen der Gegenstand und die Dauer sowie die Art und der Zweck der Datenverarbeitung festgelegt werden. Auch die Art der Daten, beispielsweise Personenstammdaten, Kommunikationsdaten oder Zahlungsdaten sowie die Kategorien der betroffenen Personen, wie etwa Kunden, Interessenten oder Beschäftigte, müssen bestimmt werden.

Die weiteren inhaltlichen Mindestanforderungen des Vertrags zur Auftragsverarbeitung ergeben sich

aus Art. 28 Abs. 3 DSGVO und können der Checkliste für AV-Verträge (siehe unten) entnommen werden.

Unterauftragsverhältnisse

Äußerst praxisrelevant sind die Bedingungen, wie mit Subunternehmern des Auftragsverarbeiters umzugehen ist. Denn auch die etwaige Berechtigung zur Begründung sogenannter Unterauftragsverhältnisse muss im AV-Vertrag festgelegt werden. Der Verantwortliche hat dabei die Möglichkeit im konkreten Fall seine schriftliche Genehmigung zu erteilen oder er erlaubt die Hinzuziehung von Subunternehmern generell.

Im letzteren Fall hat der Auftragsverarbeiter jedoch Informationspflichten gegenüber dem Verantwortlichen zu erfüllen. Er muss ihn über jede beabsichtigte Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter in Kenntnis setzen, damit dieser die Möglichkeit hat, notfalls der Änderung zu widersprechen. Als dritte Möglichkeit kann der Verantwortliche auch die Beauftragung weiterer Auftragsverarbeiter untersagen.

Inhalt eines AV-Vertrags

- ✓ Pflichten und Rechte des Verantwortlichen
- ✓ Pflichten des Auftragsverarbeiters
- ✓ Umfang von Weisungsbefugnissen
- ✓ Regelung von Unterauftragsverhältnissen
- ✓ Meldepflichten bei Datenschutzverstößen
- ✓ Rückgabe/Löschung von Daten bei Vertragsbeendigung

- Gegenstand und Dauer des Auftrags ✓
- Art und Zweck der Verarbeitung ✓
- Art der Daten ✓
- Kategorien betroffener Personen ✓
- Technische und organisatorische Maßnahmen ✓
- Gewährleistung der Betroffenenrechte ✓

Dem Unterauftragnehmer müssen dieselben Datenschutzpflichten auferlegt werden, die der Auftragsverarbeiter mit dem Verantwortlichen festgelegt hat. Im Falle einer Pflichtverletzung haftet der erste Auftragsverarbeiter für seine Unterbeauftragten.

Dokumentation in Hülle und Fülle

Auch der Auftragsverarbeiter muss, wie der Verantwortliche auch, ein Verzeichnis der Verarbeitungstätigkeiten führen (siehe Seite 50). Neben den Kontaktdaten aller Auftraggeber muss dieses Dokument Informationen zu den Kategorien der Verarbeitungen, möglichen Datenübermittlungen und den zum Schutz der Daten getroffenen technischen und organisatorischen Maßnahmen enthalten. Dieses Verzeichnis muss man nicht veröffentlichen, wohl aber der Aufsichtsbehörde bei Kontrollen zur Verfügung stellen.

Verschärfte Haftung

Der Auftragsverarbeiter haftet, wenn er seinen speziell durch die DSGVO auferlegten Pflichten nicht nachkommt oder die Anweisungen des Verantwortlichen nicht beachtet beziehungsweise gegen diese handelt. Klagen wegen Datenschutzverstößen können auch direkt gegen den Auftragsverarbeiter gerichtet werden. Zwar wird davon ausgegangen, dass in erster Linie der Auftraggeber haftet. Art. 83 DSGVO sieht jedoch vor, dass alle an der Verarbeitung personenbezogener Daten Beteiligten zunächst als Gesamtschuldner haften. Das heißt, dass sich ein potenzieller Kläger aussuchen kann, ob er den Verantwortlichen oder den Auftragsverarbeiter verklagt. Der Beklagte kann dann zwar den jeweils anderen Teil in Regress nehmen, muss aber zunächst gegenüber dem Geschädigten vollumfänglich Schadensersatz leisten.



Formzwang?

? Ist für eine Vereinbarung zur Auftragsverarbeitung die Schriftform erforderlich?

! Verträge, welche die Grundlage zur Auftragsverarbeitung bilden, müssen nicht zwingend in Schriftform abgeschlossen werden. Die eigenhändige Unterschrift der Vertragspartner ist somit nicht nötig. Die DSGVO lässt auch ein elektroni-

sches Format zu. Bei einem Onlinevertragsabschluss kann man die dazugehörige Vereinbarung zur Auftragsverarbeitung also ohne Weiteres digital bereitstellen. Entscheidend ist dabei, dass man den Vertragsschluss in einem Format dokumentiert, das nachträgliche Änderungen unmöglich macht.

Bußgeld

? Drohen bei Verstößen im Rahmen der Auftragsverarbeitung ebenfalls hohe Bußgelder?

! Die häufig erwähnten drakonischen Bußgelder, welche die DSGVO bei Datenschutzverstößen vorsieht, finden auch bei der Auftragsverarbeitung Anwendung. Allerdings liegen die maximal möglichen Bußgelder unterhalb der bekannten 20 Millionen Euro. Verstößt etwa der Auftragsverarbeiter gegen seine spezifischen Pflichten, können Datenschutzbehörden „nur“ aus einem Bußgeldrahmen von bis zu 10 Millionen Euro oder 2 Prozent des weltweit erzielten Jahresumsatzes eines Unternehmens schöpfen. Für bestimmte Verstöße und wenn

Anweisungen der Aufsichtsbehörden nicht befolgt werden, verdoppeln sich die Maximalbeträge jedoch wieder.

Altlasten

? Ich habe vor Jahren mit einem Dienstleister einen Vertrag zur Auftragsdatenverarbeitung geschlossen. Ist der Vertrag noch gültig?

! Soweit dies noch nicht geschehen ist, sollten bestehende Alt-Verträge zur Auftrags(daten)-verarbeitung überprüft werden. Da sich „nur“ die Rechtslage geändert hat, sind Alt-Verträge zwar nicht unwirksam geworden – entsprechende Verweise auf nicht mehr gültige Rechtsvorschriften können grundsätzlich im Zuge der Auslegung umgedeutet werden. Dennoch wird in aller Regel eine Neufassung oder zumindest eine Ergänzung notwendig sein, um die neuen Anforderungen der DSGVO abzubilden. Einen Mustervertrag finden Sie über [ct.de/wj8j](https://www.ct.de/wj8j).

Beispiele

? Wann handelt es sich bei der beauftragten Dienstleistung um eine Auftragsverarbeitung?

! Keine Auftragsverarbeitung liegt bei der Inanspruchnahme fremder Fachleistungen eines eigenständigen Verantwortlichen vor. Das ist etwa bei der Beauftragung von Rechtsanwälten, Steuerberatern oder Wirtschaftsprüfern der Fall. Wenn mehrere Verantwortliche gemeinsam über die Verarbeitungszwecke und -mittel entscheiden, handelt es sich auch nicht um eine Verarbeitung im Auftrag, sondern um eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO.

Zu Abgrenzungsfragen hat das Bayerische Landesamt für Datenschutz eine umfangreiche Liste von konkreten Beispielen veröffentlicht (siehe [ct.de/wj8j](https://www.ct.de/wj8j)). Die Behörde geht davon aus, dass eine Auftragsverarbeitung nur dann vorliegt, wenn ein Dienstleister im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird. Darunter fallen etwa die Finanzbuchhaltung durch Rechenzentren, Kundenbetreuung durch ein Callcenter oder Sicherheitsdienste, die Besucherdaten erheben.

Ein sehr praxisrelevanter Fall der Auftragsverarbeitung ist das Hosten von Daten durch Cloud-Dienstleister. Ab Seite 132 erläutern wir, welche rechtlichen Fallstricke beim Cloud-Computing zu beachten sind.

(anm) **ct**

Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO
[Stand: Mai 2017]

Vereinbarung

zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -
und dem/der

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

Hinweis

„Die einzelnen Festlegungen nach Art. 28 Abs. 3 DS-GVO sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.“

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der
Leistungsvereinbarung/SLA/..... vom, auf die hier
verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: (Definition der Aufgaben)

(2) Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) stellt einen Mustervertrag zur Auftragsverarbeitung zur Verfügung (siehe [ct.de/wi8i](https://www.ct.de/wi8i))

Praxishilfen und Mustervertrag zur Auftragsverarbeitung:

ct.de/wj8j



Sanktionen & Schadensersatz

Exorbitante Bußgelder und teure Abmahnungen sind aufgrund der DSGVO ebenso möglich wie Schadensersatzklagen. Nachdem sich die Behörden in der Anfangszeit auf das Beraten beschränkten, geht es nun langsam los mit teuren Bußgeldbescheiden, auch in Deutschland.

Von Nicolas Maekeler und Brian Scheuch

Konsequenzen

? Was droht mir bei DSGVO-Verstößen?

! 20 Millionen Euro oder vier Prozent des weltweit erzielten Jahresumsatzes eines Konzerns – mit diesen Zahlen hat die DSGVO wohl die meisten Schlagzeilen gemacht. Es handelt sich um das maximale Bußgeld, das bei Datenschutzverstößen verhängt werden kann. Es erscheint eher unwahrscheinlich, dass die Maximalsumme jemals verhängt wird, ausschließen kann man dies jedoch nicht. Daneben drohen Abmahnungen von Mitbewerbern und Verbraucherverbänden (siehe Seite 70) sowie Schadensersatzforderungen von Betroffenen (siehe Seite 72). Datenschlamperei kann nun richtig teuer werden.

Kurz vor dem Startschuss der DSGVO gab es kaum einen Medienbericht, der nicht ausdrücklich auf die horrenden Bußgelder hinwies, die das neue europäische Datenschutzrecht mit sich bringen würde. Selbst die größten Datenschutzmuffel in den Cheftagen der Republik wurden so mindestens wacherüttelt oder gar in Panik versetzt. Für viele dürfte die Angst vor den mutmaßlich ruinösen Sanktionen der Aufsichtsbehörden die Hauptmotivation für die Umsetzung der neuen rechtlichen Anforderungen gewesen sein.

Eine fehlende oder unzureichende Datenschutzerklärung auf der Website dürfte jedoch kaum zu einem solch exorbitant hohen Bußgeld führen. Da müsste man schon Datenschutzverstöße katastro-

phalen Ausmaßes begehen, beispielsweise in der Innenstadt USB-Sticks mit umfangreichen sensiblen personenbezogenen Daten Dritter verteilen.

Es muss nicht einmal immer gleich ein Bußgeld sein. Die Datenschutzbehörden können auch andere Maßnahmen treffen, wie eine Verwarnung, eine Rüge oder die Aussetzung der Datenverarbeitung.

Bemessungsgrundsätze

? Wovon hängt die Höhe des Bußgeldes ab?

! Grundsätzlich können Bußgelder in Deutschland nicht „einfach so“ verhängt werden, wie es fälschlicherweise gerne behauptet wird. Hinter der Verhängung von Bußgeldern steckt ein formelles Verfahren. Gemäß § 41 BDSG finden für Verstöße gegen die DSGVO in der Regel ergänzend die Vorschriften des Gesetzes über die Ordnungswidrigkeiten sinngemäß Anwendung.

Dies bedeutet, dass das Verfahren formell wie bei einem klassischen Geschwindigkeitsverstoß abläuft. Das Unternehmen wird daher im ersten Schritt erst einmal angehört. In dem Anhörungsschreiben werden sodann die Tatsachen aufgezeigt, die nach Ansicht der Aufsichtsbehörde rechtswidrig gewesen sind. Zu den Behauptungen kann man entweder Stellung nehmen oder schweigen. Gerade in der Stellungnahme sollte man darauf achten, dass man sich nicht um Kopf und Kragen redet oder schreibt, und im Zweifelsfall IT-Spezialisten und Juristen hinzuziehen.

Nach erfolgter Anhörung entscheidet die Behörde nach billigem Ermessen, ob sie überhaupt ein Bußgeld, eine Rüge oder eine Verwarnung verhängt. Folgende Faktoren können sich positiv auf die Höhe eines Bußgeldes auswirken:

- Der Datenschutzverstoß wird nicht vorsätzlich, also mit Wissen und Wollen, sondern nur fahrlässig begangen.
- Es werden Maßnahmen zur Minderung des entstandenen Schadens getroffen.
- Der Grad der Verantwortung ist unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen gering.
- Es liegen keine einschlägigen früheren Verstöße des Verantwortlichen vor.
- Es wird umfangreich mit den Datenschutzbehörden zusammengearbeitet, um Abhilfe zu leisten und nachteilige Auswirkungen zu mindern.
- Es sind keine besonders sensiblen Daten betroffen.
- Der Verstoß wird durch eine Selbstanzeige innerhalb von 72 Stunden bei den Datenschutzbehörden gemeldet.
- Andere erschwerende oder mildernde Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

Unabsichtliche Verstöße, insbesondere solche, die dem Unternehmen keinen finanziellen Vorteil bringen, sollten sich daher positiv auf die Höhe des Bußgeldes auswirken. Deutlich höhere Bußgelder werden dagegen verhängt, wenn das Unternehmen mit personenbezogenen Daten Geld verdient. Das wäre beispielsweise bei diversen Newsletter-

Anbietern sowie „Lead-Generation-Agenturen“ der Fall. Eine Übersicht über tatsächlich verhängte Bußgelder finden Sie ab Seite 62.

Auslöser für Verfahren

? Wie werden die Aufsichtsbehörden auf Verstöße aufmerksam?

! Damit überhaupt ein Bußgeldverfahren eingeleitet wird, muss die Behörde erst einmal Kenntnis von DSGVO-Verstößen erlangen. Dies kann auf unterschiedliche Weise geschehen. Die jeweils betroffene Person kann ihr Beschwerderecht aus Art. 77 DSGVO wahrnehmen und sich direkt bei der zuständigen Aufsichtsbehörde beschweren. Aber auch Konkurrenten können anonym Verstöße melden. Denkbar ist aber auch, dass die eigene Website bereits von außen so viele DSGVO-Verstöße aufzeigt (zum Beispiel fehlende Datenschutzerklärung), dass die Behörde von sich aus weitere Nachforschungen anstellt.

Einige Aufsichtsbehörden haben bereits stichprobenartig verschiedene Unternehmen angeschrieben und aufgefordert, die entsprechenden Dokumentationen wie das Verarbeitungsverzeichnis vorzulegen. Neben der Außendarstellung (siehe Seite 46) sollte man unbedingt auch die internen Prozesse zügig angehen, damit man auf Nachfrage die gesetzlich vorgeschriebenen Dokumentationen fristgerecht vorlegen kann (siehe Seite 42 und 50).

Zuletzt können auch Meldungen über Datenschutzverstöße oder Datenpannen entweder durch Dritte oder durch die datenverarbeitenden Unternehmen selbst die Aufsichtsbehörden aktivieren und sie zum Handeln zwingen. (anm) **ct**



**Aufsichtsbefugnisse/
Sanktionen:**

[ct.de/wkmx](https://www.ct.de/wkmx)

Eskalationsstufen bei Verstößen gegen die DSGVO



Verwarnung



Rüge



Aussetzung der Datenverarbeitung



Bußgeld

von bis zu
20 Mio. €

oder

4 % des weltweiten
Jahresumsatzes

Bußgelder – eine Übersicht



Die Datenschutzbehörden machen bei Bußgeldern inzwischen ernst. Strafzahlungen, auch in sieben- oder gar achtstelliger Höhe, für Datenschutzverstöße sind inzwischen keine Seltenheit mehr. Selbst Privatpersonen können Empfänger solch teurer Verwaltungsakte sein. Aktuelle Beispiele zeigen inzwischen, welche Verstöße wie viel kosten können.

Von Joerg Heidrich und Brian Scheuch

Die ersten Bußgelder wurden schon ein Jahr nach Inkrafttreten der DSGVO verhängt, aber erst das Jahr 2020 war quasi das Jahr der Bußgelder. Trotz der Pandemie waren die Aufsichtsbehörden nicht zögerlich.

Bereits im März 2020 wurde bekannt, dass gegen den Internetriesen 1&1 ein Bußgeld in Höhe von 9,55 Millionen Euro verhängt wurde. Der Bundesdatenschutzbeauftragte Ulrich Kelber verhängte dieses Bußgeld, weil der Internetkonzern keine ausreichende Authentifizierungshürde im Rahmen telefonischer Anfragen hatte. So war es möglich, gegen Nennung des Namens und des Geburtsdatums weitere Auskünfte am Telefon zu bekommen.

1&1 ging gegen dieses Bußgeld gerichtlich vor und zog vor das Landgericht Bochum. Das Landgericht Bochum stellte mit Urteil vom 11.11.2020 (Az.: 29 OWi 1/20 LG) fest, dass 1&1 einen Datenschutzverstoß begangen habe, da unzureichende technische und organisatorische Schutzmaßnahmen getroffen wurden. Jedoch reduzierte das Gericht das Bußgeld auf 900.000 Euro, knapp ein Zehntel des ursprünglichen Bußgeldes. Dieses Urteil zeigt, dass ein gerichtliches Vorgehen gegen Bußgeldbescheide nicht aussichtslos ist.

Rekordbußgeld gegen H&M

Selbst die ursprünglich verhängten knapp 10 Millionen Euro für 1&1 wären aber noch nicht der Spitzenreiter gewesen: Gegen die Modekette H&M verhäng-

ten die Behörden ein Rekordbußgeld in Höhe von 35,3 Millionen Euro, was zumindest in Deutschland das höchste verhängte Bußgeld sein dürfte. Seit 2014 soll das Unternehmen nach Angaben der Behörden private Details der Mitarbeiter ausgespäht haben. So wussten einige Vorgesetzte beispielsweise von familiären Problemen, religiösen Bekenntnissen oder Krankheitssymptomen. Nach Urlaubs- oder Krankheitsabwesenheit fanden Gespräche statt, bei denen entsprechende Urlaubsergebnisse oder Diagnosen festgehalten wurden. Die einzelnen in einer Liste gespeicherten Erkenntnisse waren teilweise für mehrere Führungskräfte zugänglich. Bekannt wurde dieses Fehlverhalten, nachdem im Rahmen eines technischen Fehlers die Liste standortübergreifend einsehbar war.

Das Unternehmen entschuldigte sich bei den betroffenen Mitarbeitern und kündigte an, diese entschädigen zu wollen. Nach bisherigen Informationen ist H&M auch nicht gegen das Bußgeld vorgegangen. Die Kommunikation des Konzerns ist ein Paradebeispiel, wie eine gute Informationspolitik im Rahmen eines Verstoßes aussehen kann.

Bußgeld wegen mangelnder IT-Sicherheit

Das erste bekannte Bußgeld in Deutschland wurde Ende 2018 in Baden-Württemberg gegen das Social-Media-Netzwerk [Knuddels.de](https://www.knuddels.de) in Höhe von 20.000 Euro verhängt. Der Betreiberin der Plattform wurde

vorgeworfen, personenbezogene Daten nicht ausreichend gesichert zu haben. Passwörter der Nutzer seien im Klartext, unverschlüsselt und ungehasht gespeichert worden. Im Juli 2018 wurde das Portal Opfer eines Hackingangriffs, woraufhin unter anderem hunderttausende Passwörter und E-Mail-Adressen im Internet veröffentlicht wurden.

Das Bußgeld fiel verhältnismäßig gering aus. Grund dafür waren unter anderem die gute Kooperation mit der Aufsichtsbehörde sowie eine entsprechende Meldung. Dieses Bußgeld zeigt, dass sich eine Zusammenarbeit extrem auf das zu verhängende Bußgeld auswirken kann.

Bußgeld wegen unzulässiger Schwarzer Liste

Ein weiteres Bußgeld in Höhe von 50.000 Euro wurde gegen eine Internetbank von der Berliner Datenschutzbehörde verhängt. Die Bank habe unbefugt personenbezogene Daten von ehemaligen Kunden verarbeitet. Frühere Nutzer seien auf einer „Schwarzen Liste“ gespeichert worden, welches lediglich bei Kunden legitim wäre, die unter dem Verdacht stehen, gegen das Geldwäschegesetz zu verstoßen.

Bußgeld für die Nichtbeachtung von Betroffenenrechten

Ein Bußgeld in Höhe von 195.407 Euro wurde ebenfalls von den Berliner Datenschutzbehörden verhängt. Hierbei handelte es sich um mehrere Einzelverstöße des Unternehmens, wie die Nichtbeachtung der Betroffenenrechte. Dem Recht auf Auskunft, Löschung sowie dem Widerspruchsrecht der betroffenen Personen sei nicht vollumfänglich nachgekommen worden. Das Unternehmen habe demnach Konten ehemaliger Kunden nicht gelöscht, die die Plattform teilweise jahrelang nicht nutzten. Ebenfalls haben einige Kunden unerwünschte Werbemails erhalten und in einem Fall wurde der Widerspruch nicht beachtet. Auch Auskünfte seien teils nicht oder nur unzureichend erteilt worden. Aufgrund mehrerer Beschwerden einzelner Personen wurde die Behörde tätig. Dieser Fall ist ebenfalls ein gutes Beispiel dafür, dass Beschwerden betroffener Personen keineswegs von den Behörden ignoriert werden.

Im Jahr 2019 wurde ein hohes Bußgeld gegen die Deutsche Wohnen in Höhe von 14,5 Millionen Euro verhängt. Berichten zufolge soll die Wohnungsgesellschaft gegen die Datenminimierungspflicht

verstoßen haben. Prüfungen aus den Jahren 2017 und 2019 hätten ergeben, dass personenbezogene Daten von Mietern in ein Archivsystem gespeichert wurden, das keine Möglichkeit zur Löschung vorsah. Die Daten seien gespeichert worden, ohne genau zu prüfen, ob die Verarbeitung zulässig ist. Bereits 2017 habe es eine Empfehlung der Behörde gegeben, das Archivsystem umzustellen. Die Deutsche Wohnen hat gegen das Bußgeld Einspruch eingelegt.

Weitere Bußgelder

Ein Bußgeld in Höhe von 80.000 Euro wurde gegen ein Krankenhaus verhängt, bei dem Gesundheitsdaten versehentlich im Internet landeten. Das Krankenhaus ist bislang namentlich nicht bekannt.

Wegen der verspäteten Meldung einer Datenpanne wurde einem anderen Unternehmen ein Bußgeld von 20.000 Euro auferlegt.



Anfangs war die Panik vor exorbitanten Bußgeldern nicht nötig. Dass sich das mittlerweile geändert haben dürfte, zeigen viele Beispiele.

2018 hatten die deutschen Aufsichtsbehörden noch keine Bußgelder im Millionenbereich angesetzt. Dies hat sich nunmehr geändert und es wurde auch in Deutschland mehrfach die Millionenmarke geknackt. Dass weitere Bußgelder folgen, dürfte außer Frage stehen. Ebenso dürfte überaus wahrscheinlich

sein, dass das Bußgeld gegen H&M wohl nicht das Höchste bleiben wird. Es bleibt aber abzuwarten, ob die Millionenbußgelder auch nach einem gerichtlichen Verfahren noch Bestand haben werden. Die Tabelle auf Seite 66 und 67 gibt einen Überblick, welche Verstöße in Deutschland bisher Buß-

Modell zur Bußgeldberechnung

Die Verhängung von Datenschutzbußgeldern obliegt den Landesbeauftragten für den Datenschutz der jeweiligen Bundesländer. Im Rahmen der Bußgeldpraxis gab es hierzu zunächst unterschiedliche Höhen.

Aufgrund der unterschiedlichen Bußgeldpraxis haben sich die Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) am 25.06.2019 auf ein einheitliches Modell zur Bußgeldberechnung verständigt, um so Abweichungen der einzelnen Bundesländer entgegenzuwirken. Dieses Modell ist überaus komplex, da andernfalls der Einzelfallabwägung nicht im notwendigen Maße Rechnung getragen werden kann. Nachfolgend soll das neue Bußgeldmodell ein wenig genauer betrachtet werden, um bei einem möglichen Datenschutzverstoß die Höhe des Bußgeldes schätzen zu können.

Das Bußgeldmodell im Detail

Ausgangspunkt für die Berechnung des Bußgeldes ist der erzielte Jahresumsatz eines Unternehmens. Offen bleibt hier, ob auch konzernverbundene Unternehmen mit einbezogen werden. Anhand des Jahresumsatzes wird sodann ein Tagessatz ermittelt, der als Grundlage zur Berechnung des Bußgeldes dient.

Ermittlung von Tagessätzen

Um die Interessen kleinerer Unternehmen zu wahren, wird bei unter 500 Millionen Euro Jahresumsatz nicht durch 360 geteilt. Der Tagessatz wird hier anhand von Größenklassen, die andere, in der Regel niedrigere Summen vorgeben, errechnet.

Der ermittelte Tagessatz wird mit einem Faktor zwischen 1 (bei leichten Verstößen) und 14,4 (bei sehr schweren Verstößen) multipliziert. Für leichte Verstöße wird daher der Jahresumsatz / 360 x 1 multipliziert und bei äußerst schweren Verstößen entsprechend mit 14,4. Ob der Höchstfaktor von 14,4 jemals zum Einsatz kommt, bleibt fraglich.

Im Rahmen der Bußgeldbemessung können noch weitere Faktoren bußgelderhöhend berücksichtigt werden, wie Art des Verstoßes, entstandener Schaden, Dauer sowie vorsätzliches oder fahrlässiges Verhalten.

Hohe und abschreckende Bußgelder

Sollten Bußgelder nach diesem Modell verhängt werden, so wird es definitiv zu hohen und abschreckenden Beträgen kommen, wie das nachfolgende Rechenbeispiel verdeutlicht:

Selbst bei einem leichten Datenschutzverstoß wird nach dem obigen Rechenbeispiel bereits ein überaus hohes Bußgeld fällig, welches alle Grenzen der derzeit bekannten Bußgelder übersteigt. Diese Summe ist allerdings noch sehr weit von der Höchstgrenze von 4 % des erzielten Jahresumsatzes entfernt.

Kritik am Modell

Aus dem Modell sind bislang wenige Faktoren bekannt, die das Bußgeld unter Umständen abmildern können, wie unverzügliche Information der betroffenen Personen und Kooperation mit den Aufsichtsbehörden.

Die Berechnung nach reinem Umsatz ist ebenfalls ein wenig starr und könnte gerade Branchen mit niedrigen Gewinnspannen vor existenzbedrohliche Probleme stellen. Es ist überaus wahrscheinlich, dass viele Sanktionen nach diesem Modell vermehrt vor Gericht landen werden.

Rechenbeispiel	
Jahresumsatz eines Unternehmens:	1 Milliarde Euro
Tagessatz:	$1.000.000.000 / 360 = 2.777.778$ Euro
Multiplikation mit Faktor:	$2.777.778 \text{ Euro} \times (1 \text{ bis } 14,4)$
Ergebnis:	Mind. 2.777.778 Euro

Die Konferenz für Frontend-Entwicklung am 9. Februar 2021 >>> ONLINE <<<

Wer seine Webseiten nicht schnell genug ausliefert, riskiert, dass die Besucher wegklicken. Und Google rankt langsam ladende Seiten auch nicht optimal, denn Performance ist für die Suchmaschine ein wichtiges Kriterium. Websites sind heute aber komplexe Gebilde:

Besucher erwarten bunte, interaktive Seiten, in denen allerlei JavaScript-Bibliotheken, Stylesheets, Bilder u.v.m. zum Einsatz kommen. Die **c't <webdev>** beleuchtet am 9. Februar 2021 in sechs Talks, wo es bei der Web-Performance haken kann, wie man Bremsen aufspürt und seine Seiten flotter macht.

Programm-Highlights

- > „Core Web Vitals – What, Why and How?“ // Martin Splitt
- > „Pufferspeicher und andere Geschwindigkeits-Optimierungen“
// Benjamin Kluck + Peter Mösenthin
- > „Responsive Images for the Web“ // Sia Karamalegos
- > „JavaScript und Browser-Engines unter der Haube“
// Peter Kröner
- > „Performance-Experimente mit Chrome Devtools und
CloudFlare Workers“ // Christian Schäfer

Preis: 279 Euro inkl. MwSt.

Jetzt
Tickets
sichern

Weitere Informationen und Tickets unter: www.ctwebdev.de

```
18 if $(  
19 $(  
20  
21 $( '.input  
22 if $(t  
23 $(t  
24 return  
25  
26 $.fn.na  
27 place  
28 onShow  
29 plac  
30  
31 #default m  
32 window.def  
33 $modal =  
34 $modal.f  
35 $modal.f  
36 $modal.a  
37 closeO  
38 if redir  
39 $( '.de  
40 loca
```

Line 37 Column

Datum	Verstoßender	Verstoß	Bußgeld
01.10.2020	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Bei der schwedischen Modekette H&M hatten Führungspersonen des Servicecenters in Nürnberg seit 2014 ausführliche Aufzeichnungen über private und intime Angelegenheiten hunderter Mitarbeiter erstellt. Diese Aufzeichnungen beeinflussten Entscheidungen über die weiteren beruflichen Laufbahnen der betroffenen Mitarbeiter in dem Unternehmen. Durch einen Fehler in der Netzwerkkonfiguration konnte zeitweise über das gesamte Unternehmensnetzwerk auf die circa 60 Gigabyte große Datensammlung zugegriffen werden.	Der Hamburger Datenschutzbeauftragte erließ einen Bescheid in Höhe von fast 35,3 Millionen Euro. Der Bescheid ist mittlerweile rechtskräftig.
30.09.2020	Rechtsanwalt	Aufgrund einer Verwechslung glaubte ein Rechtsanwalt einen Handwerker, gegen den offene Forderungen bestanden, auf dem Grundstück eines Ehepaars arbeiten gesehen zu haben. Daraufhin erwirkte der Rechtsanwalt die Pfändung der Forderung des Handwerkers gegen das Ehepaar. Allerdings stellte sich heraus, dass der gesichtete Handwerker nicht derjenige war, gegen den der Rechtsanwalt eine ausstehende Forderung hatte.	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz erlegte ein Bußgeld über 8000 Euro auf.
30.06.2020	AOK Baden-Württemberg	Die Versicherung hatte zwischen 2015 und 2019 Gewinnspiele veranstaltet, bei denen die Teilnehmer der Nutzung ihrer Daten – unter anderem die Krankenkassenzugehörigkeit – zu Werbezwecken zustimmen konnten, wenn sie dies wollten. Von über 500 Teilnehmern jedoch wurden Daten zu Werbezwecken verwendet, obwohl gerade keine entsprechende Zustimmung abgegeben wurde.	Es wurde ein Bußgeld in Höhe von circa 1,24 Millionen Euro gezahlt.
09.03.2020	LKW-Fahrer	Ein LKW-Fahrer machte dauerhaft und ohne konkreten Anlass Aufnahmen mit einer Dashcam aus seinem LKW heraus. Diese Aufnahmen veröffentlichte er auf Youtube. Zu sehen waren dort teilweise Nummernschilder anderer Fahrzeuge.	Das Bußgeld betrug 200 Euro.
Februar 2020	Berliner Landesverband der NPD	Im Februar 2018 veröffentlichte der Berliner Landesverband der NPD einen Ausschnitt aus Google Maps, in dem einige Standorte von Flüchtlingsunterkünften verzeichnet waren. Zusätzlich wurden jeder Einrichtung Namen und Kontaktdaten der dort beschäftigten Personen beigefügt. Auch wenn sämtliche Daten auch in anderen öffentlichen Quellen verfügbar waren, hatten die betroffenen Personen keine Einwilligung bezüglich der Verarbeitung ihrer Daten abgegeben.	Dem Landesverband wurde ein Bußgeld in Höhe von 6000 Euro auferlegt. Dagegen wurde Einspruch eingelegt – die gerichtliche Entscheidung steht noch aus.
2020	Schwimmbadbetreiber	Ein Betreiber eines Schwimmbades beauftragte einen Dienstleister zur Wartung der Kameraüberwachungsanlage des Schwimmbades. Weder konnte der Betreiber eine Einwilligung der Gäste und Mitarbeiter in die Aufzeichnung durch die Kameras vorweisen, noch hatte er mit dem Dienstleister ein Auftragsverarbeitungsvertrag geschlossen. Denn der Dienstleister hatte ebenfalls Zugriff auf die Aufzeichnungen der Anlage. Außerdem hatte der Betreiber auch keinen Datenschutzbeauftragten gemeldet.	Die geforderte Zahlung betrug 12.000 Euro.
09.12.2019	Rapidata GmbH	Das kleine Unternehmen aus der Branche der Telekommunikation kam seiner in Art. 37 DSGVO gesetzten Pflicht zur Benennung und Meldung eines Datenschutzbeauftragten trotz mehrfacher Aufforderung nicht nach.	Das Bußgeld belief sich auf 10.000 Euro.
09.12.2019	1&1 Telecom GmbH	Bei dem deutschen Telekommunikationsunternehmen erlangte eine Person in einem Telefonat unter Angabe von Namen und Geburtsdatum eines Kunden weitere Informationen über diesen Kunden. Dabei offenbarte der Anrufer sogar, nicht der Kunde selbst zu sein, sondern lediglich auf dessen Geheiß zu handeln. Tatsächlich hatte der Kunde keine derartige Anweisung gegeben.	Der Bußgeldbescheid des Bundesdatenschutzbeauftragten erging in Höhe von 9,55 Millionen Euro. 1&1 ließ das Bußgeld gerichtlich überprüfen. Das Landgericht Bonn hat entschieden, dass das verhängte Bußgeld zwar dem Grunde nach berechtigt, allerdings unangemessen hoch ist (Urt. v. 11.11.2020 Az. 29 OWi 1/20 LG). Das Gericht hat den Betrag daher auf 900.000 Euro herabgesetzt.

Datum	Verstoßender	Verstoß	Bußgeld
30.10.2019	Deutsche Wohnen SE	Eines der größten deutschen Immobilien-Unternehmen speicherte jahrelang persönliche Daten von Mietern, wie zum Beispiel Selbstauskunftsformulare oder Gehaltsbescheinigungen. Dabei soll es keinerlei Prüfungen hinsichtlich der Zulässigkeit einer weiteren Speicherung dieser Daten und darüber hinaus auch keinerlei Möglichkeit zur Löschung gegeben haben. Bereits 2017 war das Unternehmen aufgefordert worden, die Verstöße zu beheben, war dem jedoch nicht nachgekommen.	Es erging ein Bußgeldbescheid in Höhe von 14,5 Millionen Euro. Die Deutsche Wohnen SE hat dagegen Einspruch eingelegt.
24.10.2019	Unternehmen	Im Rahmen eines Bewerbungsverfahrens eines Unternehmens wurden sämtliche Unterlagen von Bewerbern, darunter auch persönliche Daten, unverschlüsselt übertragen und gespeichert. Durch eine Anbindung an Google konnten diese Daten mittels einfacher Google-Suche öffentlich eingesehen werden.	Das Bußgeld betrug 100.000 Euro
09.05.2019	Polizist	Ein Polizist nutzte das Zentrale Verkehrsinformationssystem (ZEVIS) des Kraftfahrtbundesamtes, um an persönliche Daten einer Privatperson zu gelangen. Diese stand in keinem Zusammenhang mit seiner polizeilichen Tätigkeit. Der Beamte beabsichtigte damit einen privaten Kontakt mit besagter Person aufzubauen.	Es wurde ein Bußgeld in Höhe von 1400 Euro verhängt.
12.04.2019	Finanzunternehmen	Ein in Baden-Württemberg ansässiges mittelständisches Finanzunternehmen hatte auf Papier gedruckte Unterlagen im Papiermüll entsorgt. Die Dokumente konnten jedoch, weiterhin lesbar, aus dem Müll entfernt werden. Personenbezogene Daten von zwei Kunden des Unternehmens gelangten so in die Hände einer Nachbarin.	Der zuständige Beauftragte für Datenschutz und Informationsfreiheit erließ daraufhin einen Bußgeldbescheid in Höhe von 80.000 Euro.
März 2019	Facebook Germany GmbH	Die deutsche Niederlassung von Facebook meldete nach Beendigung der Tätigkeit des bisherigen unternehmensinternen Datenschutzbeauftragten im Jahr 2017 keinen neuen Datenschutzbeauftragten. Diesen Verstoß gegen Art. 37 Abs. 7 DSGVO erfuhr der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit durch eine Beschwerde.	Es erging ein Bescheid über 51.000 Euro.
2019	Unternehmen	Ein Unternehmen bediente sich zur Verarbeitung persönlicher Daten eines dritten Dienstleisters. Bei Auskünften nutzte dieser Dienstleister dabei sein eigenes Firmenlogo – auch anderweitig war den Kunden des Unternehmens nicht mitgeteilt worden, dass ein Dienstleister die Daten verarbeitete. Ein für solche Konstellationen notwendiger Auftragsverarbeitungsvertrag war nicht geschlossen worden. Überdies wurden die Auskünfte in englischer Sprache abgefasst, was gegen das Gebot der Verständlichkeit aus Art. 12 Abs. 1 DSGVO verstieß.	Der Landesbeauftragte für Datenschutz und Recht auf Akteneinsicht Brandenburg erließ einen Bußgeldbescheid in Höhe von 50.000 Euro.
2019	Restaurant	Ein Restaurant-Betreiber überwachte ohne Einwilligung der Gäste und Mitarbeiter den Gastraum seines Lokals mit einer Kamera. Damit verstieß er gegen den Grundsatz der Datenminimierung.	Es gab eine Geldbuße in Höhe von 2000 Euro.
2019	Hamburger Verkehrsverbund GmbH	Der Hamburger Verkehrsverbund kam im Jahr 2018 nach einer Datenpanne seinen Meldepflichten nach Art. 33, 34 DSGVO nicht hinreichend nach. Aufgrund eines fehlerhaften Updates konnten Kunden einer HVV-Card nach Einloggen auf der Internetseite des HVV durch die Änderung der URL auf die Daten anderer HVV-Card-Kunden zugreifen. Obwohl das Unternehmen auf diesen Zustand hingewiesen worden war, gab es erst nach fast einer Woche eine entsprechende Meldung an den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ab. Art. 33 Abs. 1 der DSGVO setzt jedoch eine maximale Frist von 72 Stunden.	Es wurde ein Bußgeld in Höhe von 20.000 Euro erlassen.

gelder ausgelöst haben und wie hoch die verhängten Summen bisher waren.

Bußgelder im europäischen Vergleich

Auch in den europäischen Nachbarländern gab es Bußgeldverfahren. Ein erstes Bußgeld in Österreich 2018 traf die Betreiberin eines Wettlokals. Dieses

hatte vor dem Eingangsbereich eine Kamera montiert, die einen relativ großen Bereich des Bürgersteigs filmte. Mittels dieser Kamera wurden daher auch zufällig vorbeilaufende Passanten gefilmt, die keine Besucher des Wettbüros waren.

Eine solche großflächige Überwachung des öffentlichen Raumes ohne jeglichen Zweck stellt einen Verstoß gegen die DSGVO dar. Die zuständige Behörde verhängte daraufhin ein Bußgeld in Höhe

von 4.800 Euro. Damit bewegt sich dieses erste Bußgeld zwar noch im unteren Bereich, wenn man den Vergleich zu den möglichen Höchststrafen im Millionenbereich zieht. Dennoch ist der Betrag deutlich höher als bei vergleichbaren Fällen unter der alten Rechtslage.

Ein weiteres Bußgeld in Höhe von 400.000 Euro erhielt ein portugiesisches Krankenhaus. Berichten zufolge soll die Krankenhausbetreiberin IT-Technikern Zugang zu Patientendaten gewährt haben, auf die nur Ärzte hätten Zugriff haben dürfen. Ferner seien im internen System insgesamt fast tausend Benutzer in der Rolle als Arzt registriert gewesen und hatten demnach vollumfänglich Zugriff auf Patientendaten, obwohl das Krankenhaus nur rund dreihundert Ärzte beschäftigte. Der Verstoß bestand darin, dass abteilungsübergreifend Zugriff zu personenbezogenen, insbesondere sensiblen Daten gewährt wurde, ohne dass hierfür eine explizite Berechtigung bestand.

Rekordbußgelder in England

In England wurden seit Inkrafttreten der DSGVO bereits zwei Rekordbußgelder verhängt. Rund 183 Millionen Pfund wurden einer britischen Fluggesellschaft auferlegt. Grund hierfür war die mangelnde IT-Sicherheit. So konnten Dritte von der Fluggesellschaft unter anderem Adressen, Zugangsdaten, Name sowie Kreditkartendaten (inklusive CVV-Nummern) abgreifen. Auch wenn das Bußgeld auf dem ersten Blick exorbitant hoch erscheint, wurde der Höchstsatz noch nicht ansatzweise erreicht. Die Geldstrafe beträgt lediglich 1,4 Prozent des weltweit erzielten Konzernumsatzes.

110 Millionen Euro wurden gegen eine Hotelkette ausgesprochen. Auch hier war die mangelnde IT-Sicherheit Grund für das Bußgeld. Nach einem bekanntgewordenen Hackingangriff wurden Daten von rund 339 Millionen Kunden abgegriffen. Neben Namen und Adressdaten wurden teilweise auch vertrauliche Daten wie Pass- und Kreditkartennummern abgegriffen, die zudem unverschlüsselt waren.

Es ist nicht bekannt, ob das Bußgeld bereits rechtskräftig ist. Das Unternehmen hatte angekündigt, gegen den Bescheid vorzugehen.

Auch Google von Bußgeld betroffen

Möglicherweise war es nur eine Frage der Zeit, bis es auch einen der „Big-Player“ des Internets er-

wischt. In Frankreich wurde das erste DSGVO-Bußgeld gegen die Google Inc. in Höhe von 50 Millionen Euro verhängt. Beanstandet wurden hier mangelnde

Informationspflichten hinsichtlich der Verarbeitung personenbezogener Daten. Die Angaben hierzu seien nur über mehrere Links und Buttons erreichbar und einige Informationen nicht klar und verständlich formuliert. Der Nutzer musste sich mühe-

voll durchklicken, um die entsprechenden Informationen zu erhalten. Auch die eingeholten Einwilligungen seien nach Angaben der französischen Behörden unzureichend. Erforderlich ist nach der DSGVO eine „informierte Einwilligung“. Dieser Pflicht kam Google nach Auffassung der Behörde nicht nach.

Spanische Fußballliga

Nicht nur die gängigsten Internetunternehmen sind bußgeldgefährdet. Dies zeigt das Beispiel der spanischen Fußballliga, dem Gegenstück zur deutschen Bundesliga. Diese erhielt ein Bußgeld in Höhe von 250.000 Euro. Grund hierfür war die App „La Liga“. Sie habe auf Positionsdaten und das Mikrofon des Smartphones zugegriffen, ohne dass der Nutzer darüber informiert wurde. Mit dem Zugriff auf das Mikrofon in Verbindung mit den Positionsdaten sollte herausgefunden werden, ob jemand ohne Lizenz Spiele zeigt.

Der Betreiber der App dementierte jedoch diese Ansicht und kündigte an, gerichtlich gegen diese Entscheidung vorzugehen. Die App mache keinen Mitschnitt, sondern erfasse nur Tonfragmente.

Europäische Nachbarn deutlich strenger

Der Vergleich mit den europäischen Nachbarn zeigt, dass die Bußgelder dort teilweise deutlich höher ausfallen als hierzulande. Während in England bereits Bußgelder von hunderten Millionen verhängt wurden, bewegen wir uns in Deutschland mit dem höchsten Bußgeld von rund 35 Millionen Euro auch hoch, aber immer noch in einem niedrigeren Bereich. Auch wenn zumindest in Deutschland ein Modell zur einheitlichen Berechnung von Bußgeldern verabschiedet wurde, wäre es wünschenswert, ein einheitliches europäisches Modell zur Bußgeldberechnung einzuführen, um neben dem einheitlichen Datenschutzniveau auch ein einheitliches Bußgeldniveau zu schaffen. (anm) 

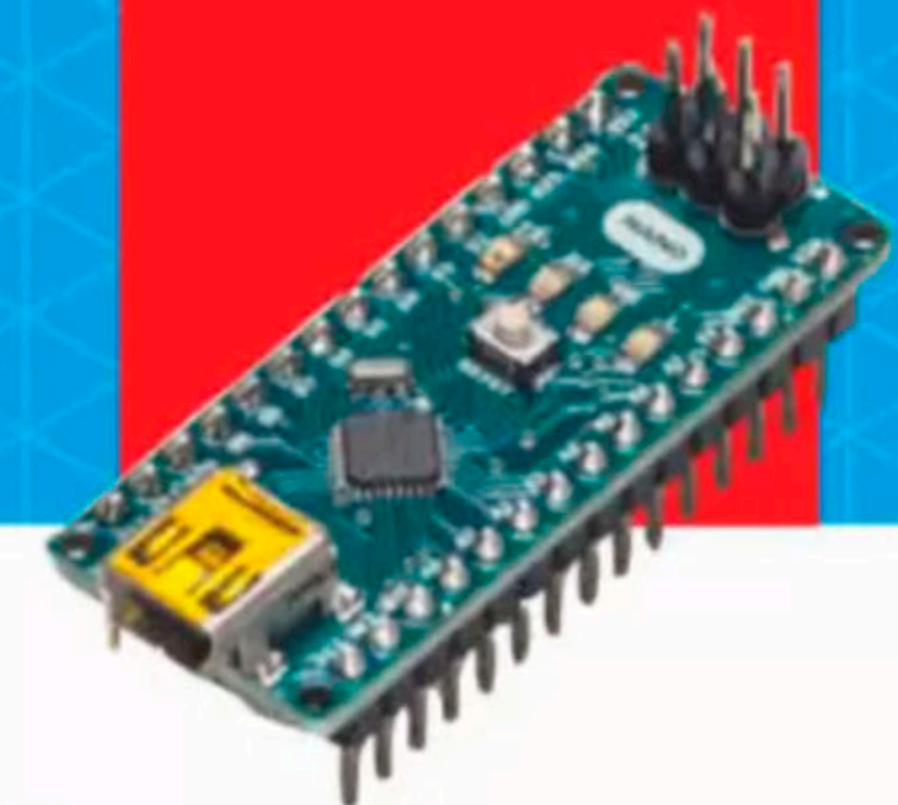
Make:



DAS KANNST DU AUCH!



GRATIS!



2× Make testen und 6 € sparen!

Ihre Vorteile:

- ✓ **GRATIS dazu:** Arduino Nano
- ✓ **NEU:** Jetzt auch im Browser lesen!
- ✓ Zugriff auf Online-Artikel-Archiv*
- ✓ Zusätzlich digital über iOS oder Android lesen

Für nur 15,60 Euro statt 21,80 Euro.

* Für die Laufzeit des Angebotes.

Jetzt bestellen: make-magazin.de/miniabo

Abmahnungen



Bislang ist die zunächst befürchtete Abmahnwelle ausgeblieben. Das muss aber nicht so bleiben.

Von Joerg Heidrich und Brian Scheuch

Für die größte Panik sorgte vor dem Inkrafttreten der DSGVO die Furcht vor Abmahnungen durch Konkurrenten und Abmahnvereine. Solche Abmahnungen gab es in der Praxis bisher allerdings nur selten: Mal wurde eine fehlende Datenschutzerklärung abgemahnt, ein anderes Mal ein fehlender Opt-In für die Verwendung von Google Analytics. In beiden Fällen wurde die Abgabe einer Unterlassungserklärung sowie die Erstattung der Rechtsanwaltskosten verlangt.

Bislang ist es nach wie vor umstritten, ob Verstöße gegen die DSGVO als Marktverhaltensregelung angesehen werden können und somit überhaupt abmahnbar sind. Während das Landgericht Bochum (Az.: 12 O 85/18) entschied, dass DSGVO-Verstöße nicht abmahnbar sind, befand das Landgericht Würzburg, dass eine fehlende Datenschutzerklärung grundsätzlich abmahnbar ist und somit einen Wettbewerbsverstoß darstellen kann (Landgericht Würzburg, Urteil vom 13.09.2018, Az.: 11 O 1741/18). Dieser Auffassung hat sich mittlerweile auch das Oberlandesgericht Hamburg (Urteil vom 25.10.2018, Az.: 3 U 66/17) angeschlossen. Klarheit kann hierbei nur der Bundesgerichtshof schaffen. Dieser hat bereits die Frage dem EuGH vorgelegt, ob DSGVO-Verstöße zu wettbewerbsrechtlichen Abmahnungen führen könnten.

Die anfängliche Furcht vor Abmahnungen war somit nicht ganz unbegründet. Auf Basis dieser ersten Entscheidungen ist zumindest nicht ganz ausgeschlossen, dass weitere Abmahnungen folgen werden. Die Frage der Zulässigkeit der Abmahnungen ist bislang noch nicht abschließend höchstrichterlich

geklärt. Die Tendenz geht wohl aber in die Richtung, dass DSGVO-Verstöße Marktverhaltensregelungen darstellen und somit abmahnbar sind. Angesichts dieser rechtlichen Unsicherheiten ist man gut beraten, wenn man die DSGVO insbesondere in der Außendarstellung entsprechend umsetzt, um sich unnötigen Ärger und Kosten zu ersparen.

Abmahnung aus Österreich

Aus Österreich gibt es seit 2019 erneut Abmahnungen betreffend der DSGVO. Dabei handelt es sich streng genommen um keine datenschutzrechtliche Abmahnung, sondern um eine urheberrechtliche.

Abgemahnt hat ein österreichisches Unternehmen, welches einen Datenschutzgenerator anbietet. Geworben wird explizit mit einer kostenlosen Datenschutzerklärung, wobei kostenlos jedoch nicht lizenzfrei bedeutet. In der Abmahnung wird sodann ein Betrag in Höhe von 3000 Euro gefordert, vergleichsweise würde man sich jedoch auf 1500 Euro einigen. Zudem wird die Abgabe einer strafbewährten Unterlassungs- und Verpflichtungserklärung verlangt. Die Beträge scheinen hier für einen

scheinbar „kostenlosen“ Generator maßlos überhöht. Immerhin müsste das Unternehmen bei einem Schadensersatzanspruch im Rahmen der Lizenzanalogie beweisen, dass sie solche Lizenzpreise aufrufen. Fraglich ist darüber hinaus auch, ob mithilfe eines Generators erstellte Datenschutzerklärungen überhaupt urheberrechtlichen Schutz haben, da es ihnen möglicherweise an der notwendigen Schöpfungshöhe fehlen könnte.



Rechtsanwaltsgebühren nach fehlerhafter Auskunft

Anfangs kursierte auch ein weiterer Fall, der nicht direkt mit Abmahnungen zu tun hat, aber ebenfalls darauf hinausläuft, die Rechtsanwaltskosten der Gegenseite zu erstatten. Hierbei registrierte sich eine natürliche Person in einem Onlineshop und gab dort ihre Adressdaten inklusive E-Mail-Adresse an. Gleichzeitig registrierte sich diese Person mit einer anderen E-Mail-Adresse für den Newsletter. Nunmehr forderte diese Person Auskunft nach DSGVO mit einer ihrer E-Mail-Adressen. Der Shop-Betreiber gab Auskunft über die registrierten Daten, vergaß aber beispielsweise, Auskunft betreffend der anderen E-Mail-Adresse zu erteilen, die sich für den Newsletter registriert hatte.

Kurz danach folgte ein Anwaltschreiben von einem Rechtsanwalt, der überwiegend im Straf- und Familienrecht tätig ist. Dieser wies den Shop-Betreiber darauf hin, dass die Auskunft fehlerhaft gewesen sei, und forderte anschließend unter Fristsetzung zur vollständigen Auskunft auf. Gleichzeitig forderte er die Erstattung der Rechtsanwaltskosten in Höhe von 334,75 Euro.

Es bleibt zweifelhaft, ob solch ein (scheinbar) rechtsmissbräuchliches Vorgehen vor Gericht Erfolg hätte. Dieses Beispiel zeigt aber einmal mehr, dass der Kreativität, Geld aus DSGVO-Verstößen zu ziehen, keine Grenzen gesetzt sind. Wie Sie richtig und vollständig Auskunft geben, lesen Sie ab Seite 78.



Abmahnwelle für fehlenden Cookie-Opt-In?

Mit dem Urteil des europäischen Gerichtshofs (EuGH) zum Thema Cookie-Einwilligung (siehe Seite 158) könnte unter Umständen eine neue Abmahnwelle kommen. Nur wenige Websites setzen derzeit die Vorgaben des EuGHs um. Fehlerhafte Cookie-Hinweise und Einwilligungen könnten ein gefundenes Fressen für Abmahner sein, denn üblicherweise bestehen die meisten Cookie-Banner lediglich aus einem "OK-Feld", was datenschutzrechtlich keiner aktiven Einwilligung entspricht.

Hier bleibt jedoch offen, welche Tendenz die gerichtliche Rechtsprechung verfolgt und wie der EuGH in der Sache entscheidend, und ob die DSGVO eine Marktverhaltensregelung im Sinne des Gesetzes gegen den unlauteren Wettbewerb (UWG) darstellt, oder nicht. Aber auch ohne höchstrichterliche Rechtsprechung bleibt die Gefahr einer Abmahnung nach wie vor bestehen.

Zwischenbilanz

Es zeigt sich, dass die Panik vor massenhaften Abmahnungen unbegründet war, aber noch nicht abschließend geklärt ist. Offen bleibt, wie sich diese Problematik weiterentwickelt. Abmahnungen dürften spätestens dann häufiger auftreten, wenn der EuGH und der Bundesgerichtshof endgültig zur Abmahnbarkeit von DSGVO-Verstößen entschieden haben. (anm) **ct**

Datenschutz-Dokumentation in Excel oder Word abhaken?

Das geht! Mit vorausgefüllten Vorlagen zum Verzeichnis von Verarbeitungstätigkeiten, technischen und organisatorischen Maßnahmen und vielen mehr.

Hier geht's zum Sonderangebot für c't Leser: dsgvo-vorlagen.de/ct

- ✓ Ohne Cloud
- ✓ Direkter Download
- ✓ Ohne Abo
- ✓ Keine versteckten Kosten



Schadensersatzansprüche

Neben den Abmahnungen und den Bußgeldern beinhaltet die DSGVO noch eine weitere Sanktionsmöglichkeit: den Schadensersatzanspruch. Gerade dieser oft immer noch unterschätzte Anspruch kann jedoch für Unternehmen sehr teuer und regelrecht existenzbedrohend werden. Und er gilt im Gegensatz zu den anderen Sanktionen auch für die Verwaltung.



Von Joerg Heidrich

Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz. Dies regelt Art. 82 des Datenschutzrechts. Eine derartige Regelung ist zwar nicht gänzlich neu. Neu ist allerdings die Möglichkeit eines Zahlungsanspruchs wegen immaterieller Schäden. Dieser Anspruch setzt zunächst Folgendes voraus:

- einen Verstoß gegen die DSGVO
- einen materiellen oder immateriellen Schaden des Betroffenen
- ein Verschulden des Verantwortlichen oder des Auftragsverarbeiters

Welche Art von Verstößen einen Schadensersatz auslösen können, wird beispielhaft in Erwägungsgrund 75 dargelegt. Dieser nennt als Beispiele Fälle, in denen die rechtswidrige Verarbeitung von Daten zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann.

Jenseits der Bagatellgrenze

Allerdings reicht nicht jede Form der Beeinträchtigung für einen Schadensersatzanspruch aus. Die Gerichte sind sich in den ersten Urteilen zu diesem Problemkreis völlig uneinig. Dabei streiten die Richter vor allem um die Frage, welche Qualität die Beeinträchtigung der Datenschutzrechte für den Betroffenen haben muss.

So entschied das Amtsgericht Diez mit Urteil im November 2018 (Az.: 8 C 130/18), dass ein geringfügiger Verstoß gegen die Vorschriften des Datenschutzes ohne ernsthafte Beeinträchtigung nicht ausreicht, um einen Anspruch nach Art. 82 DSGVO zu begründen. Gegenstand des Streits war eine E-Mail der Beklagten, mit der eine Einwilligung des Klägers zum Bezug ihres Newsletters eingeholt werden sollte. Der Empfänger der Mail machte einen Schmerzensgeldanspruch nach Art. 82 DSGVO geltend und verlangte mindestens 500 Euro. Das Gericht entschied, dass zumindest kein Anspruch vorhanden sei, der über den bereits von dem Mail-Versender freiwillig gezahlten Betrag von 50 Euro hinausgeht.

In einem anderen Fall entschied das Oberlandesgericht Dresden, dass die DSGVO bei Bagatelverstößen keinen immateriellen Schadensersatz nach Art. 82 rechtfertigt. Geklagt hatte ein Nutzer, der sich im Rahmen eines Social-Media-Angebots rassistisch geäußert hatte. Der Dienst hatte daraufhin das Posting sowie den Account des Klägers kurzfristig gesperrt. Einen Anlass für eine Geldentschädigung sah das OLG in dieser Sachlage allerdings nicht. Art. 82 sei nicht so auszulegen, dass er „einen Schadensersatzanspruch bereits bei jeder individuell empfundenen Unannehmlichkeit oder bei Bagatelverstößen, ohne ernsthafte Beeinträchtigung für das Selbstbild oder Ansehen einer Person begründet“.

5000 Euro für fehlende Auskünfte

Dieser Rechtsprechung stehen eine ganze Reihe von Urteilen gegenüber, bei denen ein Schadens-

ersatzanspruch von den Richtern bejaht wird. Danach reicht bereits ein Verstoß gegen die DSGVO aus. Ein Schaden liege in Form einer Persönlichkeitsrechtsverletzung bereits durch die unzulässige Verarbeitung vor. Hierfür reiche beispielsweise bereits eine unzulässige Offenlegung personenbezogener Daten gegenüber einem unberechtigten Dritten aus.

So hat das Arbeitsgericht Düsseldorf (Az. 9 Ca 6557/18) im März 2020 einem Kläger einen Schadensersatz in Höhe von 5000 Euro zugesprochen. Grund dafür war ein „Verlust der Kontrolle“ über seine Daten, weil das Unternehmen einen Auskunftsanspruch nicht nach den Vorgaben von Art. 15 DSGVO erfüllt habe. Dabei sei der Begriff des Schadens weit auszulegen. Zudem geht das Gericht davon aus, dass der zugesprochene Schadensersatz abschreckend wirken müsse.

Zu einem ähnlichen Ergebnis kam auch das AG Pforzheim (Az. 13 C 160/19). Es sprach einem Kläger einen immateriellen Schadensersatz zu, weil ein Psychotherapeut seine sensiblen Daten an einen Dritten weitergegeben hatte. Das Gericht stellte ebenfalls fest, dass Schadensersatz nach Art. 82 DSGVO eine abschreckende Wirkung erzielen müsse. Eine Zahlung in Höhe von 4000 Euro sei ausreichend, aber auch erforderlich, um eine Abschreckungswirkung zu erzielen und dem Kläger zugleich Genugtuung für das erlittene Unrecht zu gewährleisten.

Bedrohlich kann ein solcher Schadensersatz vor allem in solchen Fällen werden, in denen der datenschutzrechtliche Verstoß eine Vielzahl von Personen in gleicher Weise betrifft und Ausdruck einer bewussten, rechtswidrigen und im großen Stil betriebenen Kommerzialisierung ist. Unter dieser Prämisse sind Fälle vorstellbar, in denen ein sehr hoher Schadensersatz zu zahlen ist. Dies wäre etwa im medizinischen Bereich der Fall, wenn beispielsweise äußerst sensible Krankendaten unerlaubt und unter Verstoß gegen die Vorgaben der IT-Sicherheit an die Öffentlichkeit geraten und die Betroffenen dadurch einen erheblichen Nachteil erleiden.

Mitgefangen, mitgehangen

Die Regelung in Art. 82 DSGVO hält noch eine weitere Hilfe für Betroffene parat. Neben dem eigentlich für die Datenverarbeitung Verantwortlichen kann auch der Auftragsverarbeiter auf Zahlung in Anspruch genommen werden. Dies kann ein Hostprovider sein oder auch ein Cloud-Anbieter wie Amazon. Dieser haftet gesamtschuldnerisch, wodurch der Geschä-

digte ein Wahlrecht hat, wen er in Anspruch nimmt. Die Gesamtschuldner können die entstandenen Kosten dann intern ausgleichen. Für die Betroffenen bietet das den Vorteil, dass der Auftragsverarbeiter häufig solventer ist als deren Kunden – gerade, wenn eine größere Summe ansteht.

Allerdings haftet ein Auftragsverarbeiter für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder rechtmäßig erteilte Anweisungen seines Auftraggebers nicht umgesetzt hat.

Beweislastumkehr

Bemerkenswert ist auch, dass Art. 82 DSGVO eine Beweislastumkehr zugunsten des Betroffenen vorgibt. Dies wird unter anderem damit begründet, dass dieser mangels Einblick in die Datenverarbeitung kaum in der Lage ist, die notwendigen Beweise zu führen. Allerdings kann sich der Verantwortliche oder der Auftragsverarbeiter von seiner Haftung befreien, wenn er nachweisen kann, dass er für den Umstand, aufgrund dessen der Schaden eingetreten ist, in keiner Weise verantwortlich ist. Hierfür müsste er zum Beispiel nachweisen, dass er sich bei der Datenverarbeitung an den Pflichtenkatalog der DSGVO gehalten hat – einschließlich der Einhaltung des Stands der Technik in der IT.

Missbrauch

Bereits kurz nach Inkrafttreten der DSGVO versuchte ein Anwalt aus Berlin – ein alter Bekannter im Bereich Abmahnungen im E-Commerce –, Schmerzensgeldansprüche gegen Website-Betreiber geltend zu machen. Er warf den betroffenen Website-Betreibern vor, Kontaktformulare ohne SSL-Zertifikate vorzuhalten. Damit läge nach Auffassung des Anwaltes eine erhebliche Verletzung bei der Verarbeitung der Daten seines Mandanten vor. Mit dem Schreiben forderte er aufgrund der entstandenen „seelischen Belastung“ für seinen Mandanten die Zahlung eines Schmerzensgeldes in Höhe von 12.500 Euro. Dass der Jurist mit dieser eher dubiosen Vorgehensweise tatsächlich erfolgreich war, ist allerdings unwahrscheinlich. Von darauf erfolgten Zahlungen ist bislang nichts bekannt. Fest steht jedoch, dass der geforderte Betrag maßlos übertrieben ist, da solche Summen nicht einmal bei schwerwiegenden Verkehrsunfällen mit bleibenden Schäden gezahlt werden. (keh) 



Datenschutzbeauftragte

Die Bestellung eines geeigneten Datenschutzbeauftragten ist eine wichtige Voraussetzung, um die Auflagen der DSGVO zu erfüllen.

Von Brian Scheuch

Neue Benennungspflichten

? Wer muss einen Datenschutzbeauftragten benennen?

! Das neue Datenschutzrecht hatte anfangs die Anforderungen, ab wann ein Datenschutzbeauftragter (DSB) zu benennen ist, deutlich verschärft. Gemäß § 5 BDSG-neu benötigen öffentliche Stellen nun immer einen Datenschutzbeauftragten.

Für nicht-öffentliche Stellen, also Unternehmen, Vereine und andere Organisationen, war ursprünglich gemäß § 38 BDSG-neu und Artikel 37 DSGVO ein Datenschutzbeauftragter unter anderem zu bestellen, wenn:

- in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind,
- personenbezogene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung verarbeitet werden,
- Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung unterliegen,
- die Kerntätigkeit des Unternehmens in der umfangreichen regelmäßigen und systematischen Überwachung von Personen besteht,
- die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten (Gesundheitsdaten, Religionsdaten, ethnische Herkunft usw.) gemäß Art. 9 DSGVO besteht.

Mit einer Änderung des § 38 BDSG-neu hat der deutsche Gesetzgeber auf die Belastung, gerade klei-

nerer Unternehmen und Vereine reagiert. Seit Inkrafttreten der Änderung muss für nicht-öffentliche Stellen ein Datenschutzbeauftragter erst bestellt werden, wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind.

Die zuvor genannten Voraussetzungen müssen nicht kumulativ vorliegen, das heißt, die Benennungspflicht tritt ein, wenn mindestens eine dieser Alternativen gegeben ist.

Wie viele Personen an der automatisierten Verarbeitung beteiligt sind, ist dabei zum Teil schwierig zu beurteilen. Wenn beispielsweise das Unternehmen insgesamt 15 Personen beschäftigt, wovon allerdings 6 Personen gar keine Daten verarbeiten, wie etwa Reinigungskräfte, dann ist kein Datenschutzbeauftragter zu benennen. Es kommt auch nicht darauf an, ob Mitarbeiter in Vollzeit oder Teilzeit arbeiten. Auch Teilzeitmitarbeiter zählen grundsätzlich als vollwertige Mitarbeiter und nicht anteilig.

Fachliche Eignung

? Welche Voraussetzungen muss ein Datenschutzbeauftragter erfüllen?

! Artikel 37 Abs. 5 DSGVO verlangt, dass der Datenschutzbeauftragte auf Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf Grundlage seiner Fähigkeiten zur Erfüllung seiner Aufgabe benannt wird.



Eine explizite Definition, was unter beruflicher Qualifikation und Fachwissen zu verstehen ist, kann man dem Gesetz nicht entnehmen. Im besten Fall verfügt der Datenschutzbeauftragte über eine Zertifizierung oder hat an einem entsprechenden Lehrgang teilgenommen.

Grundsätzlich kann sich ein angehender Datenschützer das nötige Fachwissen auch autodidaktisch aneignen. Die Datenschutzaufsicht in Nordrhein-Westfalen vertritt beispielsweise die Auffassung, dass sich das erforderliche Niveau des Fachwissens nach den durchgeführten Verarbeitungsvorgängen und dem erforderlichen Schutzbedarf der personenbezogenen Daten richtet.

Danach gilt: Je komplexer die Datenverarbeitung und je größer die Menge der verarbeiteten Daten, insbesondere sensibler Daten, desto höhere Anforderungen sind an das notwendige Fachwissen des Datenschutzbeauftragten zu stellen.

Interessenskonflikte verhindern

? Wer darf Datenschutzbeauftragter werden?

! Der Datenschutzbeauftragte darf auch Beschäftigter des eigenen Unternehmens sein. Im Prinzip kann daher jeder Mitarbeiter, der über die entsprechende Qualifikation verfügt, als Datenschutzbeauftragter benannt werden.

Man darf jedoch niemanden benennen, der hierdurch in einen Interessenskonflikt geraten kann. Dazu gehören im Unternehmen regelmäßig folgende Gruppen:

- Geschäftsführung
- Leiter IT
- Leiter Personal
- Betriebsleiter

Diese Personengruppen können die Tätigkeit des Datenschutzbeauftragten nicht frei und unabhängig ausführen. Der IT-Leiter hat beispielsweise regelmäßig ein großes Interesse an Backups, das klassischerweise mit dem Recht auf Löschung kollidiert.

Aufgaben

? Welche Aufgaben hat der Datenschutzbeauftragte?

! Dem Datenschutzbeauftragten unterliegen gemäß Artikel 39 und § 7 BDSG-neu mindestens folgende Aufgaben:

- Unterrichtung und Beratung des Unternehmens sowie der Beschäftigten hinsichtlich der Pflichten aus europäischen und nationalen Datenschutzvorschriften
- Überwachung der Einhaltung der Datenschutzvorschriften
- Schulung und Sensibilisierung der Mitarbeiter
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit den Aufsichtsbehörden
- Anlaufstelle für die Aufsichtsbehörden, einschließlich vorheriger Konsultation gemäß Artikel 36 DSGVO

Der Datenschutzbeauftragte hat mit der Einführung der DSGVO eine Fülle an Aufgaben bekommen. Die Position des Datenschutzbeauftragten ist sowohl für ihn selbst, aber auch für das Unternehmen, das ihn benennt, nicht zu unterschätzen. Es ist keineswegs zu empfehlen, einen Datenschutzbeauftragten lediglich in der Datenschutzerklärung zu benennen, der ansonsten aber eher passiv tätig bleibt, wie es in der Vergangenheit oftmals geschehen ist.

Zu den wichtigsten Aufgaben gehören die Beratung, Schulung und Sensibilisierung des Unternehmens und der Mitarbeiter. Das Unternehmen und die Mitarbeiter sollen eine Anlaufstelle haben, um sich für Fragen des Datenschutzes entsprechend Rat einzuholen.

Unternehmenspflichten

? Welche Pflichten haben Unternehmen gegenüber dem Datenschutzbeauftragten?

! Nicht nur der Datenschutzbeauftragte hat eine Fülle an Aufgaben. Auch die Unternehmen haben ihm gegenüber einige Pflichten. Unternehmen müssen sicherstellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in allen Fragen in Bezug auf den Schutz personenbezogener Daten eingebunden wird.

Ferner müssen Unternehmen den Datenschutzbeauftragten auch unterstützen, indem sie die zur Erfüllung seiner Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung stellen.

Um seine Aufgaben ordnungsgemäß wahrzunehmen, benötigt der Datenschutzbeauftragte zunächst Arbeitszeit. Das Unternehmen muss ihm hierfür abseits seiner Haupttätigkeit ein angemessenes Stundenkontingent einräumen. Je nach Menge der Datenverarbeitung kann dies so umfangreich sein, dass diese Tätigkeit nicht nur beiläufig zum Hauptjob erledigt werden kann. Sowohl das Unternehmen als auch der Datenschutzbeauftragte selbst sollten sicherstellen, dass ein angemessenes Stundenkontingent für die Tätigkeit zur Verfügung steht.

Um Zugang zu den einzelnen Verarbeitungsvorgängen zu erhalten, muss er darüber hinaus abteilungsübergreifend in entsprechende Prozesse mit eingebunden werden. Damit sein Anspruch auf Erhaltung seines Fachwissens erfüllt wird, müssen Unternehmen eine regelmäßige Fortbildung ermöglichen.

Der Datenschutzbeauftragte muss weisungsfrei sein. Geschäftsführer und / oder Abteilungsleiter dürfen dem Datenschutzbeauftragten keine Anweisung geben, wie er seine Aufgabe zu erledigen hat. Andernfalls könnte er nicht auf die Einhaltung datenschutzrechtlicher Vorschriften hinwirken. Die Weisungsfreiheit gilt jedoch nicht bei seiner gegebenenfalls weiter ausgeführten Haupttätigkeit.

Der Datenschutzbeauftragte berichtet direkt an die höchste Managementebene. Unternehmen müssen daher sicherstellen, dass der Datenschutzbeauftragte auch entsprechend berichten kann. In kleinen und mittelständischen Unternehmen ist dies in der Regel keine Herausforderung. In großen Konzernen sind die Wege zum höchsten Management regelmäßig sehr weit, dennoch sind gerade Konzerne verpflichtet, einen entsprechenden Prozess zur Berichterstattung zu implementieren.

Kündigungsschutz

? Kann dem internen Datenschutzbeauftragten gekündigt werden?

! Der Datenschutzbeauftragte genießt gemäß § 6 BDSG-neu Kündigungsschutz. Das bedeutet: Eine ordentliche Kündigung des Datenschutzbeauf-

tragten scheidet grundsätzlich aus, sodass diesem nur aus wichtigem Grund gekündigt werden kann. Damit der Datenschutzbeauftragte wirklich weisungsfrei arbeiten kann, darf ihm bei Monierung von Datenverarbeitungsprozessen oder bei der Kommunikation mit den Aufsichtsbehörden keine Kündigung drohen. Auch wenn der Datenschutzbeauftragte seine Tätigkeit niederlegt, besteht der Kündigungsschutz noch ein Jahr fort.

Benennung

? Wie wird der Datenschutzbeauftragte benannt?

! Nach dem alten BDSG hatte die Bestellung des Datenschutzbeauftragten schriftlich zu erfolgen. Mit der Einführung der DSGVO ist dies nicht mehr zwingend notwendig. Die Benennung sollte trotzdem dokumentiert werden. Die DSGVO verlangt, dass die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und der Aufsichtsbehörde mitgeteilt werden. Fast alle Aufsichtsbehörden bieten mittlerweile die Möglichkeit an, den Datenschutzbeauftragten bequem online oder per Post zu melden.

Kontaktdaten

? Wo sind die Kontaktdaten des Datenschutzbeauftragten anzugeben?

! Liegt die Verpflichtung zur Benennung eines Datenschutzbeauftragten vor, so sind dessen Kontaktdaten auch zu veröffentlichen. Die Kontaktdaten sollten einerseits auf der Website des Unternehmens – in der Regel in der Datenschutzerklärung –, aber auch im unternehmensinternen Intranet veröffentlicht werden. Umstritten ist derzeit noch, was alles zu den Kontaktdaten gehört. Einigkeit besteht jedoch darin, dass mindestens die E-Mail-Adresse des Datenschutzbeauftragten zu veröffentlichen ist. Eine namentliche Nennung ist hingegen nicht erforderlich.



Externer DSB

? Kann ich auch einen externen Datenschutzbeauftragten benennen?

! Oftmals wird es schwierig sein, im eigenen Betrieb eine geeignete qualifizierte Person zu finden, die man als Datenschutzbeauftragten benennen kann. Dann kann man auch einen Externen als Datenschutzbeauftragten benennen. Man schont hiermit die eigenen personellen Ressourcen und kann Fortbildungskosten sparen. Ein weiterer Vorteil kann in der Neutralität bestehen, da der externe Datenschutzbeauftragte in keinem abhängigen Arbeitsverhältnis steht. Ein Nachteil besteht jedoch darin, dass dieser teilweise nicht vollumfänglich in die internen Prozesse mit eingebunden wird und Ansprechpartner sowie Betriebsabläufe nicht gut genug kennt.

Entscheidet sich das Unternehmen für die externe Lösung, sollte es auch hier darauf achten, dass je nach Umfang der Verarbeitungstätigkeiten ein ausreichendes Stundenkontingent zur Verfügung steht.

Im Internet gibt es unzählige Pauschalangebote, um einen externen Datenschutzbeauftragten zu benennen. Diese gehen von der reinen Benennung bis hin zu einem festen Beratungskontingent. Man sollte sich gut überlegen, ob man einen Datenschutzbeauftragten benennen möchte, der nur in der Datenschutzerklärung auftaucht, oder einen, der auch aktiv mitwirkt. Mit der passiven Lösung kommt man nur seiner Benennungspflicht nach. Dies führt aber regelmäßig dazu, dass man nicht vollumfänglich zum Datenschutz beraten wird und dieser auch nicht konsequent umgesetzt wird.

Lange Zeit war übrigens auch umstritten, ob der externe Datenschutzbeauftragte eine juristische Person (GmbH, AG, etc.) sein kann oder eine natürliche Person sein muss. Nach dem alten BDSG war auch die Bestellung einer juristischen Person möglich. Mit der DSGVO überwiegt nun die Ansicht, dass als Datenschutzbeauftragter immer eine natürliche Person benannt werden muss. Jedoch kann das Vertragsverhältnis mit einer juristischen Person erfolgen. (keh) **ct**

Kurzpapier der DSK:

ct.de/w2c5

Es gibt 10 Arten von Menschen. iX-Leser und die anderen.

Jetzt Mini-Abo testen:

3 digitale Ausgaben + Bluetooth-Tastatur nur 16,50 €

www.iX.de/digital-testen



www.iX.de/digital-testen



49 (0)541 800 09 120



leserservice@heise.de

iX
MAGAZIN FÜR PROFESSIONELLE
INFORMATIONSTECHNIK



Auskunftspflichten für Unternehmen

Die DSGVO bringt für Unternehmen zahlreiche Änderungen beim Umgang mit Daten. Eine der umfassendsten Pflichten stellt die Auskunftserteilung dar.

Von Niklas Mühleis

Eines der großen Ziele der DSGVO ist das Herstellen von Transparenz bei der Verarbeitung von Daten. Dazu gehören nicht nur die Informationspflichten für Datenverarbeiter (siehe Seite 46), sondern auch die Auskunftsrechte der von der Datenverarbeitung betroffenen Personen. Artikel 15 der DSGVO räumt den Bürgerinnen und Bürgern der EU umfangreiche Informationsrechte ein, die wiederum in Auskunftspflichten für Unternehmen, Vereine und Behörden münden.

Checkliste für den Datenschutz

Unternehmen sind dabei gut beraten, Auskunftsersuchen nicht auf die leichte Schulter zu nehmen. Sie sollten sich bereits vor der ersten Anfrage mit den Auskunftspflichten beschäftigen. Denn die Liste der Dinge, über die Auskunft verlangt werden kann, umfasst einen breiten Katalog an gesetzlichen Pflichten und die Zeit zur Beantwortung beträgt lediglich einen Monat.

Die Auskunftspflicht kann jedoch nicht nur als lästige Pflicht begriffen werden, sondern auch als

eine Checkliste, mit der man überprüfen kann, ob das eigene Unternehmen bereits datenschutzkonform arbeitet oder es Anlass zur Umstrukturierung gibt. Eine mögliche Auskunft, die von Betroffenen verlangt werden kann, ist beispielsweise jene über die Herkunft der gespeicherten personenbezogenen Daten. Sollten Sie feststellen, dass sie bei einem großen Teil Ihrer Kunden diese Frage nicht ohne Weiteres beantworten könnten, sollten Sie Ihre Kundendatei schleunigst auf den neuesten Stand bringen. Ein weiteres Beispiel kann die Frage nach der vorgesehenen Speicherung von personenbezogenen Daten sein. Wenn Sie diese nicht mit klaren gesetzlichen Mindestspeicherfristen oder Verarbeitungszwecken beantworten können, besteht auch hier dringender Nachholbedarf.

Keine Panik bei Albtraumbriefen

Eines der größten Schreckgespenster, das unter Datenverarbeitern derzeit umgeht, sind die ausführlichen Auskunftsverlangen, die sämtliche möglichen Auskünfte auf einen Schlag verlangen – die soge-

nannten „Albtraum-Briefe“. Die Erzählungen dazu variieren zwischen „ein Brief hat unseren Hausjuristen drei Wochen Arbeitszeit gekostet“ und „am ersten Tag der DSGVO hatten wir 20 Auskunftsverlangen im Postkasten.“ Richtig ist, dass die unvorbereitete Beantwortung eines Auskunftsverlangens mit viel Arbeit verbunden ist und nicht nebenbei erledigt werden kann.

Wichtig ist jedoch auch zu wissen, dass bei vielen Fragen oftmals eine Musterantwort gegeben werden kann, unabhängig davon, wer fragt. So lässt sich für die Frage nach der Weiterleitung von Daten in Drittländer oder an internationale Organisationen eine Musterantwort vorformulieren, die dann bei den meisten Anfragen hierzu ausreicht. Gleiches gilt für die Speicherdauer von personenbezogenen Daten und die Verwendung von automatisierter Entscheidungsfindung.



Für die weitere Vorbereitung auf Auskunftsverlangen empfiehlt es sich, personenbezogene Daten nur den Personen im Unternehmen zur Verfügung zu stellen, welche auch aktiv mit deren Bearbeitung beauftragt sind. Zudem sollte man personenbezogene Daten auf möglichst wenig unterschiedlichen Datenbanken speichern und verarbeiten, um das Zusammenstellen von Informationen zu einer spezifischen Anfrage zu erleichtern. Eine gute Vorarbeit kann somit im Falle einer Anfrage eine Menge Arbeit ersparen und selbst Albtraum-Briefen den Schrecken nehmen. Zahlreiche Unternehmen, vor allem sehr große mit immens vielen Kunden, haben mittlerweile ihre IT so weit angepasst, dass diese Auskunftsverlangen automatisiert bearbeitet und Antworten an die Kunden versendet. Welche Informationen in einem Auskunftersuchen konkret beantragt werden können, finden Sie auf Seite 24.



Bitte identifizieren

? Gibt es bestimmte Prüfpflichten vor der Auskunftserteilung?

! Damit Daten nicht in falsche Hände geraten, muss bei eingehenden Anträgen auf Auskunftserteilung zunächst die Identität des Antragstellers geprüft werden. Bei berechtigten Zweifeln, wenn etwa ein Auskunftersuchen über eine dem Unternehmen bislang unbekannte E-Mail-Adresse versendet wird, sollte ein Identitätsnachweis gefordert

werden. Dies muss im Zweifel über die Zusendung des Personalausweises in Kopie geschehen, um sicherzustellen, dass niemand in fremdem Namen Auskunftsrechte geltend macht. Doch Achtung: Eine vollständige Kopie des Personalausweises zu verlangen ist unzulässig, da dadurch Daten erhoben werden, die für die Identitätsüberprüfung nicht erforderlich sind. Kopien von Ausweisen sollten daher nur mit dem Hinweis verlangt werden, dass bis auf Namen und Adresse alle weiteren Angaben zu schwärzen sind.

Weiterhin sollte geprüft werden, ob die Frist zur Beantwortung eingehalten werden kann.

Protokolle bitte

? Erstreckt sich der Auskunftsanspruch auf interne Protokolle?

! An der Frage, wie weit der Auskunftsanspruch tatsächlich geht, scheiden sich oftmals die Geister. Während Unternehmen in der Regel so wenige Informationen wie möglich preisgeben wollen, um nicht etwa Interna oder Geschäftsgeheimnisse zu offenbaren, will der Antragsteller zumeist alle Daten

zu seiner Person einsehen können. Ein erstes Urteil zu dieser Konfliktlage wurde mittlerweile vom Oberlandesgericht Köln gefällt. Nach dessen Ansicht handelt es sich auch bei firmeninternen Telefonnotizen und Gesprächsprotokollen um personenbezogene Daten. Diese müssen also auch ungeachtet des Aufwandes oder des Zwecks der Verwendung

an den Auskunftersuchenden herausgegeben werden. Mit dieser Entscheidung wurde der sehr umfassende Auskunftsanspruch der Betroffenen noch einmal bestätigt. Es empfiehlt sich daher, auch Protokolle zu Gesprächen und Telefonaten, welche mit den Betroffenen geführt wurden, im Rahmen des Antrags auf Auskunft herauszugeben.



Überprüfung des Auskunftsverlangens

Handelt es sich um ein Auskunftsverlangen und falls ja, welche Auskünfte werden verlangt?



Dokumentation der Anfrage

Dokumentieren Sie den Eingang der Anfrage mit dem Datum des Eingangs und den gewünschten Auskünften. Versehen Sie jede Anfrage von Anfang an mit dem Datum, bis zu dem eine Antwort erfolgt sein muss.



Identitätsprüfung

Stellen Sie sicher, dass Sie wirklich wissen, wer das Auskunftersuchen gestellt hat. In der Regel gibt es in jeder Datenbank mehr als einen Thomas Müller. Bei unbekannten E-Mail-Adressen ist in jedem Fall eine Nachfrage zur Identitätsbestätigung zu stellen.



Bestandsprüfung

Prüfen Sie nun, ob Sie überhaupt über personenbezogene Daten der betroffenen Person verfügen. Sollten Sie über keinerlei Daten verfügen, erteilen Sie dem Antragsteller eine entsprechende Mitteilung. In diesem Fall wäre nun Ihre Aufgabe getan.



Fristprüfung

Sollten Sie über personenbezogene Daten verfügen, überprüfen Sie nun, ob Sie die Anfrage fristgerecht beantworten können. Im Zweifelsfall können Sie die Frist zur Beantwortung um zwei Monate verlängern. Dies müssten Sie der betroffenen Person in diesem Fall jedoch begründet mitteilen.



Auskunftserteilung

Nach den Vorprüfungen beginnt nun die eigentliche Arbeit. Gehen Sie das Auskunftsverlangen Schritt für Schritt durch, stellen Sie sämtliche gewünschten und nach Art. 15 DSGVO zulässigen Auskunftsverlangen zusammen und übermitteln Sie diese dem Antragsteller.

Form und Frist

? Welche Fristen und Formvorschriften sind zu beachten?

! Grundsätzlich muss die Auskunftserteilung unverzüglich, also ohne schuldhaftes Zögern erfolgen. Die Standardfrist zur Beantwortung beträgt einen Monat. In Ausnahmefällen, zum Beispiel, wenn besonders viele Anfragen gleichzeitig zu beantworten sind oder die Beantwortung mit einem ungewöhnlich hohen Arbeitsaufwand verbunden ist, kann die Frist um zwei Monate verlängert werden. Dies muss jedoch stets gegenüber den Auskunftssuchenden begründet werden.

Die Auskunftserteilung kann schriftlich oder elektronisch erfolgen. Sämtliche zulässig gestellten Fragen sind zu beantworten und eine Kopie der personenbezogenen Daten ist zur Verfügung zu stellen. Wurde der Antrag elektronisch gestellt, so sind die Informationen in einem gängigen elektronischen Format zu übermitteln, sofern der Betroffene nichts anderes angegeben hat. Hierzu gibt Erwägungsgrund 63 der DSGVO vor, dass die elektronische Aus-

kunftserteilung Sicherheitsanforderungen zu genügen hat. Dies kann man beispielsweise mittels einer verschlüsselten Übertragung erreichen.

Einmal Kostenerstattung bitte

? Kann ich die Kosten, die durch die Auskunftserteilung entstehen, in Rechnung stellen?

! Grundsätzlich können die Kosten, die durch die Erteilung einer Auskunft nach Art. 15 DSGVO entstehen, nicht auf den Antragsteller umgelegt werden. In wenigen Fällen ist dies jedoch möglich. Im Falle von exzessiven, also sich stetig wiederholenden Auskunftsverlangen sieht Art. 12 Abs. 5 DSGVO vor, dass man die Auskunftserteilung entweder verweigern oder ein angemessenes Entgelt als Ausgleich verlangen kann. Verlangt der Antragsteller mehr als eine Kopie seiner gespeicherten personenbezogenen Daten, kann man nach Art. 15 Abs. 3 DSGVO man hierfür ebenfalls ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen. (keh) **ct**



Kurzpapier
der DSK:

ct.de/wkeb

ct <webdev>

< 10. Februar 2021 >
ONLINE

Die Konferenz für Frontend-Entwicklung • WORKSHOP-PROGRAMM

Sven Wolfermann – Web-Performance 2021

Sven Wolfermann stellt den gesamten Performance-Werkzeugkoffer des Web-Entwicklers ausführlich vor:

- > Wie werden WebFonts effizient geladen?
- > Was ist bei CSS, JavaScript und Bildern zu beachten?
- > Wie testen Sie und wie automatisieren Sie das Monitoring?

André Kovac – Von 0 auf App: Mobile-App-Entwicklung mit React Native

In diesem Hands-on-Workshop entwickelt André Kovac gemeinsam mit Ihnen eine kleine mobile App.

- > ReactNative-Grundlagen: Komponenten, Styling und User-Interaktion
- > Lokales StateManagement mit Hooks, Umgang mit Smartphone-Sensordaten, Animationen

Peter Kröner – Unter der Haube

Peter Kröner versorgt Sie mit dem Wissen rund um JS-Engine-Internia, das Sie brauchen, um Ihre JavaScript-Projekte flott und am Laufen zu halten.

- > V8-Bytecode und die Effekte von optimierenden Compilern
- > Performance-Best-Practices
- > Tools für die Performance-Analyse

Jetzt
10 %
Kombi-Rabatt
sichern!



 Heise Medien

www.ctwebdev.de

Rechtmäßige Videoüberwachung



Die Erfassung von Personen durch Videokameras stellt potenziell einen tiefen Eingriff in die Rechte der Betroffenen dar. Deshalb sollte man vorab genau prüfen, ob und wie man die Überwachung rechtskonform durchführen kann.

Von Nick Akinci

Videoüberwachung definiert der Gesetzgeber als die „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“. Wesentliches Merkmal ist dabei, dass die Kamera ein Bildsignal überträgt. Irrelevant ist, ob auch eine Aufzeichnung stattfindet oder man lediglich eine Streaming-Lösung wählt. Ebenso wenig macht es einen Unterschied, ob ein flüssiges Video oder in regelmäßigen (kurzen) Abständen aufgenommene Einzelbilder übertragen werden.

Unter öffentlichen Räumen versteht man alle Bereiche, die der Öffentlichkeit ausdrücklich oder aufgrund einer nach außen erkennbaren Zweckbestimmung zugänglich sind. Dies gilt auch, wenn man den Bereich nur nach vorheriger Anmeldung oder gegen Entgelt betreten darf, sofern diese Möglichkeit grundsätzlich jedem offen steht.

Öffentliche Bereiche in diesem Sinne sind daher beispielsweise U-Bahn-Stationen, Tankstellen, Verkaufsflächen von Ladengeschäften, Konzertgelände,

Fußballstadien sowie öffentliche Gehwege und Straßen.

Eine rein private Nutzung von Überwachungskameras zum Beispiel im heimischen Garten unterliegt nicht den Regelungen der DSGVO. Erfasst die Videokamera dabei jedoch auch öffentliche Flächen wie den angrenzenden Gehweg, so sind die datenschutzrechtlichen Anforderungen zu beachten.

Wer eine Videoüberwachung plant, sollte genau prüfen (lassen), ob diese im jeweiligen Einzelfall rechtlich zulässig ist. Auch die Anforderungen an die IT-Sicherheit sind in der Regel vergleichsweise hoch, da Videoaufnahmen von Personen immer auch besonders sensible Daten enthalten können.

Rechtsgrundlagen

Die beiden wichtigsten Rechtsgrundlagen für die Videoüberwachung finden sich eigentlich außerhalb der DSGVO, nämlich in Paragraph 4 des BDSG. Danach ist eine Videoüberwachung unter anderem rechtmäßig, wenn sie „zur Wahrnehmung des Hausrechts“ oder „zur Wahrnehmung berechtigter Interessen



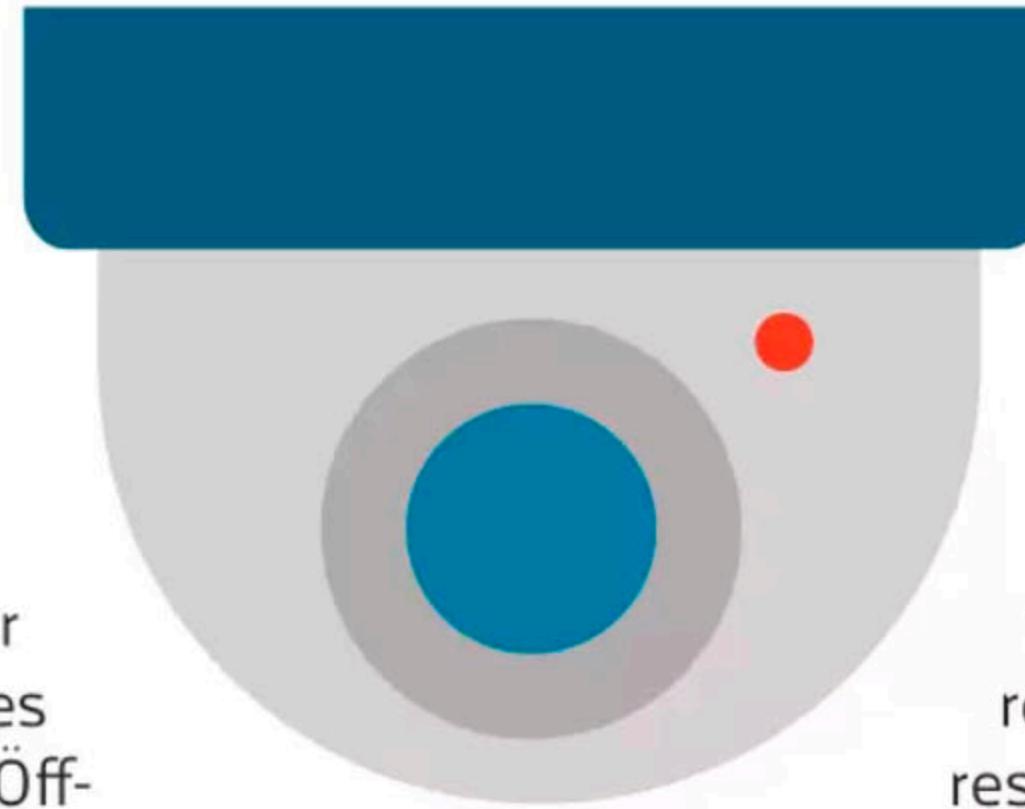
für konkret festgelegte Zwecke“ durchgeführt wird.

Das Bundesverwaltungsgericht (BVerwG) hat in seinem Urteil vom 27.03.2019, Aktenzeichen: 6 C 2/18, jedoch die Auffassung vertreten, dass die Regelung des BDSG nicht anwendbar ist, da die DSGVO als abschließendes Regelwerk keine entsprechende Öffnungsklausel für eine nationale Regelung enthalte. Problematisch erscheint in diesem Zusammenhang, dass die DSGVO keine speziellen Regelungen zur Videoüberwachung bereithält. Konsequenterweise urteilte das Gericht daher, dass die Zulässigkeit einer Videoüberwachung, wie jede andere Verarbeitung von personenbezogenen Daten, an den allgemeinen Voraussetzungen des Art. 6 DSGVO zu messen sei. Dieser Auffassung hat sich nun auch die Datenschutzkonferenz (DSK) – ein Gremium bestehend aus Vertretern der Datenschutzaufsichtsbehörden des Bundes und der Länder –, angeschlossen, die im Juli 2020 eine umfassende Orientierungshilfe zur Videoüberwachung veröffentlicht hat (siehe [ct.de/wdcx](https://www.ct.de/wdcx)). Fraglich ist daher, ob sich dadurch an der Rechtslage etwas geändert hat.

Nach dem eigentlich geltenden § 4 BDSG ist eine Videoüberwachung nur zu bestimmten Zwecken möglich. Es wäre dann jeweils zu prüfen, ob die Videoüberwachung für die Erreichung dieser Zwecke tatsächlich erforderlich ist und ob keine schutzwürdigen Interessen der Betroffenen entgegenstehen. Zumindest letztere Voraussetzung dürfte sich sehr nah an der Interessenabwägung bewegen, die auch nach Artikel 6 DSGVO zu treffen ist (siehe hierzu Seite 16).

Der offene Wortlaut der DSGVO lässt es außerdem zu, dass im Rahmen dieser Abwägung, die in § 4 BDSG genannten Zwecke trotzdem als besonders schutzwürdige Interessen berücksichtigt werden können. Insofern spricht einiges dafür, dass das Urteil des Bundesverwaltungsgerichts nur wenig Einfluss auf die eigentliche Rechtslage haben wird. Vielmehr ist davon auszugehen, dass die bisher zu § 4 BDSG und dessen Vorgängernorm entwickelten Grundsätze auch weiterhin Berücksichtigung finden werden.

Das Hausrecht umfasst insbesondere das Recht der Zugangskontrolle zu befriedetem Besitztum. Zur Überwachung öffentlich zugänglicher Betriebsgelände oder Ladenflächen kann man diese Rechtsgrundlage daher in den meisten Fällen heranziehen.



So darf zum Beispiel ein Kaufhaus den Eingangsbereich überwachen, um festzustellen, ob Personen trotz Hausverbot das Gebäude betreten.

Geht es um die Verhütung und Verfolgung von Straftaten, so dürfen in der Regel sowohl das Hausrecht als auch die berechtigten Interessen des Überwachenden zum Tragen kommen. Die Interessen des Verantwortlichen werden hier regelmäßig überwiegen und damit die Überwachung zulässig sein.

Rechtmäßig ist eine Videoüberwachung zu Sicherheitszwecken insbesondere dort, wo man nach der allgemeinen Lebenserfahrung mit der Begehung von Straftaten rechnen kann und die Überwachung durch Sicherheitspersonal unverhältnismäßig wäre, beispielsweise in U-Bahn-Stationen.

Informationspflichten

Bei der Videoüberwachung gelten für die Verantwortlichen besondere Hinweispflichten. Personen müssen sich frei entscheiden können, ob sie den überwachten Bereich betreten oder nicht. Hierzu müssen an geeigneten Stellen entsprechende Hinweisschilder gut sichtbar angebracht werden. Inhaltlich müssen diese gemäß Paragraph 4 Absatz 2 BDSG insbesondere auf den Umstand der Überwachung hinweisen und die Kontaktdaten des Verantwortlichen aufführen. Nimmt man das Urteil des Bundesverwaltungsgerichts ernst, so dürfte konsequenter Weise auch diese Regelung keine Anwendung mehr finden. Jedoch sieht Art. 13 der DSGVO ebenso vor, dass die Informationspflichten bereits im Zeitpunkt der Erhebung der Daten gelten. Auch das Nennen des Verantwortlichen ist nach der DSGVO Pflicht. Der Umstand, dass eine Videoüberwachung stattfindet, muss nach der europäischen Verordnung spätestens im Rahmen der Information über die Verarbeitungszwecke offenbart werden.

Auch an dieser Stelle dürfte sich also durch das Urteil des Bundesverwaltungsgerichts nichts an der Rechtslage ändern. Hinzu kommen die weiteren in



Art. 13 DSGVO vorgeschrieben, umfassenden Pflichtinformationen. Die DSK empfiehlt für Hinweisschilder eine Größe von mindestens DIN A4, um die Lesbarkeit zu gewährleisten.

Die Schilder sollten zunächst durch ein eindeutiges Piktogramm oder einen kurzen Text in großer Schrift deutlich auf die Überwachung hinweisen. Für die weiteren Informationen reicht eine Schriftgröße aus, die nur bei näherem Herantreten lesbar ist. Neben den Kontaktdaten des Verantwortlichen müssen insbesondere Informationen zu Rechtsgrundlage, Zweck, Speicherdauer und Datenweitergabe enthalten sein. Die Hinweisschild-Vorlage der DSK finden Sie am Ende der aktuellen Orientierungshilfe unter [ct.de/wdcx](https://www.ct.de/wdcx). Die Orientierungshilfe der DSK bietet darüber hinaus viele nützliche Hinweise bezüglich konkreter Fallkonstellationen und eine Checkliste für Betreiber.

Technische Umsetzung

Die Grundsätze der Datensparsamkeit und -minimierung gebieten es, den überwachten Bereich so klein wie möglich zu halten. Kameras sollten daher fest nur auf den Bereich ausgerichtet sein, der eine Überwachung erfordert. Dabei ist insbesondere auch darauf zu achten, dass man keine fremden Grundstücke und nur einen möglichst kleinen Bereich umliegender öffentlicher Verkehrsflächen erfasst. In Wohngebieten endet die Beobachtungsbefugnis nach Ansicht der DSK regelmäßig an der eigenen Grundstücksgrenze, da in diesem Bereich regelmäßig die Interessen der Betroffenen überwiegen.

Darüber hinaus ist auch das IT-Sicherheitskonzept nicht zu vernachlässigen (siehe auch Seite 124). Denn die Aufnahmen einer Videokamera können oftmals auch sensible Daten enthalten. Das Abbild einer Person kann regelmäßig Auskunft über seine ethnische Herkunft oder auch den Gesundheitszustand geben. Deshalb sollte man aus technischer Sicht zum Beispiel stets eine zuverlässige Verschlüsselungstechnologie einsetzen.

Der Grundsatz der Datenminimierung und das Merkmal der Erforderlichkeit gebieten es weiterhin

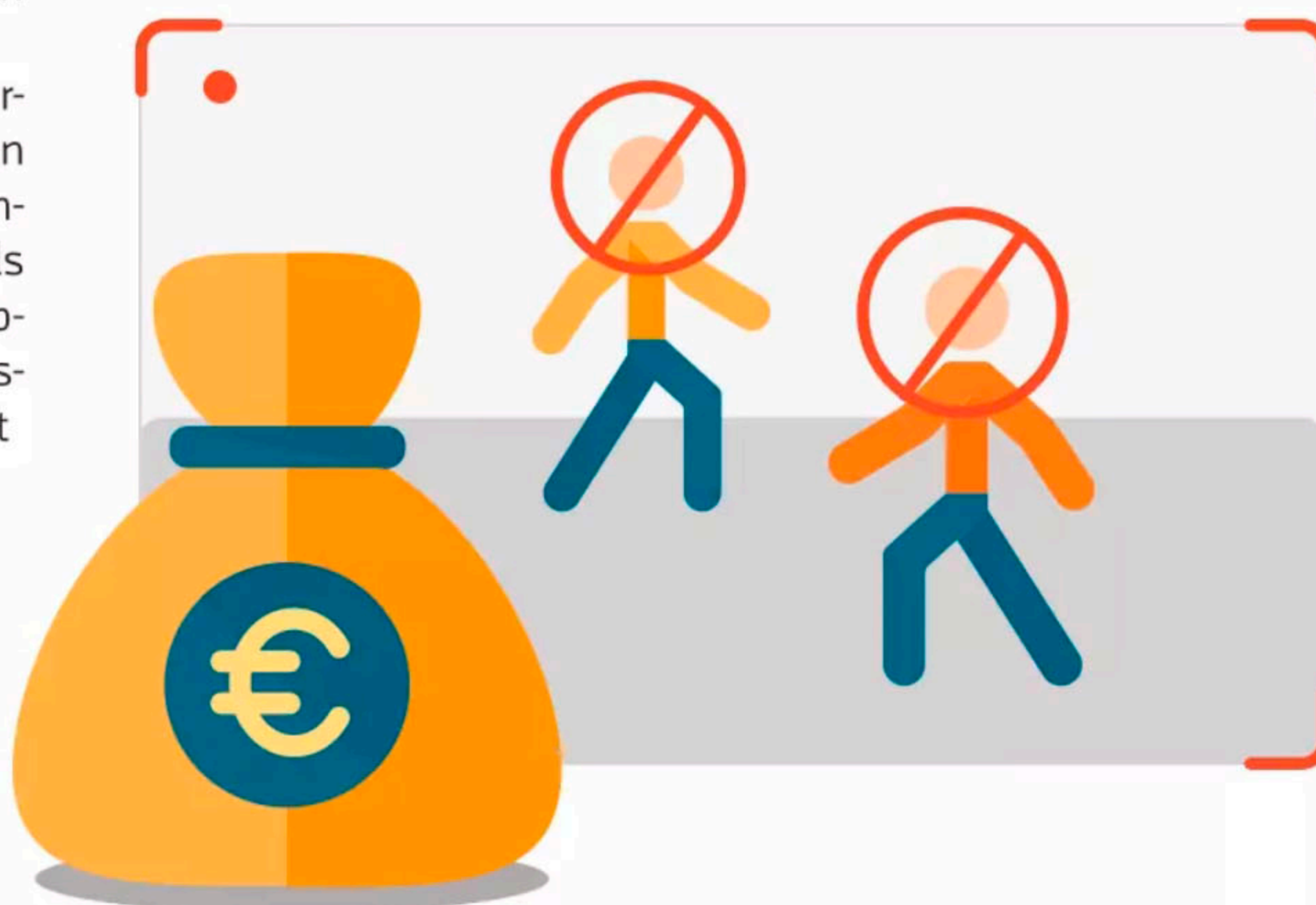
auch, dass man die Bilddaten nicht speichert, wenn auch eine Streaming-Lösung ausreichend ist. Ebenso sollte man auf einen Dauerbetrieb der Kameras verzichten, wenn die Gründe für die Überwachung nur zeitweise (zum Beispiel nachts) auftreten.

Sanktionen

Auch bei der Videoüberwachung ist die Verhängung von empfindlichen Bußgeldern möglich, wenn gegen die datenschutzrechtlichen Vorgaben verstoßen wird. In Europa, insbesondere Spanien, wurden mittlerweile bereits vielfach Bußgelder dafür verhängt, dass der Aufnahmebereich von Überwachungskameras auch fremde Grundstücke oder den öffentlichen Raum erfasste – diese bewegten sich meist im niedrigen 4-stelligen Bereich.

In Frankreich wurde einem Unternehmen ein Bußgeld in Höhe von 20.000 Euro wegen der unzulässigen Überwachung seiner Mitarbeiter auferlegt. In Deutschland musste ein Schwimmbadbetreiber ein Bußgeld in Höhe 12.000 Euro zahlen, da er unzulässiger Weise Gäste und Mitarbeiter des Schwimmbads gefilmt und die Aufnahmen gespeichert hatte. Hinzu kam, dass der mit der Wartung der Überwachungsanlage betraute Dienstleister Zugriff auf die Daten hatte, ohne dass ein Auftragsverarbeitungsvertrag mit diesem geschlossen wurde.

Mehr zum Thema Bußgelder können Sie auf Seite 62 lesen. (keh) **ct**



Beispiel
Hinweisschild:

[ct.de/wdcx](https://www.ct.de/wdcx)

NEUE
VERSION
2020/21

Ihr Erste-Hilfe-Set:

Das Notfall-System für den Ernstfall

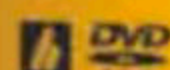
c't Desinfec't Das Rettungssystem bei Virenbefall

Windows-PCs untersuchen und säubern
Trojaner und Viren beseitigen
Daten retten und sofort wiederherstellen

Auf DVD & als Download
für USB-Sticks

c't Desinfec't

2020/21



Datenträger enthält
Info- und
Lehrprogramme
gemäß § 14 JuSchG

Die DVD für die Virenjagd

- Mit 4 Scannern: Avast, Eset, F-Secure, Sophos
- Sofort loslegen
- Windows reinigen
- 1 Jahr Signatur-Updates gratis

c't Desinfec't Das Rettungssystem bei Virenbefall

Windows-PCs untersuchen und säubern
Trojaner und Viren beseitigen
Daten retten und sofort wiederherstellen
Auf DVD & als Download
für USB-Sticks

c't Desinfec't



Die DVD für die Virenjagd
Mit 4 Scannern: Avast, Eset, F-Secure, Sophos
Sofort loslegen
Windows reinigen
1 Jahr Signatur-Updates gratis

Auch komplett auf
USB-Stick oder
als **Heft inkl. PDF**
mit **29% Rabatt**
erhältlich.

JETZT NEU! c't wissen Desinfec't 2020/21

Ist Ihr Windows erst verseucht, sind persönliche Daten in Gefahr. Hier greift Desinfec't 2020/21 ein, denn das Sicherheitstool bringt sein eigenes Betriebssystem mit und startet direkt von einem USB-Stick. So ist weiterer Schaden gebannt und mit den 5 Viren-Scannern geht's dann auf die Jagd nach dem Übeltäter.

shop.heise.de/desinfect2020

Einzelheft
für nur

14,90 € >

 **heise shop**

shop.heise.de/desinfect2020 >

> Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

Online-Gewinnspiele



Online-Gewinnspiele sind ein beliebtes Marketinginstrument, um auf Produkte aufmerksam zu machen, Adressdaten zu generieren oder die Markenidentität zu schärfen. Dabei werden naturgemäß personenbezogene Daten der Teilnehmer verarbeitet, die es zu schützen gilt.

Von Nick Akinci

Bei der Veranstaltung von Online-Gewinnspielen sind umfangreiche rechtliche Vorgaben zu beachten. So ergibt sich insbesondere aus dem Telemediengesetz (TMG) die Pflicht, umfassende Teilnahmebedingungen vorzuhalten. Aber auch das Thema Datenschutz spielt im Rahmen von Gewinnspielen eine wichtige Rolle. Denn ohne die personenbezogenen Daten der Teilnehmer geht es nicht – der Gewinner muss ermittelt und über seinen Gewinn benachrichtigt werden.

Datensparsamkeit

Auch im Rahmen von Gewinnspielen ist der Grundsatz derersparsamkeit zu beachten. Konkret bedeutet dies, dass von den Teilnehmern wirklich nur die personenbezogenen Daten erhoben und gespeichert werden sollten, die für die Durchführung des Gewinnspiels notwendig sind. Hierzu wird neben dem Namen und der Anschrift regelmäßig die E-Mail-Adresse und gegebenenfalls auch die Telefonnummer für den Fall der Bekanntgabe und Zusendung des jeweiligen Gewinns gehören. In Fällen, in denen lediglich digitale Inhalte verlost werden, kann man auf die Anschrift in der Regel verzichten. Auch sollte man darüber nachdenken, gegebenenfalls statt des Klarnamens nur ein frei zu wählendes Pseudonym zur Unterscheidung der Teilnehmer zu erheben, wenn mangels Postversand des Gewinns der echte Name nicht zwingend erforderlich ist.

Daneben darf man die für das Gewinnspiel erhobenen personenbezogenen Daten – wie auch sonst – ausschließlich für den Zweck nutzen, für den man sie erhoben hat. Daher sollte man die Daten der Teilnehmer zum Beispiel normalerweise nicht für Werbezwecke verwenden.

Noch eine Datenschutzerklärung?

Darüber hinaus muss man die Teilnehmer, ebenso wie bei dem Besuch einer Website, über die im Rahmen des Gewinnspiels stattfindenden Datenverarbeitungen informieren. Hierzu erstellt man entweder eine separate Gewinnspiel-Datenschutzerklärung oder man nimmt einen entsprechenden Abschnitt in die gegebenenfalls bereits auf der Website vorhandene Datenschutzerklärung auf. Wichtig ist, dass jeder Teilnehmer die Möglichkeit hat, sich vor der Teilnahme an dem Gewinnspiel über die damit einhergehenden Datenverarbeitungen zu informieren. Hierzu weist man in der Ankündigung des Gewinnspiels auf die Datenschutzerklärung hin und verlinkt diese dort.

Die für das Gewinnspiel erhobenen Daten sollte man nach der Ermittlung des Gewinners kurzfristig wieder löschen, soweit keine gesetzlichen Aufbewahrungsfristen bestehen. Steht der Gewinner fest, endet das Gewinnspiel und die Speicherung oder anderweitige Verarbeitung der Daten ist nicht mehr nötig.

Gegebenenfalls kann man die Daten der Nichtgewinner nach Ende des Gewinnspiels noch für einen kurzen Zeitraum aufbewahren, um einen neuen Gewinner auszulosen, für den Fall, dass man den ausgelosten Gewinner nicht ausfindig machen kann oder er den Gewinn nicht annehmen will. Hier kann ein Zeitraum von bis zu drei Wochen angemessen sein.

Grundlegende Informationen

Die Informationen, die man jedem Nutzer zur Verfügung stellen muss, ergeben sich aus Art. 13 DSGVO (vgl. hierzu den Artikel Datenschutzerklärung ab Seite 46). Hierzu gehören insbesondere die Information, auf welcher Rechtsgrundlage und zu wel-

chen Zwecken die Verarbeitung erfolgt, sowie die Dauer der Speicherung.

Als Rechtsgrundlage kommt bei Gewinnspielen regelmäßig die Verarbeitung zur Erfüllung eines Vertrages gemäß Art. 6 Abs. 1 S. 1 Buchst. b) DSGVO in Betracht. Denn durch die Teilnahme an dem Gewinnspiel kommt zwischen dem verlosenden Unternehmen und jedem einzelnen Teilnehmer ein Vertrag unter Einbeziehung der Gewinnspielbedingungen zustande. Bei der Angabe der Speicherdauer sollte man gegebenenfalls zwischen Gewinnern und Nichtgewinnern unterscheiden. Außerdem ist die für das Gewinnspiel verantwortliche Stelle zu nennen und der Teilnehmer über seine Rechte aus der DSGVO aufzuklären.

Öffentliche Bekanntgabe

Unproblematisch ist die öffentliche Bekanntgabe des Gewinners im Internet, wenn lediglich ein Pseudonym, wie etwa eine Losnummer oder ein Nickname genannt werden. Auch die Bekanntgabe unter hinreichender Anonymisierung des Gewinners, wie etwa „Gewonnen hat Uwe aus Hamburg.“ ist unbedenklich. Will man den Gewinner jedoch öffentlich mit seinem vollen Namen bekannt geben, so stellt dies einen weiteren Datenverarbeitungsvorgang dar, der seinerseits einer Rechtsgrundlage bedarf. Denn genau genommen ist die öffentliche Bekanntgabe des Gewinners für die Durchführung des Gewinnspiels nicht unbedingt notwendig – man kann den Gewinner auch direkt benachrichtigen. Viele Gewinnspielanbieter wünschen sich jedoch die öffentliche Bekanntgabe wegen ihres besonderen Werbeeffekts. Soll der Klurname des Gewinners genannt werden, benötigt man als sichere Rechtsgrundlage regelmäßig die Einwilligung des Teilnehmers. Diese muss man ausdrücklich, beispielsweise im Wege eines Opt-Ins durch Anklicken einer entsprechenden Checkbox einholen. Des Weiteren muss man die Einwilligung so ausgestalten, dass dem Teilnehmer bewusst ist, was mit seinen Daten geschieht.

Social Media-Gewinnspiele

Online-Gewinnspiele werden nicht nur auf Websites, sondern häufig auch auf Social-Media-Plattformen wie Facebook oder Instagram durchgeführt. Hier muss man neben wettbewerbs-, telekommunikations- und datenschutzrechtlichen Regelungen auch die Vorgaben der jeweiligen Social-Media-Plattform berücksichtigen. Facebook schreibt etwa vor, dass

die Teilnahme an einem Gewinnspiel nicht durch das „Teilen“ eines Beitrags auf dem eigenen Profil oder über einen sogenannten Hashtag erfolgen darf.

Werbeeinwilligung

Viele Unternehmen möchten den Teilnehmern des Gewinnspiels im Nachhinein Werbung zusenden – etwa in Form eines Newsletters. Auch hierfür braucht es eine ausdrückliche Einwilligung des Teilnehmers. Mit der Einwilligung bestätigt der Nutzer zum einen, dass seine Daten für Werbezwecke verarbeitet werden dürfen (datenschutzrechtliche Einwilligung) und zum anderen, dass er mit dem Erhalt von Werbung einverstanden ist (wettbewerbsrechtliche Einwilligung).

Besonders findige Anbieter machen die Anmeldung zum Newsletter zur Voraussetzung der Teilnahme am Gewinnspiel. Da der Gesetzgeber in Artikel 7 Absatz 4 DSGVO ein sog. Kopplungsverbot geregelt hat, ist dies problematisch. Denn grundsätzlich muss eine datenschutzrechtliche Einwilligung freiwillig erfolgen und darf nicht an einen Vertragsschluss gekoppelt werden.

Gänzlich freiwillig wäre die Einwilligung in den Newsletter-Erhalt aber nur, wenn eine Teilnahme an dem Gewinnspiel auch ohne Newsletter möglich ist. Es wird jedoch die Auffassung vertreten, dass man Gewinnspielteilnahme und Newsletter-Einwilligung dann koppeln kann, wenn man diese gegenüber den Teilnehmern klar kommuniziert. Dem Nutzer soll bewusst gemacht werden, dass er die Teilnahme am Gewinnspiel „mit seinen Daten bezahlt“. Gewinnspiele, bei denen man die Werbeeinwilligung zur Teilnahmevoraussetzung macht, sollte man daher niemals als „kostenlos“ bewerben. Um dem Teilnehmer deutlich zu machen, dass es sich um eine Art Tauschgeschäft „Daten gegen Gewinnmöglichkeit“ handelt, sollte man eine möglichst transparente Formulierung wählen. So kann man zum Beispiel dem Teilnehmer erklären, dass er „im Gegenzug“ für die Teilnahme am Gewinnspiel in den Erhalt eines Newsletters einwilligen soll. Im Übrigen gilt es bei der Kopplung von Gewinnspielen und Werbemaßnahmen insbesondere die wettbewerbsrechtlichen Anforderungen im Blick zu behalten. So muss unter anderem dem Teilnehmer die Möglichkeit eingeräumt werden, seine Einwilligung jederzeit zu widerrufen. Die Einwilligung sollte im Wege des Double-Opt-In-Verfahrens dokumentiert werden, bei dem der Einwilligende seine Einwilligung ein zweites Mal über eine ihm zugesandte E-Mail bestätigt. (keh) 

Gesundheitsdaten schützen



Gesundheitsinformationen zählen zu den sensibelsten Informationen über einen Menschen und bergen ein hohes Missbrauchspotential. Umso erstaunlicher ist es, dass Ärzte, Krankenhäuser oder Hersteller medizinischer Apps damit oft nachlässig umgehen. Doch wie genau sehen die gesetzlichen Vorgaben zum Umgang mit diesen Daten aus?

Von Joerg Heidrich

Die Zeiten, in denen Patienteninformationen allenfalls in einem geschützten Raum zwischen Ärzten, Laboren und Krankenkasse hin und her geschickt wurden, sind vorbei. Medizinische Daten sind längst ein Milliardenmarkt, von dem von Pharmagiganten über Forschungseinrichtungen bis hin zu mehr oder weniger seriösen App-Herstellern alle ihr Stück abhaben wollen.

Das zentrale Schutzobjekt der DSGVO sind die personenbezogenen Daten. Das sind Informationen, die sich auf eine natürliche Person beziehen und diese identifizieren oder mithilfe von zusätzlichen Informationen identifizierbar machen.

Gesundheitsdaten in der DSGVO

Noch stärker geschützt sind die „besonderen Kategorien von personenbezogenen Daten“. Art. 9 der DSGVO definiert darunter „Daten, aus denen die rassische und ethnische Herkunft, politische Mei-

nungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen“. Ebenso fallen darunter genetische Daten, biometrische Daten zur Identifizierung von Personen, Informationen zum Sexualleben oder der sexuellen Orientierung – und eben auch die Gesundheitsdaten.

Letztere definiert die DSGVO als Informationen, „die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“. Diese Definition ist sehr weit ausgelegt

und umfasst auch solche Angaben, aus denen auf den Gesundheitszustand einer Person geschlossen werden kann, also Diagnosen, Laborbefunde, Rezepte oder Pflegeinformationen. Nicht relevant ist die Herkunft der Daten, also ob diese direkt von einem Arzt oder einem Krankenhaus kommen oder



auch von einem Apotheker oder dem Beschäftigten einer Krankenkasse.

Ebenfalls zu den Gesundheitsdaten gehören solche Angaben, die einen Rückschluss auf die Konstitution einer Person zulassen: EKG-Werte, Dioptrien, Gewicht, Reha-Aufenthalte, Medikamentenliste. Schließlich fallen auch solche Daten darunter, die typischerweise an Gesundheits-Apps übermittelt werden, wie Puls oder Herzwerte, aber auch genetische Daten aller Art. Auch können Dokumente als Gesundheitsdaten unter den strengen Schutz des Art. 9 DSGVO fallen. Das gilt beispielsweise für Kontoauszüge, aus denen sich regelmäßige Zahlungen an eine Diabetes-Praxis oder der Kauf von orthopädischem Gerät ergibt.

Gesundheitsdaten rechtssicher nutzen

Hinsichtlich jeder Art von Nutzung personenbezogener Daten sieht die DSGVO ein Verbot mit Erlaubnisvorbehalt vor. Dies bedeutet, dass die Erfassung, Verarbeitung oder Weitergabe der Informationen erst einmal verboten ist – sofern nicht ausnahmsweise eine gesetzliche Erlaubnis vorliegt. Für „normale“ Daten sieht Art. 6 hier sechs verschiedene Möglichkeiten vor. Relevant sind insbesondere die Verarbeitung zu Zwecken der Erfüllung eines Vertrags und auf Basis eines „berechtigten Interesses“, welches allerdings das Interesse der betroffenen Personen überwiegen muss. Ebenfalls möglich ist es, eine Einwilligung des Betroffenen einzuholen.

Eine passende Rechtsgrundlage zu finden ist bereits im Rahmen von Art. 6 DSGVO schwer genug (siehe Seite 16). Für sensible Informationen wie Gesundheitsdaten schränken strenge Regelungen in Art. 9 die Möglichkeiten noch stärker ein. Dort findet sich beispielsweise eine Erlaubnis zur Verarbeitung „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren“. Ausnahmsweise rechtlich möglich ist auch die Nutzung der Krankheitsdaten im Bereich der Gesundheitsvorsorge, der Arbeitsmedizin oder der Forschung. Einige spezielle Sonderregelungen gibt es zudem

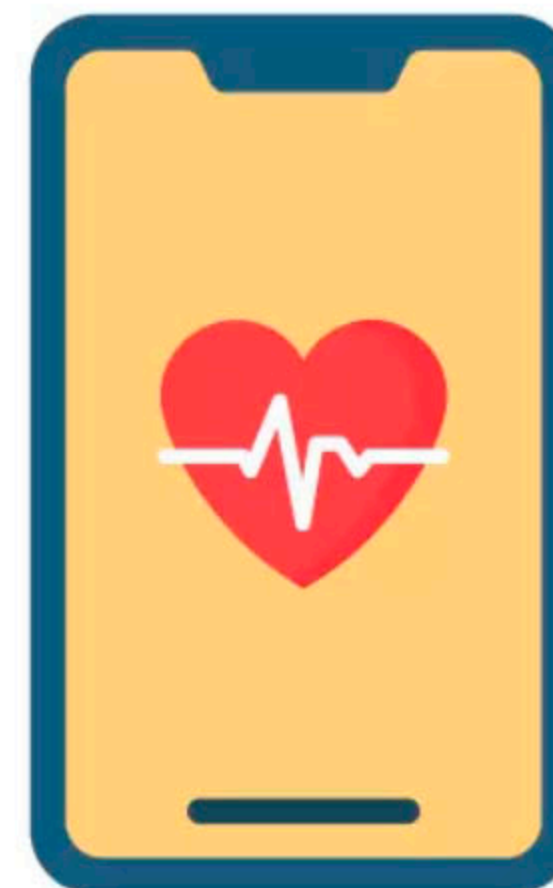
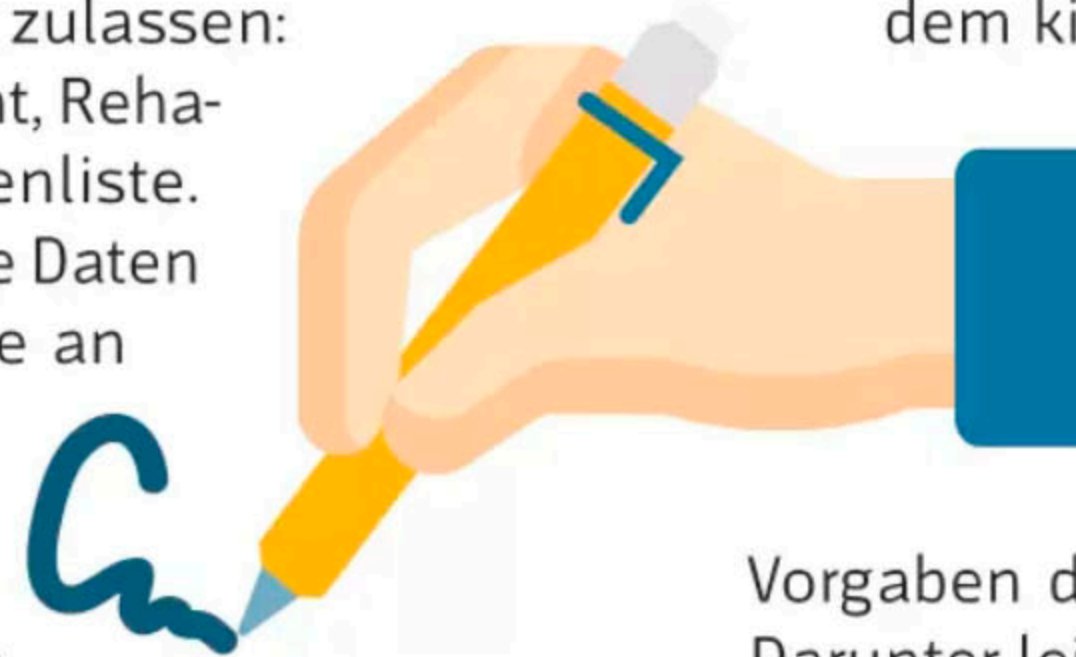
im Bereich der betrieblichen Nutzung durch die Paragraphen 22 und 26 des Bundesdatenschutzgesetzes (BDSG) sowie durch Regelungen in den Sozialgesetzbüchern, den Landesgesetzen oder dem kirchlichen Datenschutz.

Gut informiert?

Eine Nutzung außerhalb des klassischen Ärzte-, Krankenhaus- und Forschungsumfelds sehen die strengen Vorgaben der DSGVO nur sehr eingeschränkt vor. Darunter leiden insbesondere die Anbieter von Gesundheits-Apps – zumindest soweit sie den Datenschutz tatsächlich ernst nehmen, was nicht immer der Fall ist. Denn die einzige Möglichkeit zur Nutzung der sensiblen Kundendaten ist in der Regel die Einholung einer Einwilligung der Betroffenen. Und dies rechtswirksam zu tun, ist alles andere als trivial. Denn eine Einwilligung muss nicht nur freiwillig erfolgen: Die jeweilige Person muss detailliert darüber belehrt werden, was genau wie mit ihren Daten passieren soll.

Dabei reichen pauschale Formulierungen wie „Ich bin damit einverstanden, dass Anbieter XY meine Daten verarbeitet“ nicht aus. Nicht ausreichend ist es auch, Einwilligungen beispielsweise in den AGB oder der Datenschutzerklärung zu verstecken und diese pauschal abnicken zu lassen. Tatsächlich muss darüber informiert werden, wer welche Daten wie und gegebenenfalls auch wo verarbeitet. Wichtig ist auch die Angabe, dass der Betroffene seine Einwilligung jederzeit widerrufen kann, und die Angabe der Kontaktdaten, gegenüber wem er seine Zustimmung zurücknehmen kann. Seine Einwilligung auf dieser Basis muss der Betroffene dann explizit bestätigen, offline durch eine Unterschrift, online zum Beispiel durch das Ankreuzen eines Kästchens.

Auf Basis dieser Informationen muss der Betroffene wissen, worauf er sich mit der Einwilligung und der damit verbundenen Datenweitergabe einlässt. Stimmt er dem dann freiwillig zu, so können auch sensible Informationen verarbeitet werden. Ist die Information allerdings unvollständig, so fehlt es an einer Rechtsgrundlage zur Erhebung der Daten – was schlimmstenfalls mit einem Bußgeld geahndet werden kann. Die Erfahrung einer unrichtigen Einwilligung musste etwa Ende 2017 Facebook machen. Dort gab es kos-

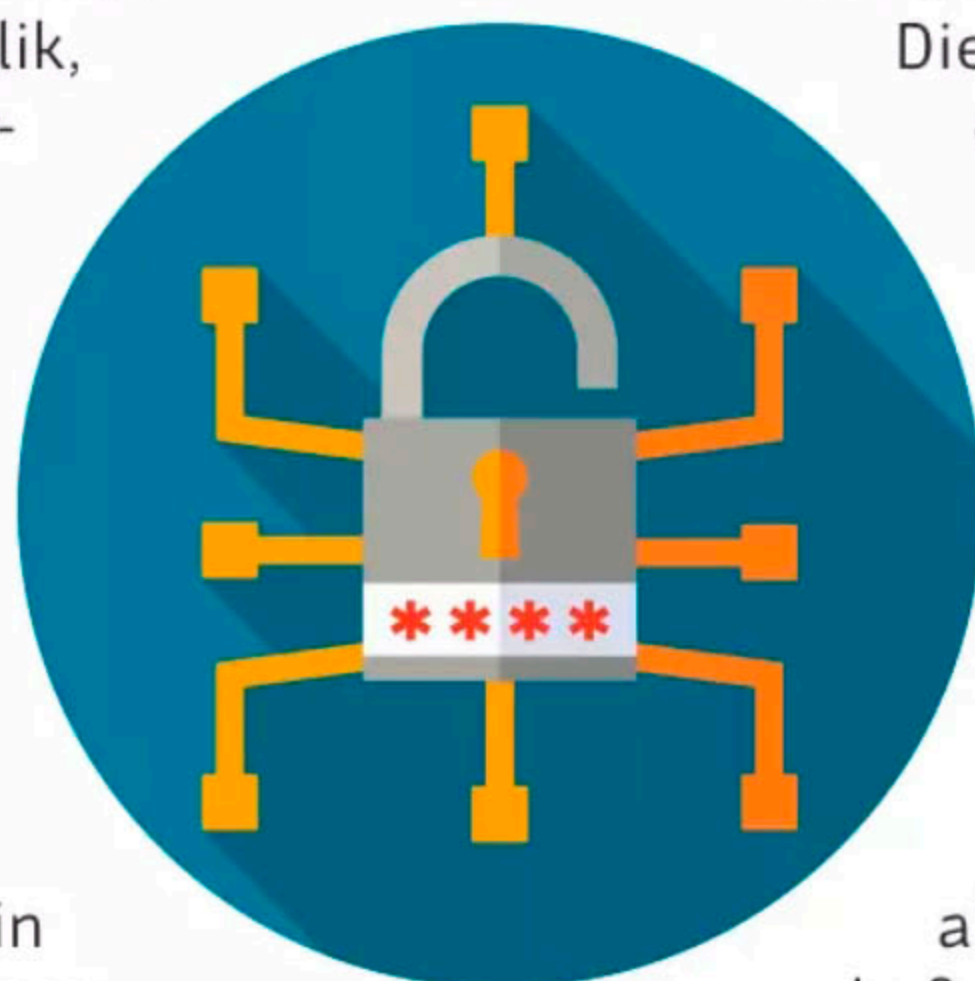


tenlose Spiele von Drittanbietern. Nach einer Entscheidung des Kammergerichts Berlin (Az. 5 U 155/14) waren die bereitgestellten Informationen allerdings nicht geeignet, die User ausreichend zu informieren oder eine freiwillige Einwilligung in die Weitergabe ihrer personenbezogenen Daten einzuholen.

Heftige Sicherheitsanforderungen

Neben diesen umfangreichen rechtlichen Vorgaben für die Nutzung von Krankendaten sieht die DSGVO auch noch weitere Anforderungen im Bereich der IT-Sicherheit vor (siehe auch Seite 124). Dabei gilt grundsätzlich, dass personenbezogene Daten in einer Weise verarbeitet werden müssen, „die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet“. Zentrale Vorschrift ist der Art. 32 der DSGVO. Danach muss der Verarbeiter der Daten geeignete technische und organisatorische Maßnahmen ergreifen, um ein „dem Risiko angemessenes Schutzniveau zu gewährleisten“. Wichtig dabei: Bei dem zu beurteilenden Risiko handelt es sich um die Gefahren, die für die Rechte und Freiheiten der betroffenen Person bestehen – nicht etwa für das verarbeitende Unternehmen. Um ein angemessenes technisches Schutzniveau zu erreichen, ist dabei insbesondere der Stand der Technik zu berücksichtigen, aber auch die Schwere des bestehenden Risikos.

Verarbeitet man Gesundheitsdaten, so entsteht daraus in den allermeisten Fällen ein potenziell hohes Risiko für den Betroffenen. Werden solche Informationen publik, können durch deren Nutzung erhebliche Nachteile entstehen. Hieraus ergibt sich, dass die Anforderungen an die IT-Sicherheit auch entsprechend hoch sein müssen. So dürfen diese Informationen im Normalfall nicht unverschlüsselt gespeichert werden, schon gar nicht offen in der Cloud. Auch die Weitergabe der Daten an Dritte ist in vielen Fällen kritisch und nur eingeschränkt möglich. Dies gilt umso mehr, wenn diese Dritten außerhalb der EU sitzen, etwa in den USA.



Teurer Schadenersatz

Verstöße gegen die DSGVO werden von den zuständigen Landesdatenschutzbehörden sanktioniert. Nachdem mittlerweile auch in Deutschland Millionenbußgelder verhängt wurden (siehe Seite 62), ist kaum damit zu rechnen, dass die Behörden hier speziell bei einem Verstoß hinsichtlich Patientendaten Milde walten lassen.

Hinzu kommt noch das Damoklesschwert des drohenden Schadensersatzes nach Art. 82 DSGVO. Danach hat jede Person, der wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf

Schadenersatz gegen den Verantwortlichen (siehe Seite 72). Ein solcher immaterieller Schaden kann zum Beispiel dann anzunehmen sein, wenn im Rahmen des Betriebs einer App die Gesundheitsdaten von Betroffenen offen im Netz auftauchen. Besonders bedrohlich für die Unternehmen ist dabei die Tatsache, dass jeder Einzelne der Betroffenen einen solchen Anspruch hat. Auch wenn das Gericht einen solchen Schaden nur mit 1000 Euro pro Person bemisst, kann der Schaden bei einer Vielzahl von Betroffenen schnell existenziell bedrohlich werden.

Fazit

Der europäische Gesetzgeber hat mit der DSGVO sehr hohe Hürden für den Umgang mit den höchst sensiblen Gesundheitsdaten aufgestellt. Diese für neue Geschäftsmodelle oder eben auch die medizinische Forschung zu nutzen, ist daher schwierig. Vor allem gilt das für Erfassung, Speicherung und Weitergabe im Rahmen von privatwirtschaftlicher Nutzung, besonders bei Apps und entsprechenden Websites. Hier bleibt den Betreibern meist nur, eine informierte Einwilligung der Betroffenen einzuholen. Wird dabei nicht alles richtig gemacht, so drohen Geldbußen und Schadensersatzansprüche durch die Betroffenen. Es steht zu befürchten, dass man in der Zukunft häufiger von solchen Bußgeldern im medizinischen Bereich hören wird. (anm) **ct**

>> Continuous Lifecycle >> [Container Conf]

Die Konferenzen für Continuous Delivery, DevOps, Containerisierung und Cloud Native

So bilden Sie sich in den nächsten Monaten fort:

- >>> 10. Februar 2021: Cloud-Native Day
- >>>>> 3. März 2021: Dev(Sec)Ops Day



Online-Workshops vertiefen die Deep-Dive-Themen weiter:

5. Februar 2021:
Monitoring innerhalb von Kubernetes

22. Februar 2021:
Evolutionäre Continuous Delivery

Tickets ab sofort verfügbar! Sämtliche Thementage und Workshops sind individuell buchbar – für Paket- und Kombitickets gelten attraktive Rabatte.

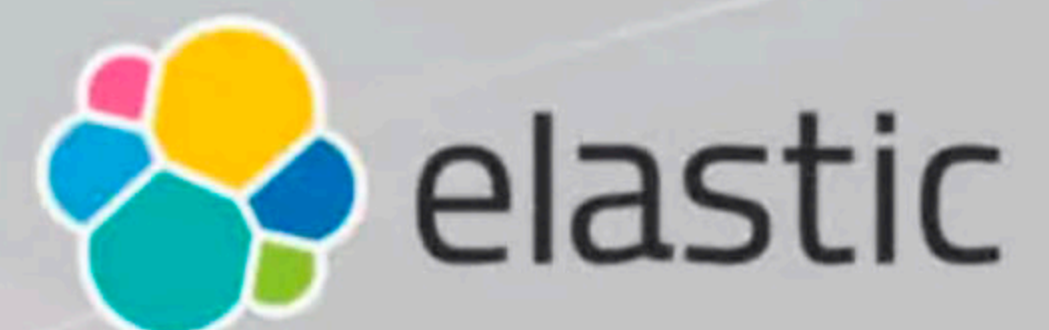
www.continuouslifecycle.de

www.containerconf.de

Platinsponsor



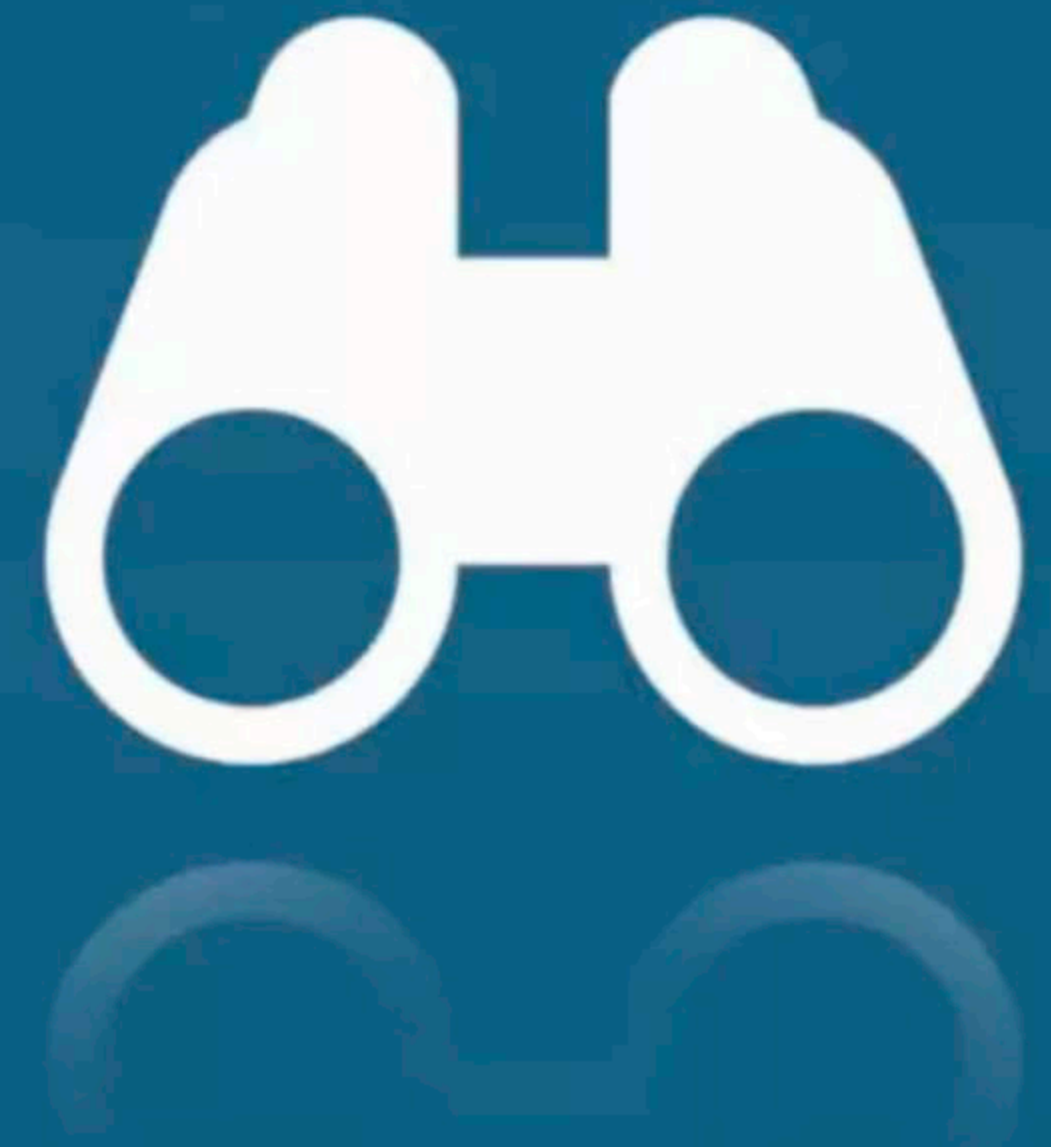
Goldsponsor



heise Developer

dpunkt.verlag

Mitarbeiter- überwachung



Der gläserne Mitarbeiter – eine verführerische Vorstellung für manchen Arbeitgeber. Digitale Workflows geben Unternehmen vielfache Überwachungsoptionen in die Hand. Dazu gehört auch manches, was die Grenzen des rechtlich Erlaubten überschreitet.

Von Joerg Heidrich

Der Fall machte Schlagzeilen: Ausspähung und Datenmissbrauch am Arbeitsplatz in großem Stil. Betroffen waren mehrere hundert Beschäftigte beim deutschen Kundencenter des schwedischen Bekleidungsunternehmens Hennes & Mauritz (H&M) in Nürnberg. Ihre Vorgesetzten überwachten sie bis in privateste Lebensumstände hinein; die Ergebnisse dieser Überwachung wurden dauerhaft gespeichert. Dabei wurden auch Krankheitssymptome und Diagnosen erfasst. Ebenso sammelte man umfassende Informationen über das Privatleben der Mitarbeitenden, was auch religiöse Bekenntnisse und sogar familiäre Probleme betraf.

Die so erhobenen Daten dienten nicht nur einer akribischen Auswertung der individuellen Arbeitsleistung, sondern auch dazu, ein Profil der Beschäftigten für Maßnahmen und Entscheidungen im Arbeitsverhältnis zu erhalten. Die digital gespeicherten Erkenntnisse waren für bis zu 50 Führungskräfte im ganzen Haus einsehbar.

Über 35 Millionen Euro Bußgeld

Ironischerweise wurde das Ganze dadurch bekannt, dass erfasste Daten infolge eines Konfigurationsfehlers im Oktober 2019 für einige Stunden unternehmensweit zugänglich waren. Diese Totalüberwachung brachte H&M 2020 nicht nur den „Big Brother Award“ in der Kategorie Arbeitswelt ein – für „jahrelange, hinterhältige und rechtswidrige Verarbeitung von Beschäftigtendaten“ (siehe [ct.de/wh2z](https://www.ct.de/wh2z), [1]). Für das Unternehmen, das mit dem Slogan „Wir glauben an den Menschen“ wirbt, wurde es auch richtig teuer. Denn Anfang Oktober dieses Jahres ver-

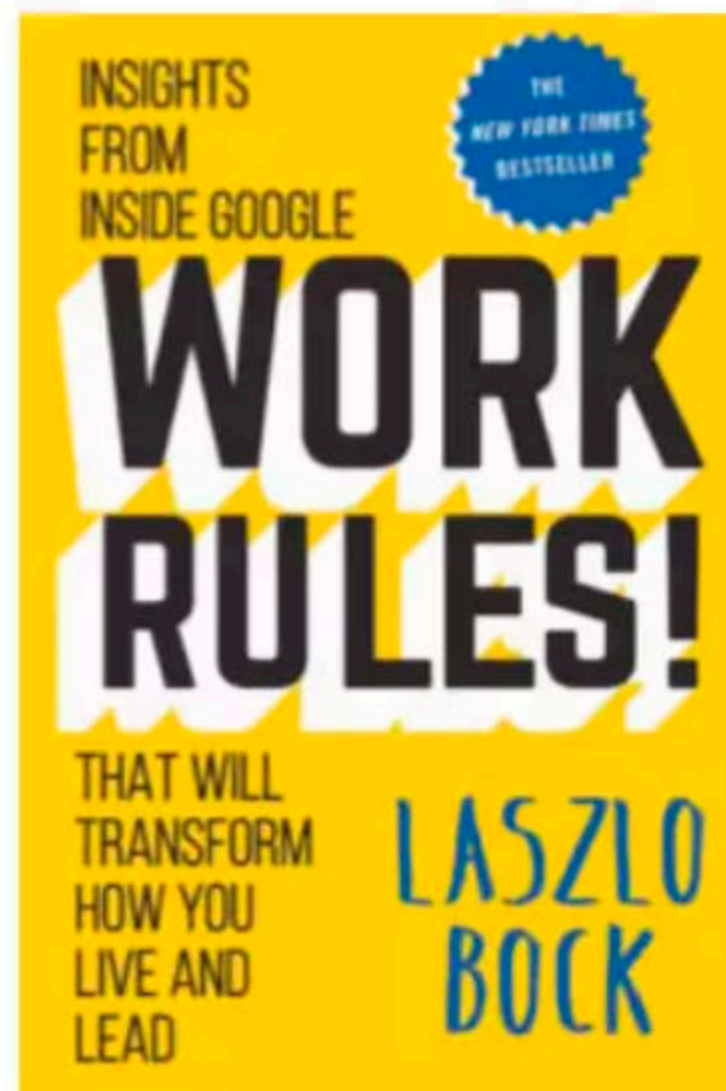
hängte der Hamburgische Beauftragte für Datenschutz Johannes Caspar ein Bußgeld in Höhe von 35.258.707,95 Euro – die höchste bislang in Deutschland für Datenschutzverstöße geforderte Summe (siehe auch Seite 62). Caspar zufolge dokumentiert der Fall „eine schwere Missachtung des Beschäftigtendatenschutzes“ (siehe [ct.de/wh2z](https://www.ct.de/wh2z), [2]). H&M hat das Bußgeld inzwischen akzeptiert, was wohl auch damit zu tun hat, dass man so schnell wie möglich aus den Negativschlagzeilen kommen wollte.

Der Fall ist spektakulär, zugleich wirft er aber ein Schlaglicht auf die Lage des Datenschutzes für Mitarbeiter von Unternehmen – und auf die gelebte Praxis. Hier stehen Interessen einander gegenüber, die bisweilen nur schwer in Einklang zu bringen sind. Es lässt sich nachvollziehen, dass ein Arbeitgeber etwa die Arbeitsleistung von Beschäftigten, die im Homeoffice arbeiten, in irgendeiner Form kontrollieren will. Unter bestimmten Aspekten ist er dazu sogar rechtlich verpflichtet – etwa aus Gründen von Compliance und IT-Sicherheit, zum Verhindern von Datenverlusten und zum Eindämmen von Betrugsmöglichkeiten.

Verführerische Technik

Die technischen Optionen, die der Markt bietet, ermöglichen eine Überwachung in geradezu orwellischem Ausmaß. Das Spektrum der Möglichkeiten reicht von trackbaren Wearables über genetische Tests für Mitarbeiter, Monitoring von Tastatur- und Netzaktivität am Computer bis hin zu People-Analytics-Methoden. Das Schlagwort „People Analytics“ steht für ein zunehmend populäres Instrumentarium im Personalwesen, das eigentlich in den Zusammen-

Den Stein des „People Analytics“-Trends hat Laszlo Bock, der ehemalige Chef der „People Operations“ bei Google, 2015 mit seinem Buch „Work Rules!“ ins Rollen gebracht.



hang von Recruitment und Talentfindung gehört: Eine möglichst große Menge intern und extern erhobener Daten über Personen, etwa auch aus sozialen Netzwerken, wird zu umfassenden Profilen verknüpft.

Noch weiter gehen Projekte im Bereich Social Physics: Hierbei werden zum Beispiel Informationen über

das Verhalten von Probanden wie die Dauer von Gesprächen, Stimmlage, Gestik, Sprech- und Zuhöranteil oder die körperliche Position gesammelt. Auf Basis dieser Daten sollen Erfolgsfaktoren der Zusammenarbeit in Teams abgebildet und prognostiziert werden.

Grenzen der Überwachung

Den schier grenzenlosen Überwachungskonzepten, die vor allem dem US-amerikanischen und asiatischen Raum entstammen, stehen in Europa Grundrechte und Datenschutz der Beschäftigten gegenüber. Speziell in Deutschland ist dieser Schutz stark ausgeprägt.

Einerseits hat ein Arbeitgeber grundsätzlich das Recht, die Arbeit seiner Beschäftigten zu überwachen. Nur wenn er die Betriebsabläufe kennt, kann er von seinem Weisungsrecht sinnvoll Gebrauch machen und sein Unternehmen erfolgreich führen. Außerdem muss er in der Lage sein, Verstöße gegen rechtliche Vorgaben zu erkennen und zu sanktionieren.

Andererseits hat dieses Kontrollrecht Grenzen: Eine dauerhafte Überwachung ist grundsätzlich verboten und greift in geschützte Grundrechte der Beschäftigten ein. Weitere Grenzen setzen die Vorschriften des Datenschutzes. Der erlaubt die Erhebung und Verarbeitung von persönlichen Daten der Mitarbeiter nur dann, wenn hierfür eine ausdrückliche rechtliche Erlaubnis besteht. Neben den allgemeinen Rechtsgrundlagen der europäischen Datenschutz-Grundverordnung (DSGVO) ist dabei vor allem Paragraph 26 des neuen Bundesdatenschutzgesetzes (BDSG) maßgeblich.

Dieser regelt die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses. Danach dürfen personenbezogene Informationen im Rahmen eines

Arbeitsverhältnisses dann verarbeitet werden, wenn dies „für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung“ erforderlich ist. Ebenfalls erlaubt ist das Festlegen von Rechten und Pflichten im Rahmen von Kollektivvereinbarungen wie Betriebs- oder Dienstvereinbarung.

Fast freiwillige Zustimmung

Die Speicherung persönlicher Daten von Mitarbeitern ist auch dann zulässig, wenn die Betroffenen individuell eingewilligt haben. Dazu müssen sie vorab detailliert über das geplante Vorhaben informiert worden sein. Der Weg über die Einwilligung hat für den Arbeitgeber allerdings den Nachteil, dass es für jeden Beschäftigten die Möglichkeit geben muss, jederzeit die gegebene Zustimmung zu widerrufen. Das kann ganze Projekte gefährden.

Allerdings herrscht im Arbeitsverhältnis potenziell ein besonderer Druck, einem Vorhaben des Arbeitgebers zuzustimmen, etwa wenn es um die Überwachung der Internetnutzung geht. Diesen indirekten Zwang hat auch der Gesetzgeber gesehen. Daher wirft § 26 BDSG ein scharfes Auge auf die Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis: Bei deren Beurteilung sind die bestehende Abhängigkeit der beschäftigten Person und die Umstände zu berücksichtigen, unter denen sie die Einwilligung erteilt hat.

Freiwilligkeit kann insbesondere dann vorliegen, wenn „für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen“. Das dürfte bei einer durch Druck erzeugten Einwilligung von Beschäftigten zu deren Überwachung eben gerade nicht gegeben sein.

Darüber hinaus hat bei der Einführung von Hard- und Software zur Überwachung in einem Unternehmen auch der Betriebsrat ein Wort mitzureden, sofern es ihn denn gibt. Paragraph 87 des Betriebsverfassungsgesetzes (BVerfG) erfordert eine Mitbestimmung dieses Gremiums bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“.

Online am Arbeitsplatz

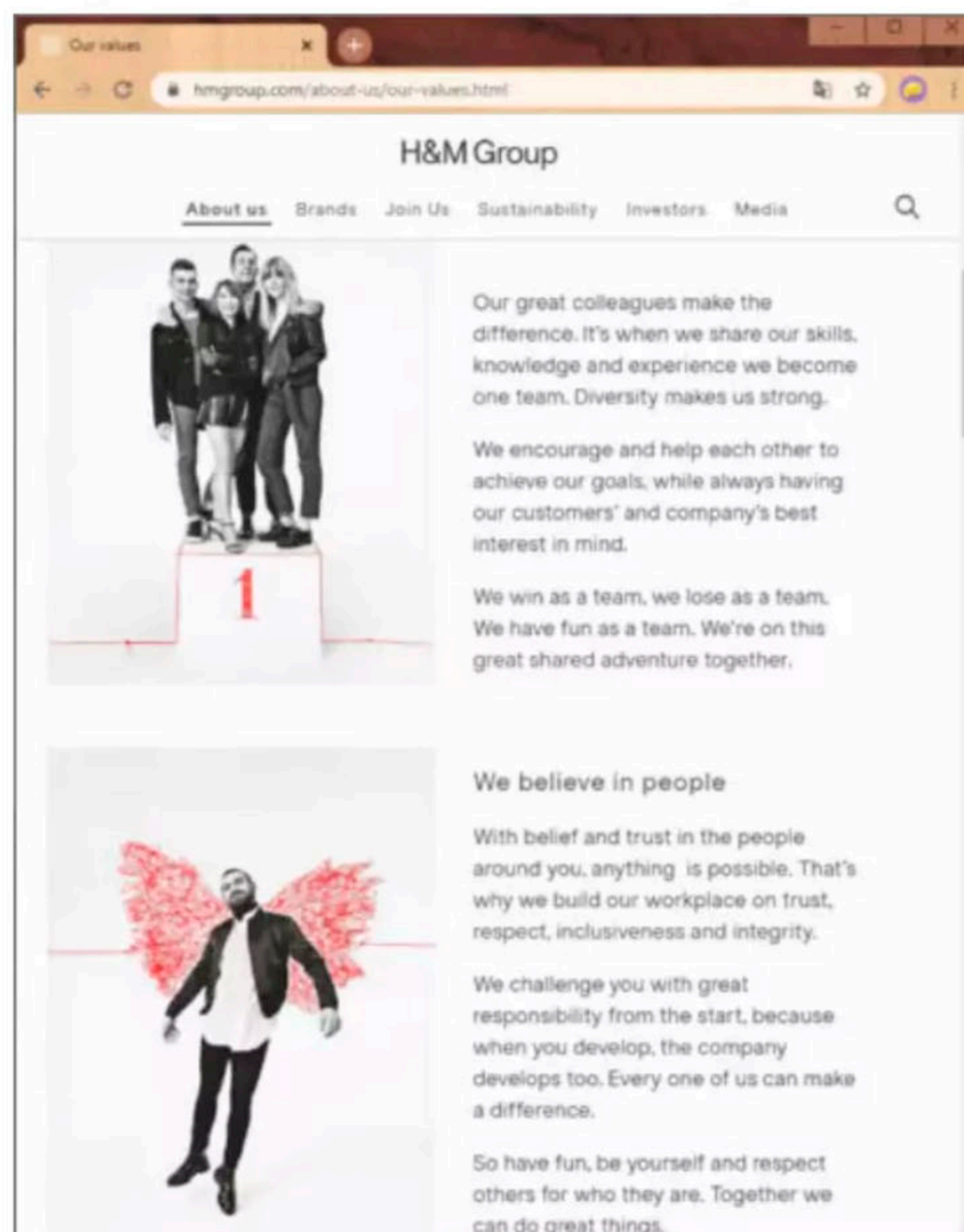
Ein typischer Bereich, den all das berührt, ist die Regulierung der Web-, Chat- und E-Mail-Nutzung am

Arbeitsplatz. Hier treffen nicht nur unterschiedliche Interessen aufeinander, sondern auch mehrerlei Vorschriften, deren Umsetzung sich nur schwer unter einen Hut bringen lässt. So muss ein Arbeitgeber einerseits alle eingegangenen betriebsbezogenen E-Mails aus steuerlichen Gründen archivieren. Andererseits muss er dafür sorgen, dass sich in diesem Archiv keine privaten Nachrichten befinden. Weiterhin muss er für umfassende IT-Sicherheit sorgen, zu der naturgemäß auch eine Protokollierung etwa bei Firewalls gehört. Dem steht aber das legitime Interesse jedes Beschäftigten daran gegenüber, dass sein persönliches Arbeitsverhalten nicht anlass- und lückenlos überwacht wird.

Was dem Chef dabei an Einblick erlaubt oder verboten ist, hängt in erster Linie davon ab, ob das Unternehmen die private Nutzung von E-Mail und Web am Arbeitsplatz gestattet oder untersagt. Private Mails und andere Online-Kommunikation darf der Arbeitgeber normalerweise nicht inhaltlich kontrollieren oder auswerten. Ausnahmen gibt es, wenn etwa der Verdacht einer Straftat besteht, oder in Notfällen wie etwa bei einem akuten Angriff auf die IT-Infrastruktur.

Wenn die Privatnutzung untersagt ist, kann das Unternehmen davon ausgehen, dass alle versandten Mails ebenso wie alle Webseitenabrufe dienstlich verursacht sind. In diesem Fall ist eine Überwachung der Aktivitäten von Mitarbeitern zumindest stichprobenartig erlaubt, ebenso wie Vorgesetzte auch dienstliche Briefe und andere Arbeitsergebnisse überprüfen dürfen.

Das gilt grundsätzlich auch für den Zugriff auf Chatprotokolle. Allerdings kommt es wie so oft auf die konkreten Umstände des Einzelfalls an. 2016 legte ein rumänischer Vertriebsingenieur beim Europäischen Gerichtshof für Menschenrechte (EGMR) Beschwerde gegen Entscheidungen von Gerichten seines Heimatlands ein, bei denen er erfolglos gegen die Kündigung durch seinen Arbeitgeber geklagt hatte. Er hatte den dienstlich für Kundenkontakte eingerichteten Yahoo-Messenger auch privat genutzt. Als Beleg bekam er einen 45-seitigen Ausdruck von Chats mit seinem Bruder und seiner Verlobten vorgelegt. Er wehrte sich gegen die Auswertung seiner Nachrichten: Das Vorgehen seines Arbeitgebers verletze sein Recht auf Achtung des Privat- und Familienlebens aus Artikel 8 der Europäischen Menschenrechtskonvention (EMRK). Eine „kleine Kammer“ des EGMR ließ ihn 2016 zunächst abblitzen: Es sei eindeutig untersagt gewesen, auf dem Dienstrechner privat zu chatten oder zu mailen.



Im Web betont das schwedische Unternehmen H&M die Wertschätzung seiner Mitarbeiter. Die rechtswidrige Überwachung beim Nürnberger Kundenzentrum will nicht recht dazu passen.

Daher habe der Arbeitgeber auch kontrollieren dürfen, ob das Verbot eingehalten wurde. Das sei im Verhältnis auch angemessen, da die private Nutzung des Unternehmensnetzes „kein Menschenrecht“ sei.

Allerdings wurde die Sache auf Antrag des Mannes an die 17-köpfige „große Kammer“ des EGMR verwiesen (siehe [ct.de/wh2z](https://www.ct.de/wh2z), [3]). Diese entschied 2017 doch noch zu seinen Gunsten und nannte eine Reihe von Kriterien, die ausschlaggebend dafür sein können, ob die Überwachung der Kommunikation von Beschäftigten durch den Arbeitgeber noch als verhältnismäßig durchgeht oder nicht. Die rumänischen Gerichte hätten nicht geprüft, ob der Vertriebsingenieur wirklich hinreichend vorab über Möglichkeit, Art und Ausmaß von Kontrollen informiert worden war. Sie hätten auch nicht geklärt, ob ein legitimer Grund für die Kontrollmaßnahmen vorlag und ob nicht mildere Überwachungsmethoden ausgereicht hätten. Auch hätten sie die Schwere des Rechtseingriffs nicht geprüft und die Konsequenzen der Überwachung nicht berücksichtigt, nämlich die Kündigung. Es geht also ganz zentral darum, ob der Grundsatz der Verhältnismäßigkeit gewahrt bleibt.

Regelungen unerlässlich

Um eine saubere Lösung zu gestalten und zugleich Rechtssicherheit für alle Beteiligten zu schaffen,

empfiehlt es sich in jedem Unternehmen, den Umgang mit der digitalen Kommunikation genau zu regeln. Spätestens bei einem unharmonisch verlaufenden Ausscheiden eines Mitarbeiters kann es zu Ärger darüber kommen. Außerdem ist es wichtig, dass alle mit der IT-Administration befassten Personen genau wissen, was sie dürfen und was sie lassen sollten.

In einer Betriebsvereinbarung oder per Dienstweisung ist etwa zu regeln, was beim Ausscheiden eines Mitarbeiters oder bei längerer Abwesenheit mit seinen nicht abgerufenen Mails passiert. Außerdem gilt es festzulegen, wer in welchen Fällen auf Mails zugreifen darf und wie dieses Verfahren durchzuführen ist – sinnvollerweise nach dem Vier-Augen-Prinzip. Nicht erst seit Beginn der Coronakrise empfiehlt es sich auch, den Umgang mit der IT im Homeoffice und beim Umgang mit eigenen Geräten zu regeln.

Ein völliges Verbot privater Onlinenutzung am Arbeitsplatz passt nicht mehr unbedingt in die Zeit, wenn man mal von Hochsicherheitsbereichen wie bei Banken absieht. Einer von vielen gangbaren Wegen besteht etwa darin, zwar die Nutzung der Unternehmens-IT zu untersagen, gleichzeitig aber eine zeitlich eingeschränkte private Onlinenutzung mit dem eigenen Smartphone zu erlauben.

IT-Sicherheit vs. Privatsphäre

Die DSGVO kennt insbesondere in Artikel 32 strenge Anforderungen an die IT-Sicherheit. Dafür können auch Maßnahmen erforderlich sein, die die Rechte von Mitarbeitern betreffen – etwa im Bereich Protokollierung, Backups oder Archivierung. Gerade solche Informationen eignen sich grundsätzlich für eine detaillierte Auswertung des Verhaltens von Beschäftigten. Dem hier drohenden Konflikt können Unternehmen durch eine strenge Zweckbindung begegnen, was die Nutzung der Informationen betrifft. So lässt sich beispielsweise in einer Betriebsvereinbarung festschreiben, dass Logfiles zwingend nur aus Gründen der IT-Sicherheit ausgewertet werden können und keinesfalls für die Überwachung von Mitarbeitern.

Rechtlich unproblematisch ist die Auswertung solcher Daten, die sich nicht auf einzelne Mitarbeiter herunterbrechen lassen. Dazu gehört etwa die nicht personenbezogene Überwachung von Traffic, eine eingeschränkte Protokollierung zur Erhaltung der Systemsicherheit, eine Filterung von URLs oder das automatisierte Scannen von E-Mails und Attachments auf Malware.

Elektronische Augen

Besonders problematisch ist der Einsatz von Videokameras am Arbeitsplatz. Ob dergleichen überhaupt zulässig ist, hängt von Art und Einsatzzeit der verwendeten Videotechnik ebenso ab wie vom beobachteten Raum. Grundsätzlich ist § 26 BDSG zu beachten: Beschäftigtendaten dürfen nur dann erhoben werden, wenn es für das Arbeitsverhältnis notwendig ist. Zu den personenbezogenen Daten, um die es dabei geht, gehören auch Bilder und Filme von Mitarbeitern.

Unter diesen Gesichtspunkten ist eine Überwachung dann erlaubt, wenn sich im gefilmten Bereich besondere Gefährdungen ergeben – etwa durch Maschinen und verwendete Substanzen oder aus dem Risiko von Straftaten wie bei Tankstellen und Banken. Sollen zum Beispiel die Kassen eines Kreditinstituts beobachtet werden, darf sich der Blick der Kameras nach Ansicht der Datenschutzbehörden ausdrücklich nicht auf die Beschäftigten richten.

In einem solchen Fall würden die Betroffenen nämlich „ununterbrochen an ihren Arbeitsplätzen überwacht werden, was ein besonders tief greifender Eingriff in ihre Grundrechte und Grundfreiheiten wäre“. Erlaubt ist dagegen die Aufzeichnung beispielsweise in Eingangsbereichen oder bei Tanksäulen, an denen sich Personen nur kurzfristig aufhalten. Zusätzlich sind die Beschäftigten bei einer beabsichtigten Aufzeichnung von ihrem Arbeitgeber darüber zu unterrichten und Aushänge müssen auf die Überwachung hinweisen (siehe auch Seite 82).

§ 26 BDSG regelt auch, wann Aufzeichnungen am Arbeitsplatz zur Aufdeckung von Straftaten genutzt werden dürfen: nämlich nur, wenn „tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat“.

Nicht folgenlos

Wenn ein Arbeitgeber im Hinblick auf den Mitarbeiterdatenschutz Fehler macht oder die gesetzlichen Vorgaben gar vorsätzlich ignoriert, kann das teuer werden. So erstritt eine Mitarbeiterin eines Unternehmens im Oktober 2010 einen Schadenersatz in Höhe von 7000 Euro. Sie war mit einer Kamera überwacht worden, was nach Ansicht des hessischen Landesarbeitsgerichts eine „schwerwiegende und hartnäckige Verletzung des informationellen Selbstbestimmungsrechts“ darstellte (siehe [ct.de/wh2z](https://www.ct.de/wh2z), [4], [5]). Seit Einführung der DSGVO würden die

Datenschutzbehörden einem solchen Unternehmen sehr wahrscheinlich zusätzlich ein Bußgeld aufbrummen, möglicherweise würden Betroffene heute auch einen Anspruch auf ein weit höheres Schmerzensgeld durchsetzen können (siehe [ct.de/wh2z](https://www.ct.de/wh2z), [6]).

Ein absolutes Tabu ist das zusätzliche Aufzeichnen von Tonspuren bei einer Videoüberwachung. Damit kann man gegen Paragraph 201 des Strafgesetzbuchs (StGB) verstoßen, der die Vertraulichkeit des Wortes schützt. Wer unbefugt „das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt“ oder eine so hergestellte Aufnahme einem Dritten zugänglich macht, muss mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe rechnen. Soweit Unternehmen Audioaufnahmen etwa zur Qualitätskontrolle bei Telefonaten durchführen wollen, ist es zwingend erforderlich, dass der Mitarbeiter und der Gesprächspartner der Aufnahme ausdrücklich zugestimmt haben.

Auch der Einsatz von Keyloggern ist ein probates Mittel, sich strafbar zu machen: Tastatureingaben von Beschäftigten ohne deren Einwilligung zu erfassen, kann allenfalls im Einzelfall erlaubt sein, wenn der konkrete Verdacht einer Straftat oder schwerer arbeitsvertraglicher Pflichtverletzungen besteht.

Sag mir, wo

Nicht nur viele Speditionen kontrollieren den Standort ihrer fahrenden Belegschaft über GPS. Eine sol-

che Ortung wird genutzt, um Dienstfahrzeuge und Außendienstmitarbeiter besser zu koordinieren und ihren Einsatz zu optimieren. Damit wächst allerdings die Gefahr, dass die Technik zur anlasslosen Verhaltens- und Leistungskontrolle von Beschäftigten eingesetzt wird. Grundsätzlich unzulässig ist es, auf diese Art Bewegungsprofile zu erstellen sowie eine durchgängige Pausen- und Leistungsüberwachung vorzunehmen.

Nur wenn ein berechtigtes Interesse an einer Überwachung via Satellit vorliegt, ist diese zulässig. Das dürfte eindeutig für Bereiche wie Geld- oder Gefahrguttransporte gelten, aber auch für Lieferdienste, etwa Paket- oder Essensboten. Allerdings darf sich die Auswertung zwingend nur auf die Arbeitszeiten beschränken. Wenn zum Beispiel ein getrackter Geschäftswagen auch privat genutzt werden darf, muss der Arbeitgeber eine Lösung finden, um zwischen privaten und dienstlichen Fahrten zu unterscheiden.

Sag mir, wann

Die Erfassung der Arbeitszeit birgt ebenfalls einiges an Konfliktpotenzial. Es gibt viele Zeiterfassungssysteme, die auf sehr unterschiedlichen technischen Wegen ein Ein- und Ausloggen an speziellen Stationen oder direkt am Arbeitsrechner verwalten. Auch hierbei gibt es rechtliche Grenzen. Die Kontrolle der Arbeitszeit ist grundsätzlich zulässig und arbeitsrechtlich sogar geboten. Der Eingriff in Grundrechte

§ 26 BDSG: Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder ... für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

(2) Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.



Das Microsoft 365 Admin Center bietet im Bereich „Reports“ neuerdings umfangreiche Auswertungen in Bezug auf den „Productivity Score“ des Unternehmens. Die Angaben reichen bis hinab zum Verhalten der einzelnen Mitarbeiter.

der Beschäftigten muss aber auch hier verhältnismäßig sein. So hat das Landesarbeitsgericht (LAG) Berlin-Brandenburg im Juni 2020 den Einsatz eines fingerabdruckgestützten Systems in einer Radiologiepraxis abgelehnt: In dem konkreten Fall sei es nicht erforderlich gewesen, biometrische Daten zu verarbeiten. Diese sind besonders geschützt (siehe [ct.de/wh2z](https://www.ct.de/wh2z), [7], [8]).

Überwachung im Homeoffice

Auch eine Überwachung von Mitarbeitern im Homeoffice ist nur eingeschränkt zulässig. Vor allem der Einsatz der hemmungslosen Tools von Anbietern aus Übersee, die eine Dauerbespitzelung von Beschäftigten durchführen und Elemente wie Keylogging, Screen-Captures oder Mikrofonaufzeichnungen verwenden, ist hierzulande grundsätzlich nicht erlaubt. Eine Überwachung am heimischen Arbeitsplatz greift potenziell auch noch in die Privatsphäre der Beschäftigten ein. Insoweit dürfte eine umfassende Überwachung dort nicht einmal mit Einwilligung der Betroffenen statthaft sein.

Erlaubt sind Maßnahmen, die die IT-Sicherheit in der Unternehmensinfrastruktur gewährleisten – etwa zum Schutz vor Malware, zur Beschränkung von Zugängen oder zur Abwendung von Betrübereien. Und auch im Homeoffice unterliegt ein Arbeitnehmer rechtmäßig der Arbeitszeitüberwachung.

Kritisch sind allerdings gerade im Hinblick aufs Homeoffice ausufernde Monitoring-Systeme US-

amerikanischer Machart. Sie überwachen ganze Unternehmen oder Abteilungen detailliert, wobei sie bis auf die Ebene einzelner Mitarbeiter hinab laufend Aktivitäten erfassen und speichern. Das betrifft etwa Microsofts Konzept des Productivity Score, das der Hersteller vor Kurzem ins Admin Center des Anwendungs- und Cloud-Komplexes Microsoft 365 integriert hat (siehe [ct.de/wh2z](https://www.ct.de/wh2z), [9]).

Sobald sich die Aufzeichnungen solcher Systeme auf die Aktivitäten einzelner Mitarbeiter herunterbrechen lassen, ist deren Einsatz hierzulande allenfalls mit Zustimmung der Betroffenen oder einer entsprechenden Betriebs- beziehungsweise Dienstvereinbarung erlaubt.

Komplette Selbstvermessung

Manche Softwareangebote setzen auf digitale Selbstoptimierung von Mitarbeitern speziell im Homeoffice. So soll Microsofts „MyAnalytics“ Nutzern helfen zu verstehen, „wie sie ihre begrenzte Zeit verbringen und mit wem sie sie verbringen“. Das System präsentiert dann auf Abruf „intelligente Tipps, wie Sie intelligenter arbeiten können“. Dafür verarbeitet MyAnalytics Daten aus vielerlei Quellen, wertet Mail- und Kalenderdaten sowie Chat- und Anrufsignale aus und beobachtet die Nutzung von Teams, Skype und Windows 10.

Auf dieser Basis entsteht eine komplette Selbstvermessung des Mitarbeiters. Microsoft zufolge ist das Ergebnis nur für den jeweiligen Nutzer selbst sichtbar – und potenziell auch für den Softwarekonzern. Solange solche Angebote mit qualifizierter Einwilligung durch die Verwender arbeiten, die Bestimmungen der DSGVO eingehalten werden und ein Zugriff von Arbeitgeberseite vollständig ausgeschlossen ist, lässt sich rechtlich nichts dagegen sagen. Allerdings muss ein solches Angebot zwingend so gestaltet sein, dass der Nutzer es selbst ausdrücklich aktiviert. Es darf nicht standardmäßig aktiv sein.

Kein Paradies für Spähfreudige

Die strengen arbeits- und datenschutzrechtlichen Vorgaben stehen hierzulande einer tiefgreifenden Überwachung von Mitarbeitern im Büro und im Homeoffice entgegen. Erlaubt sind notwendige Aufzeichnungen und Auswertungen von Daten zu betrieblichen Zwecken und zur Gewährleistung der IT-Sicherheit. Und Gerichte haben gezeigt, wie wichtig es im Einzelfall ist, den Grundsatz der Verhältnismäßigkeit zu wahren.

(anm) **ct**

Quellen und weiterführende Informationen

[ct.de/wh2z](https://www.ct.de/wh2z)



Datenschutz und Corona

2020 hatte die Corona-Pandemie das Land fest im Griff! Viele Unternehmen mussten nicht nur ihre Arbeitsabläufe digitalisieren, sondern auch Mitarbeiter quasi über Nacht ins Homeoffice schicken. Doch was ist mit dem Datenschutz? Wie muss ein Homeoffice-Arbeitsplatz datenschutzkonform gestaltet sein? Und was ist bei Videokonferenzen zu beachten?

Von Brian Scheuch

Seitdem die Pandemie grassiert und Kontaktbeschränkungen eher die Regel als die Ausnahme sind, arbeiten viel mehr Mitarbeiter als zuvor im Homeoffice und setzen dabei die unterschiedlichsten Videokonferenz- und Chatlösungen ein. Viele Unternehmen vergessen dabei jedoch gerne, dass das Bereitstellen einer Videokonferenzlösung durch einen externen Dienstleister eine klassische Auftragsverarbeitung ist. Hier werden personenbezogene Daten – Namen, IP-Adressen, Bild und Ton – der Mitarbeiter und Kunden verarbeitet.

Mit diesen Dienstleistern ist in jedem Falle eine Vereinbarung zur Auftragsverarbeitung zu schließen (siehe Seite 56). Fraglich ist jedoch, ob die jeweiligen Vereinbarungen zur Auftragsverarbeitung in jedem Fall auch standhalten. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hatte im Juli 2020 ein Ampelsystem für Video-Konferenz-Lösungen

herausgebracht und etwaige Mängel bezüglich der Auftragsverarbeitung herausgearbeitet. In der Liste der Berliner Aufsichtsbehörde sind damals nach diesem Ampelsystem beispielsweise die Anbieter Blizz, Google Meet, Microsoft Teams, Skype und Zoom durchgefallen (siehe ct.de/wkr2).

Der überwiegende Teil der Anbieter hat aber bereits nachgebessert, sodass man nicht mehr davon ausgehen kann, dass das Ampelsystem der Berliner Aufsichtsbehörde noch aktuell ist, und selbst prüfen muss, ob die genutzte Lösung den Datenschutzanforderungen entspricht.

Aufzeichnungen ohne Einwilligung sind tabu

Erschwerend kommt hinzu: Viele der eingesetzten Tools sind technisch sehr einfach in der Lage, Meetings

aufzuzeichnen – zum Beispiel zur Arbeitskontrolle, zur Nacharbeit oder um Besprechungen anderen Mitarbeitern zugänglich zu machen, die abwesend waren. Hier ist jedoch Vorsicht geboten! Eine Aufzeichnung und Speicherung eines Meetings bedarf zwingend der Einwilligung sämtlicher am Meeting teilnehmenden Personen. Ohne sie wäre eine Aufzeichnung rechtswidrig und dürfte einen Datenschutzverstoß darstellen, der Bußgelder und Schadensersatzansprüche nach sich ziehen kann. Solche grundsätzlichen Datenschutzregeln gelten natürlich auch dann, wenn die Videokonferenzlösung vom Unternehmen selbst gehostet wird (siehe Seite 92).

Wer auf Nummer sicher gehen will, sollte Aufzeichnungen tunlichst unterlassen und unter Umständen eine entsprechende Regelung in den internen IT-Richtlinien mit aufnehmen. Das Arbeitsgericht Schwerin (ArbG Schwerin, Urteil vom 26.06.2015 - 3 Ca 1362/14) verurteilte bereits einen Arbeitgeber, der Mitarbeiterfotos ohne Einwilligung auf die Website gestellt hatte, zu einem Schadensersatz von 750 Euro.

Auf den Standort kommt es an

Weitere wichtige Fragen, die es zu klären gilt, sind: In welchen Ländern hat der Diensteanbieter seinen Sitz und wo betreibt er seine Server?

Sehr beliebt ist beispielsweise das Videokonferenz-Tool „Zoom“: Seine Bedienung ist einfach, die Performance gut und das Angebot verhältnismäßig günstig, teilweise sogar kostenlos. Jedoch wies Zoom in der Vergangenheit Sicherheitslücken auf, die es Dritten ermöglichte, unerlaubt an Meetings teilzunehmen. Außerdem wurde in verschiedenen Artikeln berichtet, dass eine Datenweitergabe an Facebook stattgefunden haben soll. Zoom reagierte auf diese Vorwürfe und gab mittlerweile bekannt, die Datenweitergabe gestoppt und die Sicherheitslücken geschlossen zu haben.

Ein großes Problem bereitet jedoch nach wie vor der Wegfall des Privacy-Shield-Abkommens (siehe Seite 108 ff.), denn auch bei Zoom handelt es sich um ein Unternehmen mit Sitz in den USA. Auch wenn deutsche Nutzer nach Angaben von Zoom ausschließlich über Server innerhalb Europas kommunizieren und das Unternehmen über EU-Standardvertragsklauseln verfügt, bleibt nach derzeitiger

Auffassung offen, ob dies ausreichend ist. Es fehlt bislang an einer eindeutigen Positionierung der Aufsichtsbehörden insgesamt.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat in seinem Ampelsystem jedoch nahezu alle Tools mit Sitz in den USA als kritisch eingestuft. Das Problem besteht hierbei im CLOUD Act (Clarifying Lawful Overseas Use of Data Act). Amerikanische Unternehmen wären nach diesem Gesetz verpflichtet, US-Behörden den Zugriff auf gespeicherte Daten auch dann zu gewähren, wenn die Speicherung außerhalb der USA, also beispielsweise auf einem innerhalb der EU betriebenen Server erfolgt.

Dies gilt auch für die Microsoft-Lösungen Skype und Teams.

Microsoft steht noch immer im Visier der Aufsichtsbehörden. Eine eindeutige Positionierung fehlt aber auch hier, da die Aufsichtsbehörden in ihren bisherigen Entschei-

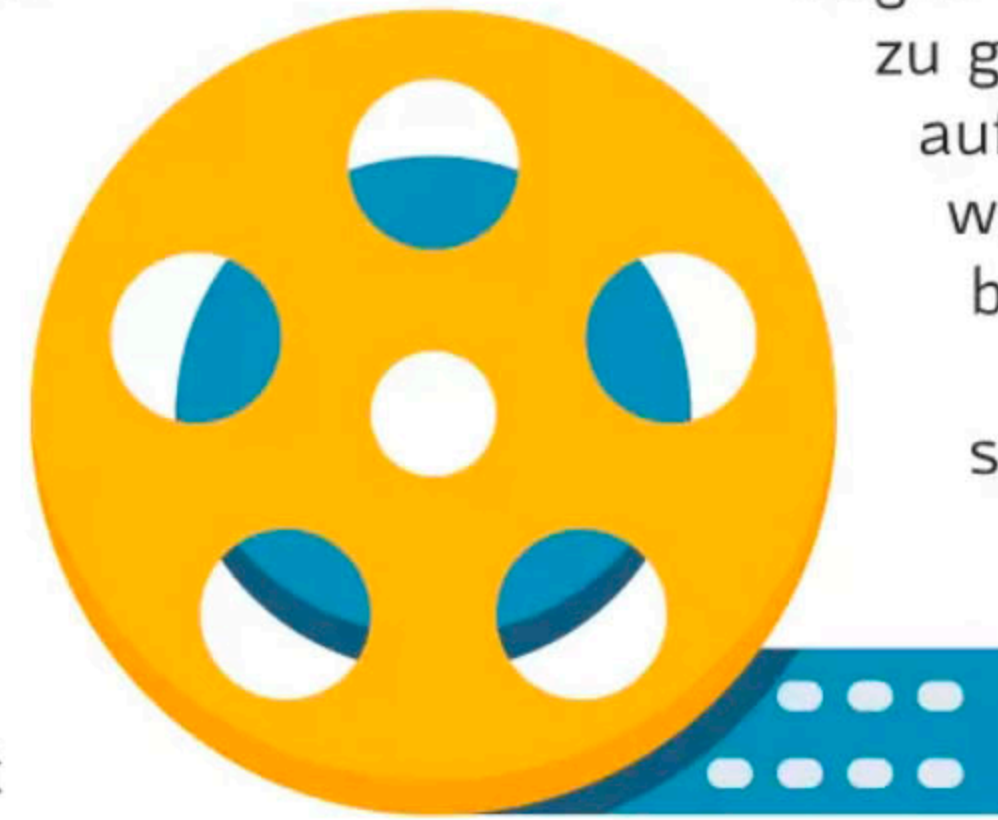
dungen oft veraltete Daten- und Nutzungsbedingungen von Microsoft zugrunde gelegt haben.

Fazit: Befindet ein Anbieter sich in einem Drittstaat, also außerhalb der EU, sollte sehr genau geprüft werden, ob die Übermittlung zulässig ist. In jedem Fall müssten EU-Standardvertragsklauseln mit dem Anbieter vereinbart werden, wobei auch hier geprüft werden muss, ob diese wirksam sind (siehe Seite 108 ff).

Wer auf Nummer sicher gehen möchte, sollte einen Anbieter mit Firmen- und Serversitz innerhalb der europäischen Union wählen. Aufgrund des einheitlichen Datenschutzstandards innerhalb der EU ist dies die aus Datenschutzsicht risikoärmste Variante. Sofern die notwendigen Mittel und Ressourcen zur Verfügung stehen, kann es aus Datenschutzsicht auch eine gute Möglichkeit sein, selbst eine Videokonferenz-Lösung auf den eigenen Servern zu hosten.

Datenschutzeinstellung der jeweiligen Tools beachten

Bei der Wahl des Anbieters spielt auch eine wichtige Rolle, welche technischen Schutzmaßnahmen das Videokonferenzsystem anbietet. Je nachdem, für welches Tool man sich entscheidet, hat man unterschiedliche Einstellungsmöglichkeiten für den Datenschutz. Sehr wichtig ist, dass die Verbindun-



Ampel-Kriterien des Berliner Datenschutzbeauftragten

Für seine Überprüfung, ob Video-Konferenz-Lösungen datenschutzkonform nutzbar sind, entwickelte der Berliner Beauftragte für Datenschutz und Informationsfreiheit ein Ampelsystem (siehe [ct.de/wkr2](https://www.ct.de/wkr2)), anhand dessen die Behörde die untersuchten Anbieter eingestuft hat:

„Grün markiert sind Anbieter, bei denen wir bei unserer Kurzprüfung keine Mängel gefunden haben.

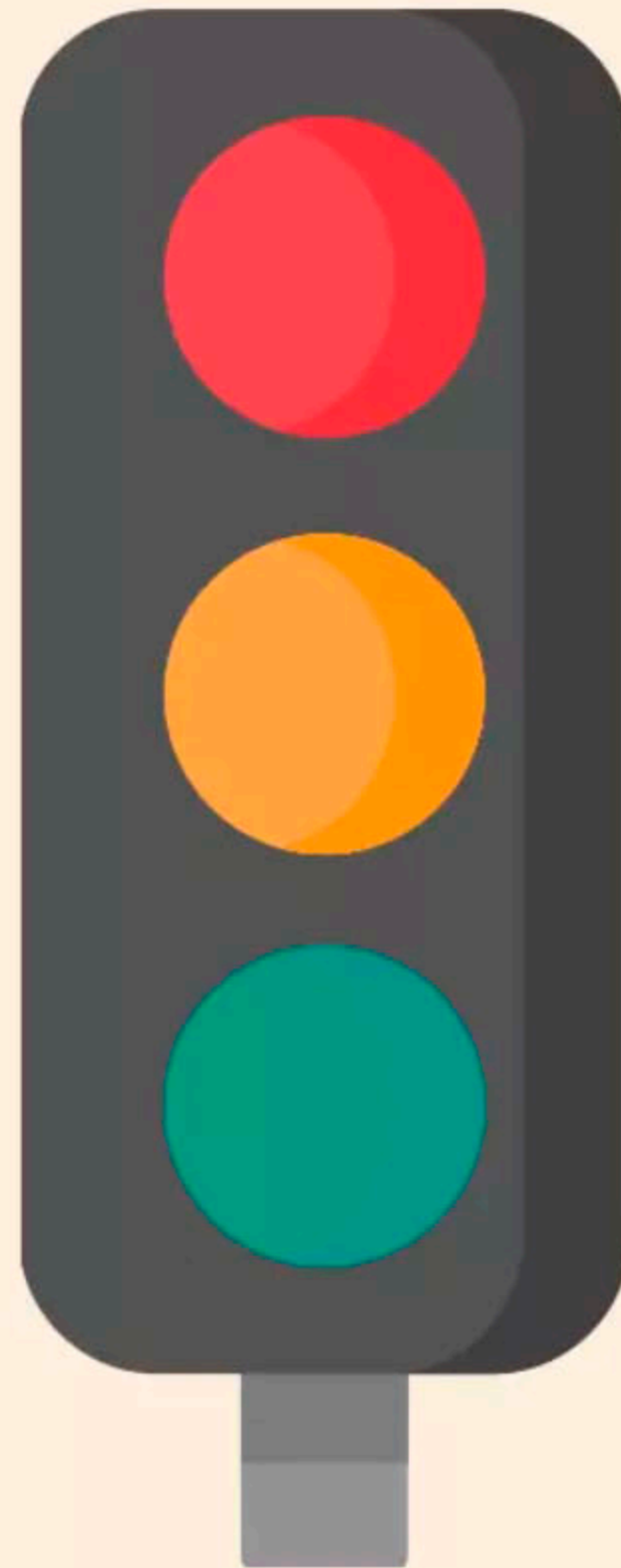
In der rechtlichen Prüfung gelb markiert sind Anbieter, bei denen wir Mängel gefunden haben, die eine rechtskonforme Nutzung des Dienstes zwar ausschließen, deren Beseitigung allerdings vermutlich ohne wesentliche Anpassungen der Geschäftsabläufe und der Technik möglich ist. In der technischen Prüfung bedeutet eine gelbe Markierung, dass die Anbieter derzeit (nur) unter Beachtung bestimmter Rahmenbedingungen nutzbar sind.

Rot markiert sind Anbieter, bei denen Mängel vorliegen, die eine rechtskonforme Nutzung des Dienstes aus-

schließen und deren Beseitigung vermutlich wesentliche Anpassungen der Geschäftsabläufe und / oder der Technik erfordern, etwa wenn nach dem Vertrag die Anbieter Auftragsdaten auch zu eigenen Zwecken verarbeiten, der Vertrag Datenlöschungen nur verspätet

oder eingeschränkt vorsieht oder die Anforderungen an die Einbindung von Subunternehmern derzeit nicht ausreichend ausgestaltet sind und voraussichtlich Änderungen in den Verträgen zwischen Anbietern und Subunternehmern erforderlich sind.“

Auch wenn die Einzelbewertungen der Anbieter möglicherweise nicht mehr in allen Punkten aktuell sind, lassen sich aus der online veröffentlichten Übersicht viele Hinweise ziehen, welche konkreten rechtlichen und technischen Datenschutzprobleme bei der Auswahl eines Anbieters und der Nutzung seines Videokonferenzsystems auftreten können.



gen ausschließlich verschlüsselt stattfinden und der Grundsatz der Datenminimierung beachtet wird, also so wenig personenbezogene Daten wie möglich verarbeitet werden.

Bei fast jedem Video-Konferenztool ist ein Chat inkludiert. Was häufig übersehen wird: die jeweiligen Chatprotokolle. Hier sollte bereits im Vorfeld (siehe Seite 140) festgelegt werden, wann die Protokolle gelöscht werden sollen.

Gelöscht werden muss spätestens dann, wenn die Daten nicht mehr benötigt werden und keine gesetzliche Aufbewahrungsfrist der Löschung entgegensteht (siehe Seite 136). Unternehmensinterne Chats sollten daher automatisiert so schnell wie möglich gelöscht werden, was sich in der Regel beim jeweiligen Anbieter einstellen lässt.

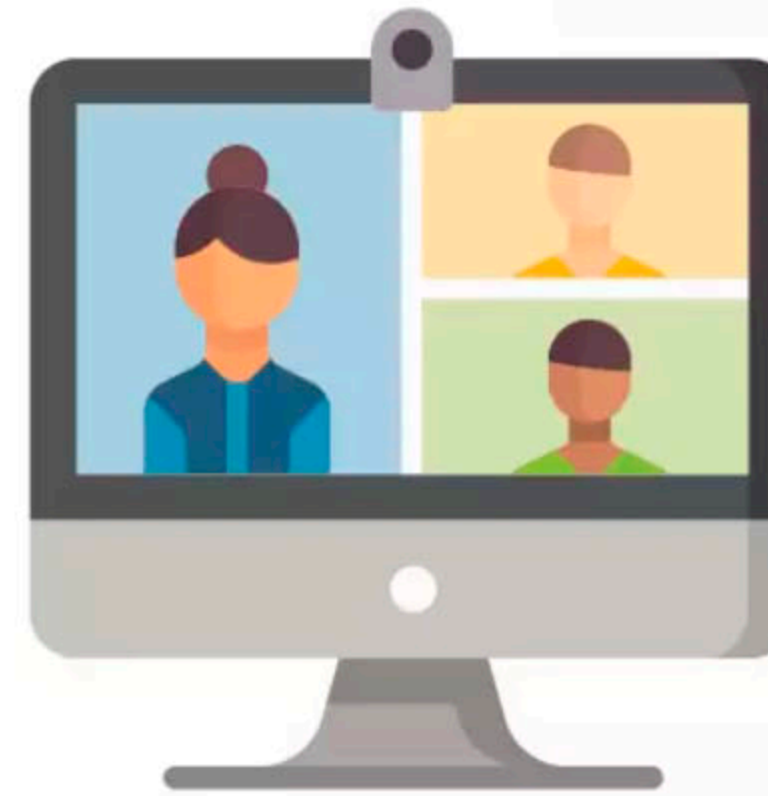
Länger können Speicherfristen beispielsweise sein, wenn im Chat Verträge geschlossen oder ergänzende Vereinbarungen getroffen werden. Bei den gängigen Tools kann der Administrator Aufbewahrungsrichtlinien festlegen für die einzelnen Chats oder Kanalnachrichten. Die Festlegung der Aufbewahrungsfristen sollte die IT zusammen mit dem Datenschutzbeauftragten koordinieren.

Beteiligung des Datenschutzbeauftragten und des Betriebsrates

Um nichts zu übersehen, sollte auf jeden Fall ein Datenschutzbeauftragter involviert werden – auch in die Auswahl der Software vor dem Betrieb des jeweiligen Tools (siehe Seite 74). Zusammen mit ihm

können Mindestvoraussetzungen und die notwendigen Einstellungen erarbeitet werden.

Und sofern im Unternehmen ein Betriebsrat existiert, müsste dieser aller Wahrscheinlichkeit gemäß § 87 Abs. 1 Nr. 6 BetrVG zustimmen. Denn grundsätzlich sind diverse Video- und Chattools geeignet, das Verhalten und die Leistung der Mitarbeiter zu überwachen – zum Beispiel, wenn ein Tool mit grünen, gelben oder roten Ampeln arbeitet, um die Verfügbarkeit eines Mitarbeiters anzuzeigen. Einige Tools ändern automatisch die Anwesenheitsfarbe von grün auf gelb, wenn innerhalb einer bestimmten Zeit keine Interaktion am Computer erfolgt. Mit der „Überwachung“ der Ampelfarben des Mitarbeiters könnten daher theoretisch Rückschlüsse gezogen werden, in welchen Zeiten er Eingaben am PC getätigt hat oder auch nicht.



Die einzelnen Tools neu bewerten

Als es zu Beginn der Pandemie schnell gehen musste, haben die Aufsichtsbehörden möglicherweise in den ersten Monaten noch ein Auge zugeedrückt, wenn datenschutzrechtliche Regelungen nicht sofort beachtet wurden. Davon kann man nun nicht mehr ausgehen. Besondere Probleme dürfte in diesem Zusammenhang der Wegfall des Privacy-Shield-Abkommens bereiten.

Unternehmen sollten daher dringend überprüfen, ob das jeweilige Tool den aktuellen datenschutzrechtlichen Anforderungen genügt.

Auftragsverarbeitungsvereinbarungen sind zwingend nachzuholen. Wer auf Nummer sicher gehen will, sollte sich zudem für Lösungen mit Standorten in Europa entscheiden. (anm) **ct**

Datenschutz im
Homeoffice

ct.de/wkr2



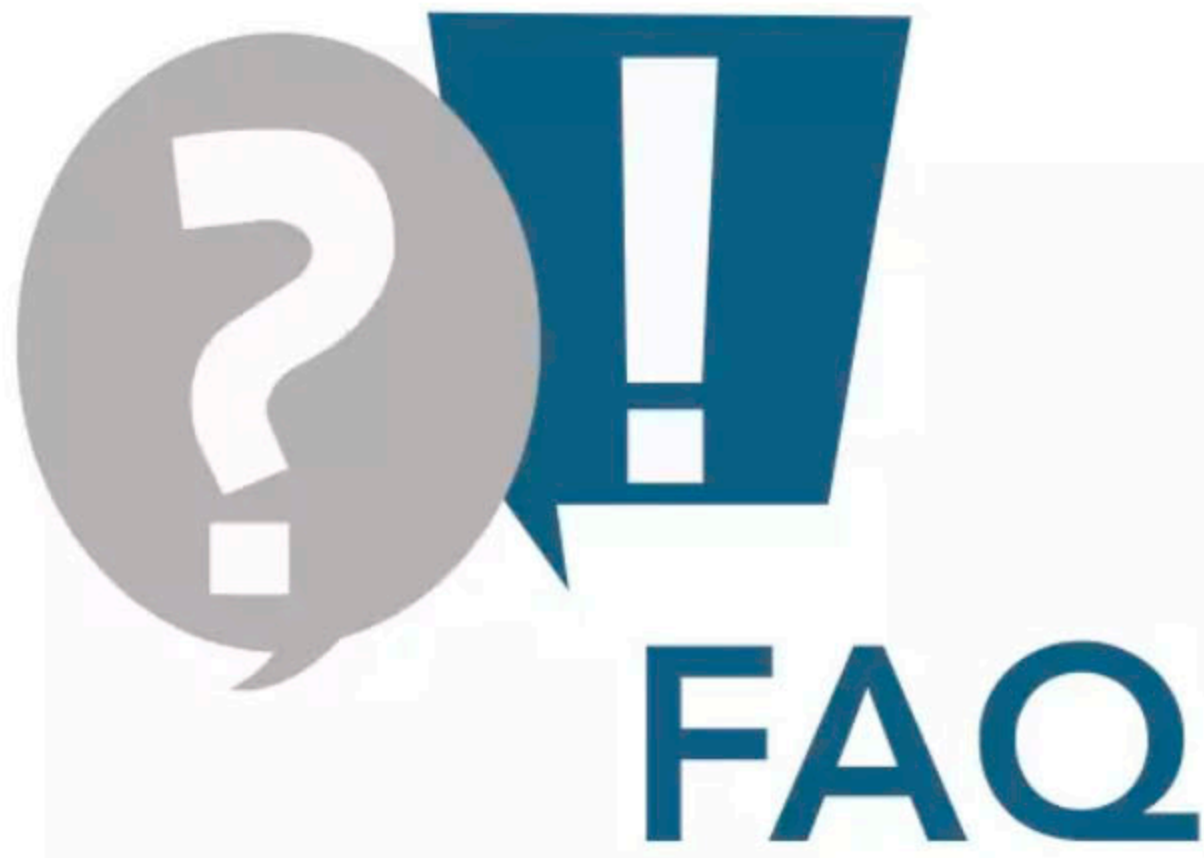
Jetzt im Handel

oder im heise shop:

shop.heise.de/wissenschaft21

180 Seiten
Faszinierende
Fakten und
Bilder

180 Seiten – vollgepackt mit Fakten, Bildern und Illustrationen



Homeoffice & Datenschutz

In vielen Unternehmen ist das Arbeiten im Homeoffice mit der Pandemie von der Ausnahme zur Regel geworden. Dies wirft für etliche Firmen neue datenschutzrechtliche Fragen auf – besonders wenn Familienangehörige zu Hause sind oder die Arbeit über private Hardware erledigt wird (Bring-your-own-Device – BYOD). In jedem Fall muss der Arbeitgeber auch für Mitarbeiter im Homeoffice ausreichende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ergreifen.

Von Brian Scheuch

Verantwortlicher

? Wer ist für die Datenverarbeitung im Homeoffice verantwortlich?

! Datenschutzrechtlicher Verantwortlicher für die Datenverarbeitung bleibt nach wie vor der Arbeitgeber. Daher obliegt es dem Arbeitgeber, sicherzustellen, dass sämtliche Arbeitnehmer entsprechende Anweisungen auch befolgen.

Arbeitgeberpflichten

? Was muss ich als Arbeitgeber unternehmen?

! Um Risiken zu minimieren, sollten Arbeitgeber verbindliche Regelungen für die Arbeit im Homeoffice aufstellen. Nach Ansicht der Aufsichtsbehörde in Niedersachsen sollten sie diese Homeoffice-Vereinbarung individualvertraglich mit jedem Arbeitnehmer schließen. So können Beschäftigte zur Einhaltung spezifischer Schutzmaßnahmen verpflichtet und sensibilisiert werden. Die Aufsichts-

behörde in Niedersachsen vertritt die Auffassung, dass entsprechende Maßnahmen vor dem Beginn des Homeoffice zu ergreifen sind.

Homeoffice-Vereinbarung

? Was sollte eine Homeoffice-Vereinbarung regeln?

! Der genaue Regelungsinhalt hängt stets vom individuellen Einzelfall ab. Generelle Grundsätze wie die **10 Gebote des Homeoffice** im Kasten rechts sollten sich jedoch in allen Vereinbarungen wiederfinden.

Zentrale Administration

? Welche Maßnahmen sind auf technischer Ebene zu beachten?

! Sofern der Arbeitgeber die Endgeräte zur Verfügung stellt, sollten diese zentral administriert werden, ebenso wie die Geräte innerhalb des Be-

Die 10 Gebote des Homeoffice

- 1. Nur notwendige Ausdrücke**
Beschäftigte sollten angewiesen werden, im Homeoffice auf das klassische Ausdrucken von Dokumenten mit personenbezogenen Daten zu verzichten. Denn gerade ausgedruckte Dokumente bergen die Gefahr, dass diese in falsche Hände geraten.
- 2. Datenschutzkonforme Vernichtung von personenbezogenen Daten**
Sofern gedruckte Dokumente anfallen, sollte nochmals auf die datenschutzkonforme Vernichtung hingewiesen werden, insbesondere mit Aktenvernichtungsgeräten. Eine Entsorgung von personenbezogenen Daten im Hausmüll sollte untersagt werden.
- 3. Zugangsbeschränkung der Arbeitsräume und Arbeitsgeräte**
Arbeitnehmer sollten sicherstellen, dass Dritte – dazu gehören insbesondere Familienangehörige oder Mitbewohner – keinen Zugang zu personenbezogenen Daten haben. Daher sollte die Anweisung erfolgen, die Arbeitstätigkeit – sofern möglich – in einem separaten abschließbaren Raum auszuführen, der für Dritte nicht uneingeschränkt zugänglich ist. Das klassische Beispiel wäre hierbei das heimische Arbeitszimmer. Sämtliche Unterlagen sollten in abschließbaren Schränken aufbewahrt werden. Sofern der räumliche Platz eingeschränkt ist, sollten Bildschirme so positioniert werden, dass keine direkte Einsicht möglich ist. Das Sichtfeld kann man beispielsweise mit einer separaten Displayfolie noch weiter einschränken.
- 4. Sperren der Geräte**
Arbeitsgeräte sollten stets – das gilt übrigens auch im normalen Büroalltag – bei Verlassen des Raumes (automatisch) gesperrt beziehungsweise ausgeschaltet werden.
- 5. Sichere Videokonferenzumgebung**
Videokonferenzen sollten über Headsets geführt werden und nicht über Lautsprecher. Dies minimiert das Risiko, dass Dritte unternehmensinterne Gespräche mitbekommen. Zusätzlich sollte die Anweisung erfolgen, sich für Videokonferenzen in einen separaten Raum, abseits der anderen Familienmitglieder zu begeben. Außerdem sollten Fenster und Balkone während der Konferenzen geschlossen sein.
- 6. Verschlüsselte Speicher**
Daten auf Speichermedien, einschließlich PCs und Notebooks, sollten grundsätzlich verschlüsselt werden.
- 7. Trennung von beruflichen und privaten Daten**
Keine Vermischung von geschäftlichen mit privaten Unterlagen: Dies gilt vor allem dann, wenn eigene Endgeräte (BYOD) im Einsatz sind. Betriebliche Daten sollten verschlüsselt und unzugänglich für Dritte gespeichert werden.
- 8. Sicheres Authentifizierungsverfahren**
Die Authentifizierung sollte grundsätzlich mit sicheren/starken Passwörtern beziehungsweise anderen geeigneten Verfahren wie Tokens und Chipkarten stattfinden. Die sichere Passwortvergabe sollte insbesondere auch für das heimische WLAN eingehalten werden.
- 9. Regelmäßige Backups**
Je nachdem wie die heimische IT-Infrastruktur aufgebaut ist, kann es sein, dass keine automatischen Backups durchgeführt werden. Deshalb ist es umso wichtiger, manuelle Datensicherungen zu erstellen. Dafür sollte ein entsprechendes Backup- und Recovery-Konzept für das Homeoffice eingeführt werden.
- 10. Digitale Sprachassistenten sind tabu**
Digitale Sprachassistenten sollten während der Arbeit am heimischen Arbeitsplatz ausgeschaltet sein.

triebes. So kann man beispielsweise USB-Ports für betriebsfremde Geräte sperren. Zugänge zum firmeninternen Netzwerk sollten mittels verschlüsselter Verbindung (zum Beispiel VPN-Netzwerk) hergestellt werden. Auch eine Transportverschlüsselung ist für den Datenaustausch unumgänglich.

Datenpannen

? Was ist bei einer Datenpanne im Homeoffice zu unternehmen?

! Grundsätzlich sollten im Vorfeld Beschäftigte sensibilisiert und geschult werden. Wenn eine Datenpanne im Homeoffice passiert, gelten dieselben Regelungen wie bei einer Datenpanne im Unternehmen (siehe Seite 144).

Private Endgeräte

? Darf ich überhaupt private Endgeräte benutzen?

! Der Arbeitgeber kann nicht ohne weiteres die Nutzung privater Endgeräte für die betriebliche Nutzung verlangen. Eine Nutzung der privaten Endgeräte kommt ausschließlich dann in Betracht, wenn der Beschäftigte einwilligt.

Sowohl Arbeitgeber als auch Arbeitnehmer sollten sich beim Einsatz privater Endgeräte der entsprechenden Risiken bewusst sein. In jedem Fall sollte die IT-Abteilung vor ihrer Nutzung prüfen, ob die jeweiligen Endgeräte ein angemessenes Schutzniveau bieten.

Sensible Personendaten

? Was ist mit sensiblen personenbezogenen Daten?

! Sofern im Homeoffice sensible personenbezogene Daten verarbeitet werden, steigen die Anforderungen an die technischen und organisatorischen Maßnahmen. Der Einsatz privater Endgeräte ist hier tabu. Zudem könnte sich die Frage stellen, ob der Arbeitgeber für die Verarbeitung sensibler personenbezogener Daten im Homeoffice eine Datenschutzfolgenabschätzung durchführen muss (siehe Seite 128). Das wäre immer dann der Fall,

wenn die Verarbeitung ein besonders hohes Risiko für die betroffene Person darstellt.

Keine Ausnahmen

? Was ist zu tun, wenn ein Arbeitnehmer Vorgaben nicht einhalten kann?

! Wenn Arbeitnehmer die Homeoffice-Vorgaben nicht einhalten können – etwa mangels Platz in der eigenen Wohnung –, sollte man Alternativen für sie finden. Da es bislang keine Homeoffice-Pflicht gibt, wäre nach aktuellem Stand anzuraten, diese Mitarbeiter weiterhin im klassischen Büro arbeiten zu lassen, sofern aktuelle Verordnungen nicht dagegen sprechen.

Sanktionen für Arbeitgeber

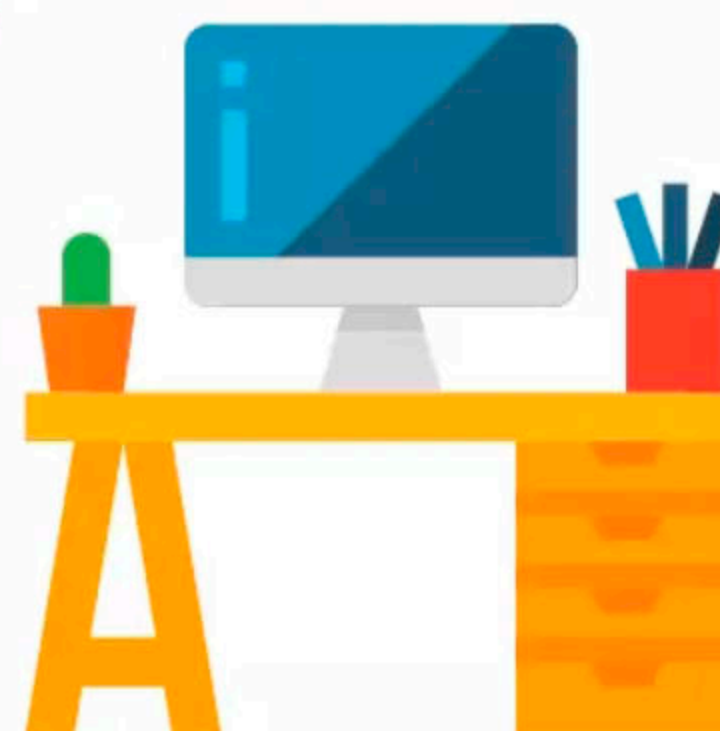
? Was droht mir als Arbeitgeber, wenn ich keine Regeln aufstelle?

! Sofern der Arbeitgeber keinerlei Regelungen aufstellt, können im schlimmsten Fall Bußgelder und Schadensersatzforderungen drohen (siehe Seite 60 ff). Daran ändert selbst eine Sondersituation wie eine Pandemie nichts.

Sanktionen für Arbeitnehmer

? Was droht mir als Arbeitnehmer, wenn ich gegen die Homeoffice-Vereinbarung verstoße?

! Verstöße gegen die Homeoffice-Vereinbarung können im Zweifel arbeitsrechtliche Konsequenzen nach sich ziehen, wenn der Arbeitnehmer sich beharrlich weigert, diese zu befolgen. Aber nicht jede Kleinigkeit dürfte Konsequenzen rechtfertigen, etwa wenn ein Kind einmal in eine Videokonferenz „reinplatzt“. (anm) **ct**



IMMER AUF AUGENHÖHE

2x Mac & i mit 35 % Rabatt testen
und Geschenk sichern!

Mac & i – Das Magazin rund um Apple

- Tipps & Workshops
- Hard- & Softwaretipps
- Apps und Zubehör

Für nur 14,40 € statt 21,80 €



Jetzt bestellen:

www.mac-and-i.de/miniabo

✉ leserservice@heise.de ☎ 0541 80 009 120

Mac & i. Das Apple-Magazin von c't.

Kontrollen am Arbeitsplatz



Der Schutz der Gesundheit ist eine wichtige Arbeitgeberaufgabe, ganz besonders in Pandemiezeiten. Hierzu durchgeführte Gesundheitskontrollen am Arbeitsplatz werfen aber auch datenschutzrechtliche Probleme auf.

Von Brian Scheuch

Viele Unternehmen versuchen verständlicherweise sich und ihre Mitarbeiter vor einer Corona-Infektion zu schützen. Hierzu fragen sie unter anderem spezifische Symptome ab oder führen entsprechende Gesundheitskontrollen am Arbeitsplatz durch. Da es sich gerade bei der Verarbeitung von Gesundheitsdaten um besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 DSGVO handelt, kommt dem Datenschutz hier ein besonders hoher Stellenwert zu. Viele der durch die Pandemie aufgeworfenen praktischen Fragestellungen sind für Unternehmen und Aufsichtsbehörden jedoch neu und damit bisher oft nicht oder nur teilweise geklärt.

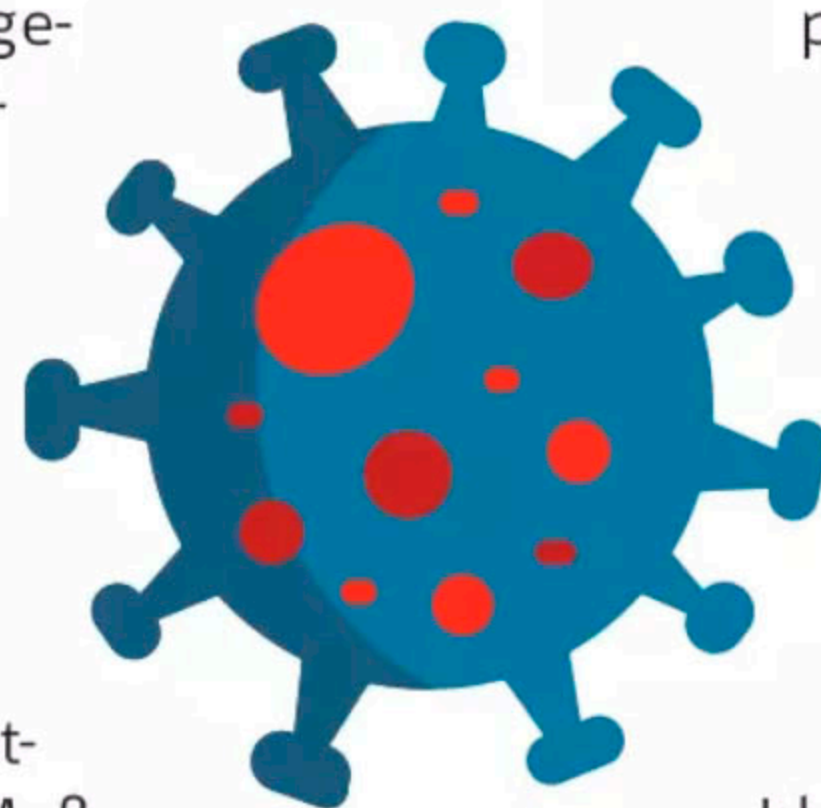
Schutz der Mitarbeiter

Fraglich ist zunächst, ob der Arbeitgeber überhaupt verpflichtet ist, Maßnahmen zum Schutz der Mitarbeiter vor einer Corona-Infektion zu treffen. Der Arbeitgeber hat grundsätzlich eine entsprechende Fürsorgepflicht und ist für die Einhaltung des Arbeitsschutzes verantwortlich. Ergänzt wird der Arbeitsschutz aktuell durch die entsprechenden Corona-Verordnungen.

Arbeitgeber sollten daher ihre Mitarbeiter über das Infektionsrisiko aufklären und geeignete Maß-

nahmen treffen. Dies bedeutet vor allem ein umfangreiches Hygienekonzept zu erstellen und Home-office-Lösungen einzurichten. Wenn die jeweils notwendigen Maßnahmen nicht umsetzbar sind oder getroffene Vorkehrungen nicht greifen, bleibt als Ultima Ratio nur noch eine Betriebsschließung.

Der Arbeitgeber ist verpflichtet, Mitarbeiter, die offensichtliche Symptome einer Infektion aufweisen, zum Schutz der anderen Mitarbeiter unverzüglich nach Hause zu schicken. Er ist auch verpflichtet, zu gewährleisten, dass die Hygieneregeln in seinem Unternehmen umgesetzt werden und die Mitarbeiter diese auch einhalten. Dies geht in der Regel nur mit entsprechenden Kontrollen.



Gesundheitstests am Arbeitsplatz

Etliche Betriebe kamen daher früh auf die Idee, aufgrund steigender Infektionszahlen entsprechende Gesundheitstests am Arbeitsplatz durchzuführen. Konkret geht es beispielsweise um das Fiebermessen vor Beginn der Arbeit am Betriebs-tor. Dies kann entweder manuell erfolgen oder mittels Wärmebildkamera.

Mindestens bei letzterem wird das für den Datenschutz zentrale Persönlichkeitsrecht der betroffenen Personen berührt, denn auch beim Einsatz von Wär-

mebildkameras handelt es sich um die Verarbeitung von personenbezogenen Daten.

Anlassloses Fiebermessen für alle

Misst der Arbeitgeber anlasslos Fieber bei allen Mitarbeitern, beispielsweise mittels Wärmebildkamera, muss er eine Abwägung der betroffenen Rechtsgüter vornehmen. In einem Unternehmen ohne konkrete Infektionen dürfte kaum zu rechtfertigen sein, dass man generell bei allen Mitarbeitern auch ohne Erkrankungssymptome oder andere Rechtfertigungsgründe Fieber misst.

Dies käme allenfalls in Betracht, wenn das Unternehmen von einem Superspreader-Event betroffen ist. In diesem Fall sollte das Unternehmen das weitere Vorgehen aber sowieso mit dem zuständigen Gesundheitsamt abstimmen, das gegebenenfalls eine Betriebsschließung beziehungsweise für den Großteil der Mitarbeiter eine Quarantäne anordnet.

In einer besonderen Situation sind Krankenhäuser und Pflegeeinrichtungen, vor allem, wenn sie ein erhöhtes Infektionsaufkommen hatten. Hier dürften die Rechtsgüter der Patienten und Risikogruppen überwiegen. Gerade bei solchen Einrichtungen kommt auch die Einführung von Corona-Schnelltests vor Arbeitsbeginn oder Besuchen durch Angehörige infrage.

Freiwilliges Fiebermessen

Statt einer Pflicht zum Fiebermessen könnten Arbeitgeber möglicherweise auf die freiwillige Teilnahme der Belegschaft setzen. Hierzu könnte das Unternehmen beispielsweise zwei separate Eingänge vorsehen, wo jedoch nur an einem die entsprechende Kontrolle stattfindet. Es müsste jedoch sicherstellen, dass auch tatsächlich die Freiwilligkeit gewahrt bleibt. So könnten sich Verweigerer dem sozialen Druck ihrer Kollegen ausgesetzt sehen, so dass sie doch lieber den „Testeingang“ verwenden. Problematisch wäre die Freiwilligkeit indes auch, wenn vor Einführung der Maßnahme alle Mitarbeiter um ihre Zustimmung gebeten werden.

Vorlage von negativen Tests oder Impfnachweisen

Ob und wenn ja wann Arbeitgeber einen negativen Testbefund oder einen Impfnachweis verlangen dür-

fen, ist gerichtlich noch nicht geklärt. Das anlasslose Verlangen von Testbefunden dürfte unverhältnismäßig und damit rechtswidrig sein, zumindest bei Betrieben, die nicht im Gesundheitsbereich tätig sind. Eine Ausnahme kann sich ergeben, wenn der Arbeitnehmer mit Symptomen erkrankt war, die einer Covid-19-Erkrankung ähneln und kürzer als vierzehn Tage krankgeschrieben war. Hier dürften die Interessen des Arbeitgebers und der übrigen Beschäftigten überwiegen.

Noch problematischer wäre das Verlangen eines Impfnachweises, da es faktisch einer angeordneten Impfpflicht gleichkäme. Da das Recht auf körperliche Unversehrtheit und die allgemeine Handlungsfreiheit aus Art. 2 Grundgesetz berührt sind, bedürfte diese einer entsprechenden rechtlichen Vorgabe, die es bei Redaktionsschluss nicht gab.

Weitergabe von Gesundheitsdaten an andere Mitarbeiter

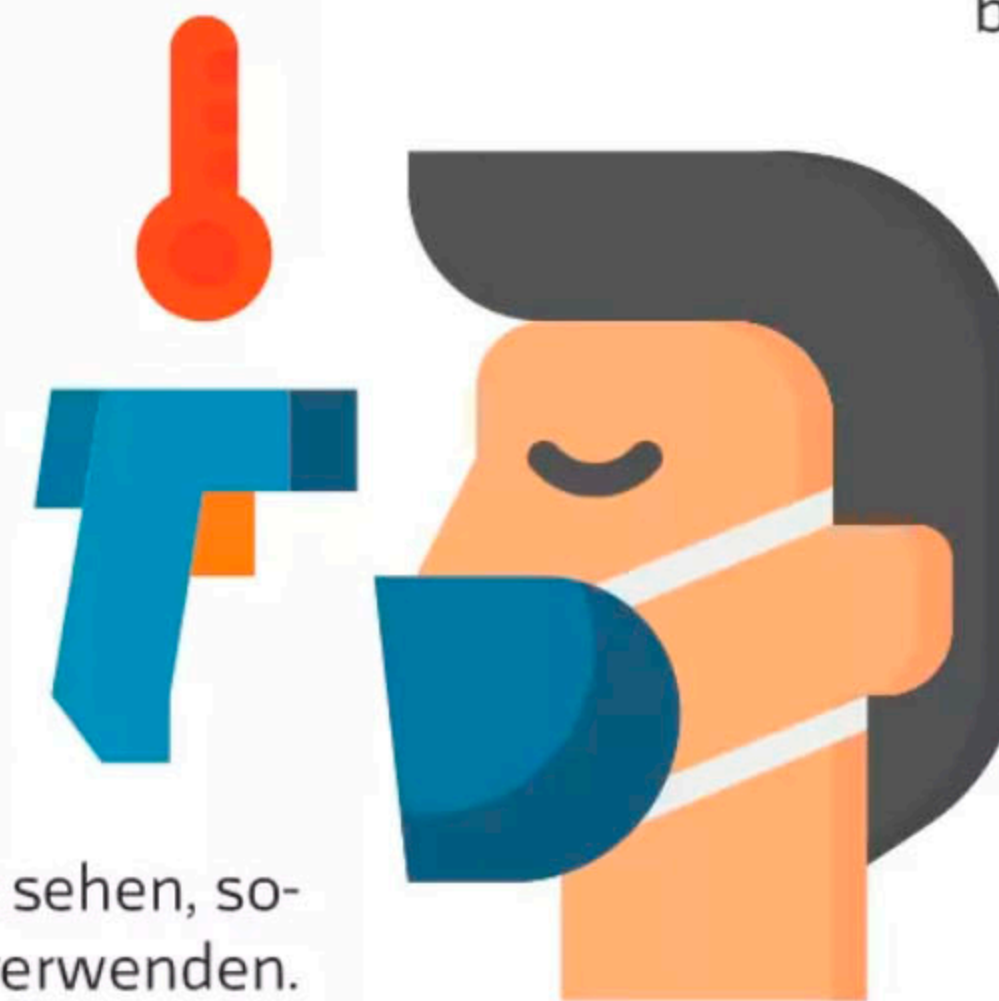
Steht ein Mitarbeiter in Verdacht, sich mit Coronaviren infiziert zu haben, stellt sich die Frage, ob der Arbeitgeber die Mitarbeiter, die Kontakt zu ihm hatten, informieren muss und ob er dies überhaupt darf.

Eine Information an Mitarbeiter, die direkten Kontakt zum Verdachtsfall hatten, könnte datenschutzrechtlich möglicherweise gemäß Art. 6 Abs. 1 lit. d) DSGVO gerechtfertigt sein. Danach wäre die Verarbeitung erlaubt, um lebenswichtige Interessen der

betroffenen Person oder einer anderen natürlichen Person zu schützen. Hierbei sollte jedoch der Grundsatz der Datenminimierung beachtet werden. Eine namentliche Nennung des betroffenen Mitarbeiters oder die Frage an die Mitarbeiter, wer zu ihm Kontakt hatte, sollte nur dann stattfinden, wenn anders nicht sichergestellt werden kann, dass alle Betroffenen erreicht werden. Eine entsprechende

Information an die übrigen Mitarbeiter könnte dann zum Schutz der anderen Interessen gerechtfertigt sein.

Bei einer nachgewiesenen Corona-Infektion werden die Mitarbeiter, die Kontakt zu einem Infizierten hatten, in der Regel von Amts wegen vom Gesundheitsamt informiert. (anm) **ct**





Daten ins Ausland übertragen

In einer internationalisierten Datenwelt spielen Landesgrenzen häufig kaum mehr eine Rolle. Das sieht der Datenschutz allerdings ganz anders. Um die sensiblen Informationen der Bürger jeweils größtmöglich zu schützen, teilt die DSGVO die Welt im Wesentlichen in drei Teile. Besondere Bedeutung hat hierbei der Datenexport in die USA.

Von Joerg Heidrich

Will man Daten in ein anderes Land transferieren, so sieht die DSGVO hierfür eine zweigliedrige Prüfung vor. Zunächst einmal muss die Übermittlung der Daten über die Landesgrenzen als solche zulässig sein. Hierfür gelten die bekannten Rechtsgrundlagen von Art. 6 DSGVO, etwa die Einwilligung, die Erfüllung eines Vertrags oder das berechtigte Interesse. Handelt es sich um besonders sensible Daten, gelten die strengen Voraussetzungen des Art. 9 DSGVO.

Liegt eine der benannten Rechtsgrundlagen vor, so muss in einem weiteren Schritt geprüft werden, ob die Übertragung von Daten in das jeweilige Land

zulässig ist. Dieses ist gerade bei IT-Projekten von großer Bedeutung und stets schon im Planungsstadium zu berücksichtigen. Hierbei wird die Welt in drei verschiedene Bereiche eingeteilt, für die jeweils unterschiedliche Voraussetzungen gelten.

Sichere Datenweitergabe

Rechtlich unproblematisch ist die Weitergabe von persönlichen Informationen innerhalb der EU. In diesem Bereich gilt einheitlich die DSGVO. Diese gilt darüber hinaus auch im Bereich des Europäischen Wirtschaftsraums (EWR), der die vollen Rechte und

Pflichten des EU-Binnenmarkts ausdehnt. Dies bedeutet konkret, dass der europäische Datenschutz auch in den EWR-Staaten Norwegen, Island und Lichtenstein gilt.

Dann gibt es noch eine weitere Kategorie von Ländern, in die ein Transfer uneingeschränkt möglich und erlaubt ist. Das sind die sicheren Drittländer. Sicher sind solche Staaten, denen die Europäische Kommission im Rahmen eines Angemessenheitsbeschlusses ein den europäischen Vorgaben entsprechendes Datenschutzniveau bestätigt hat. Hierzu gehören derzeit: Andorra, Argentinien, Kanada (nur kommerzielle Organisationen), Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay und Japan.

Unsichere Drittstaaten

Alle anderen Länder dieser Welt werden als unsichere Drittstaaten qualifiziert, deren nationales Recht keinen hinreichenden Schutz der Daten europäischer Bürger gewährleistet. Das bedeutet allerdings nicht, dass eine Weitergabe von Informationen in diese Länder grundsätzlich verboten ist. Vielmehr muss der Verantwortliche anderweitig sicherstellen, dass die personenbezogenen Daten im Land des Empfängers ausreichend geschützt werden. Hieraus folgen einige rechtliche Hürden, die vor der ersten Übertragung geklärt werden müssen.

Höchste praktische Bedeutung hatte bei dieser Frage seit jeher der Transfer von Daten über den Atlantik in die USA. Hier gab es lange eine besondere Regelung. Unter den Vorgaben des „Privacy Shield“ konnten sich US-Unternehmen in ein Verzeichnis eintragen und garantierten so, angemessene Datenschutzvorgaben im Sinne der EU einzuhalten. Für Experten wenig



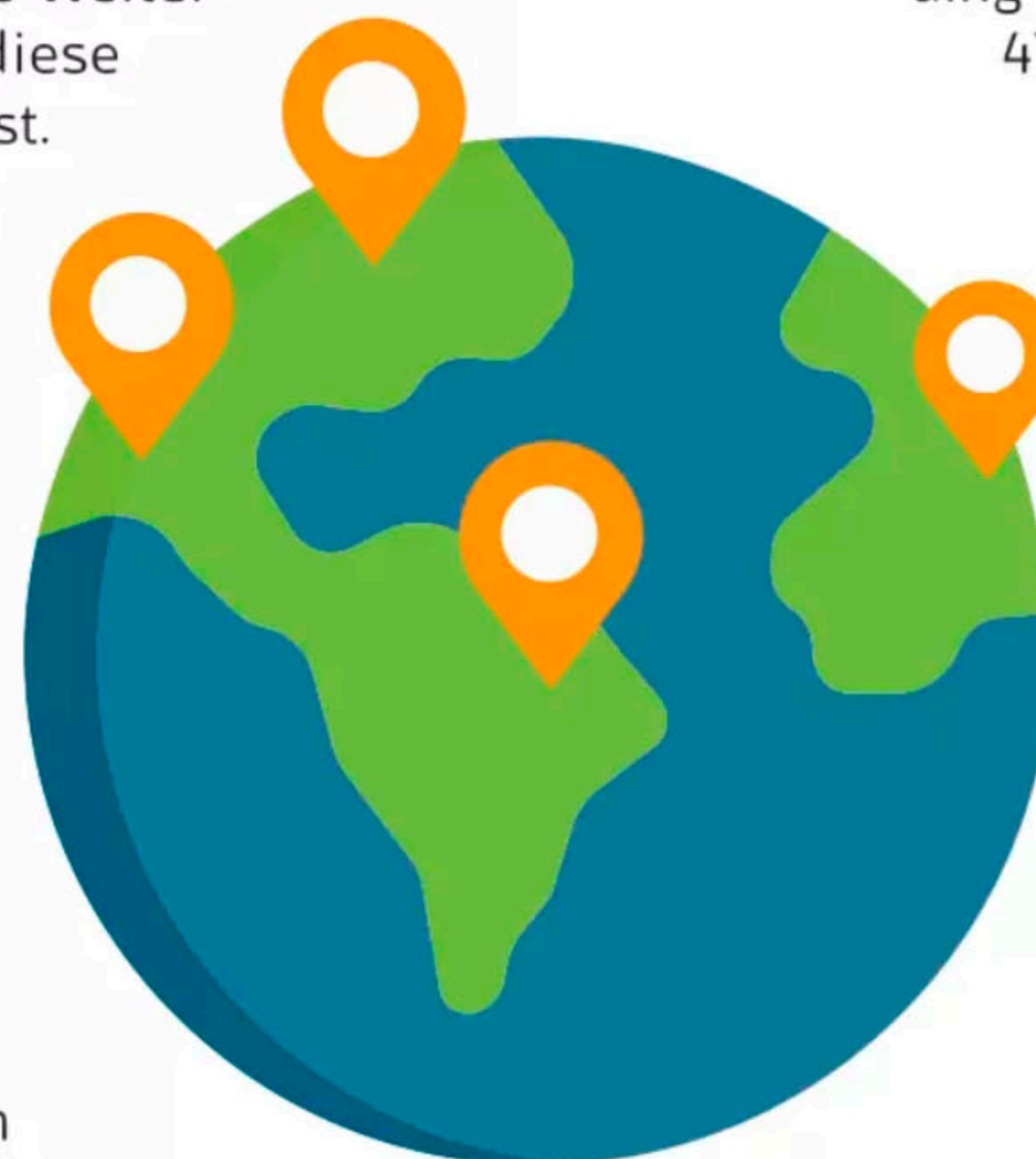
überraschend hat jedoch der Europäische Gerichtshof im Rahmen des Urteils vom 16. Juli 2020 (Az.: C-311/18) diese Regelung für unwirksam erklärt (siehe Seite 112). Über Nacht entfiel so die wichtigste Rechtsgrundlage für den transatlantischen Datentransfer.

Rechtsgrundlagen beim Datenexport in unsichere Staaten

Für die Vereinigten Staaten gelten damit nun die gleichen Regelungen wie für den nichtprivilegierten Rest der Welt, also etwa Indien, Russland oder China. Für solche Staaten gelten die strengen Vorschriften der Art. 44 ff. DSGVO. Praktisch relevant ist hierbei vor allem der Abschluss von Standardvertragsklauseln. Das sind Vertragsvorgaben der EU-Kommission, die im Rahmen von individuellen Vereinbarungen zwischen dem Datenexporteur und dem Empfänger für den Schutz der Daten sorgen sollen. Allerdings ist auch diese Rechtsgrundlage durch das EuGH-Urteil „angeschossen“ und in aller Regel nur noch mit erheblichen zusätzlichen technischen und organisatorischen Schutzmaßnahmen möglich (siehe Seite 116).

Für Konzerne gibt es eine weitere Möglichkeit des Datenaustauschs im Rahmen von „Binding Corporate Rules“ (BCR) nach Art. 47 DSGVO. Diese müssen rechtlich bindend für alle Mitglieder einer Unternehmensgruppe gelten, die eine gemeinsame Wirtschaftstätigkeit ausüben. Zusätzlich müssen den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen werden.

Inhaltlich müssen die Vereinbarungen sämtliche Grundprinzipien und durchsetzbare Rechte enthalten, die geeignete Garantien für die Übermittlungen von personenbezogenen Daten bieten. Die BCR stehen unter einem Genehmigungsvorbehalt durch die zuständige Aufsichtsbehörde des jeweiligen Bundeslands.

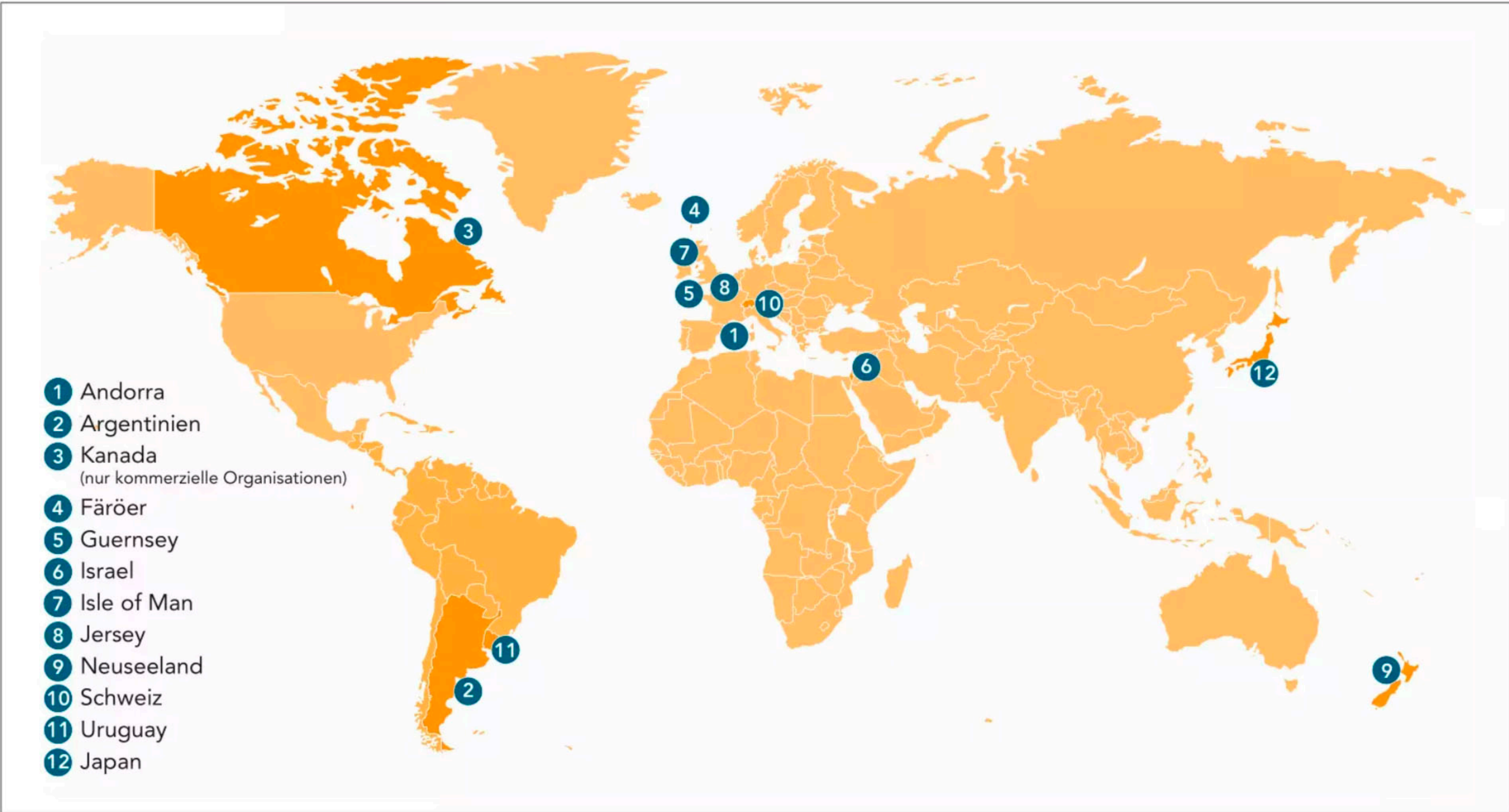


Einwilligung in den Datentransfer

Eine Datenübertragung in ein Drittland kann auch durch die Einwilligung der jeweiligen Betroffenen legitimiert werden, auch wenn der Schutz der personenbezogenen Daten nicht ausreichend sichergestellt werden kann. Dabei sind die Anforderungen an die Freiwilligkeit der Zustimmung zu beachten (siehe Seite 16). Eine weitere Schwierigkeit in der Praxis stellt die Vorgabe dar, dass der Betroffene vor seiner Einwilligung explizit über die geplante Verarbeitung seiner Daten informiert werden muss. Erst wenn der User genau beurteilen kann, was geschehen soll, kann er wirksam einwilligen. Hinzu kommt



noch, dass der Nutzer seine Zustimmung auch jederzeit widerrufen kann. In diesem Fall müssen die Informationen über ihn unverzüglich gelöscht werden. Schließlich gibt es noch eine Reihe von derzeit eher wenig praxisrelevanten Ausnahmen. Wichtig werden könnte in einigen Bereichen die Möglichkeit der Zertifizierung nach Art. 40 DSGVO. So könnte sich zum Beispiel ein amerikanisches Unternehmen nach dessen Vorgaben zertifizieren lassen und so zugleich garantieren, die Vorgaben des europäischen Rechts einzuhalten. Dies könnte zum Beispiel im Cloud-Bereich umgesetzt werden. Allerdings fehlt es immer noch an klaren Vorgaben zur Vergabe von Zertifikaten im EU-Bereich. (anm) **ct**



Diese Länder gelten für die EU-Kommission in Sachen Datenschutz als sichere Drittstaaten.

KRITIS:

Zusätzliche Prüfverfahrenskompetenz für § 8a BSIG

01. – 02. Februar 2021
online



Servermanagement mit Saltstack

02. – 04. Februar 2021
online



Elastic Stack Fundamentals

02. – 04. Februar 2021
online



Docker-Container: Administration und Orchestrierung

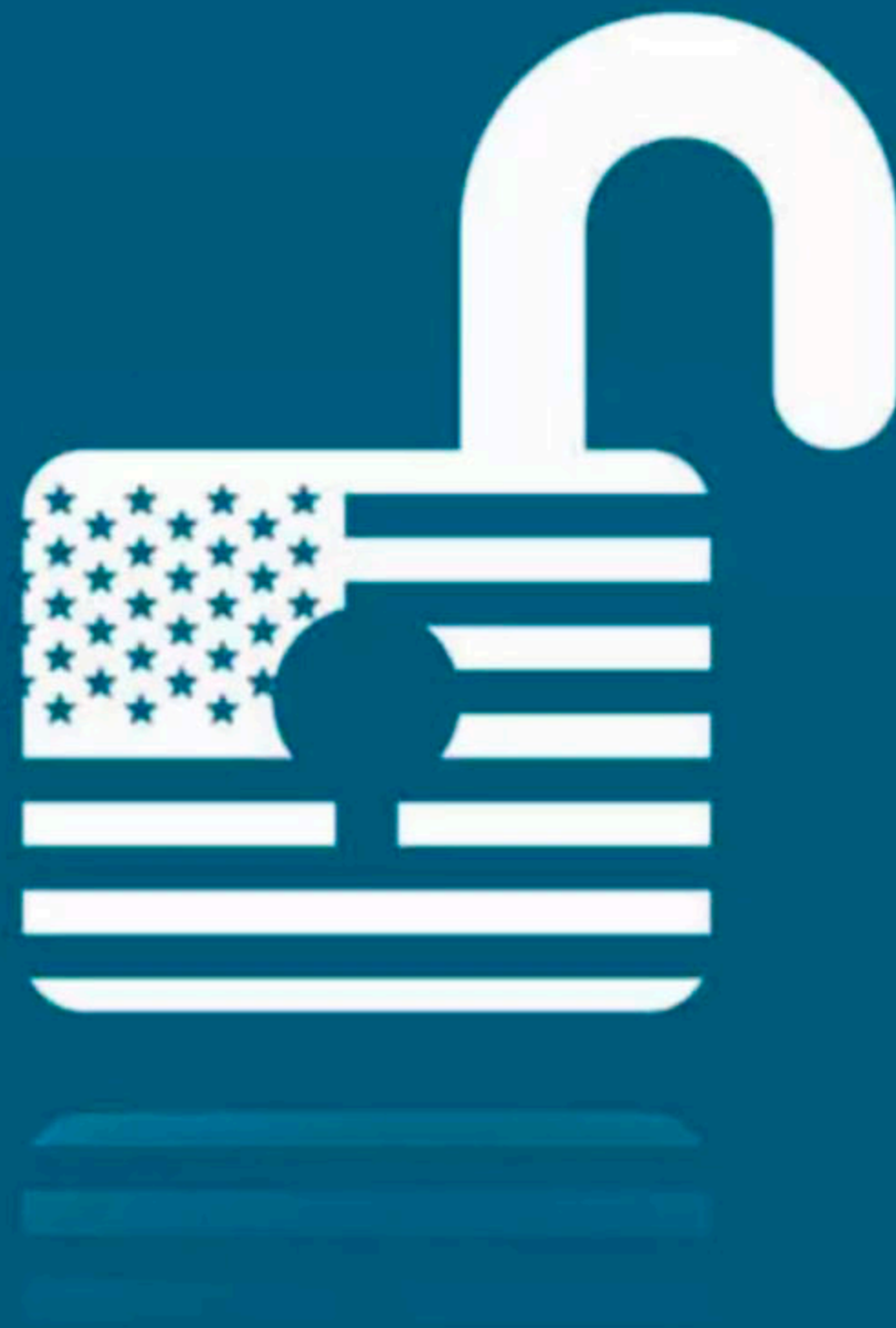
02. – 05. Februar 2021
online



DNSSEC in der Praxis

05. Februar 2021
online





Das Ende des Privacy Shield

Für einen lauten Knall sorgte am 16. Juli 2020 der Europäische Gerichtshof (EuGH), als er das „Privacy Shield“-Abkommen zwischen der EU und den USA für unwirksam erklärte. Unternehmen, die trotzdem noch Daten in die USA übertragen wollen oder müssen, sehen sich schwierigen und wenig transparenten Vorgaben gegenüber.

Von Joerg Heidrich

Für viele war es ein Déjà-vu: Wieder einmal hat der EuGH die zentrale Regelung für Datenübermittlungen von Europa in die USA gekippt (Az. C-311/18). Wieder einmal war der Kläger der österreichische Datenschutzaktivist Max Schrems. Und wieder einmal gab Facebook den Anlass. Die Parallelen der jetzigen Entscheidung gegenüber dem Urteil zu „Safe Harbor“ aus dem Jahr 2015 (Az.: C-362/14) sind so offensichtlich wie bemerkenswert. Doch anders als 2015 könnte die jetzige Entschei-

dung dauerhafte Konsequenzen für den transatlantischen Informationsaustausch haben. In jedem Fall sind die Folgen schwerwiegend.

Formal hat der EuGH „den Beschluss 2016/1250 der Europäischen Kommission über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes“ für ungültig erklärt. Dem Gerichtsbeschluss liegt die Überlegung zugrunde, dass Daten zwar innerhalb der EU ohne weitere Vorgaben frei transferiert werden dürfen. Für Staaten außer-

halb der EU gilt diese Freiheit aber nicht. Es gibt eine Reihe von privilegierten Ländern, bei denen die EU-Kommission aufgrund der dort herrschenden Rechtslage beschlossen hat, dass dort vergleichbar hohe Datenschutzstandards herrschen wie im Unionsraum. Dazu gehören etwa Israel, Kanada, die Schweiz, Neu-



seeland oder auch Japan. Zu diesem Kreis soll nach Willen beider Parteien mittelfristig auch das Vereinigte Königreich zählen. Bis Mitte 2021 bleibt aber erst einmal alles beim Alten und die Übermittlung von Daten nach UK ist weiter zulässig. Nicht zu diesem exklusiven

Kreis gehören allerdings die USA. Dort gibt es zwar in einzelnen Staaten ausgeprägte Datenschutzvorgaben, etwa in Kalifornien. Dies gilt aber nicht für das ganze Land. Um dennoch Daten übermitteln zu können, bediente man sich eines bemerkenswerten Verfahrens: Ein amerikanisches Unternehmen konnte sich in ein Verzeichnis eintragen lassen und verpflichtete sich damit, die Datenschutzrechte der europäischen Bürger angemessen zu würdigen. Dieses Verzeichnis hieß bis 2015 Safe Harbor. Nach dem ersten Urteil des EuGH 2015 folgte darauf der Privacy Shield.

Lippenstift auf Schweinen

Allerdings war das auch schon fast die einzige Änderung. Max Schrems nannte den Vorgang damals „Putting lipstick on a pig“ – das identische Schwein, nur etwas aufgehübscht. Denn was bisweilen euphemistisch „Privacy-Shield-Zertifizierung“ genannt wurde, bestand in der Praxis im Wesentlichen daraus, dass sich ein amerikanisches Unternehmen in ein vom U. S. Department of Commerce geführtes Verzeichnis eintragen und einige Selbstverpflichtungen abnicken musste. Einen wirklichen Schutz der Daten von EU-Bürgern enthielt dagegen keines der beiden



Abkommen. Die Datenwaren und sind nahezu uneingeschränkt den Zugriffen der US-Geheimdienste und diverser Behörden ausgesetzt. Ebenso fehlt es an wirksamen Rechtsmitteln der Betroffenen gegenüber solchen Zugriffen in den USA – ein Zustand, den Datenschutzbehörden seit Jahren bemängeln.

Die Entscheidung des EuGH im Jahr 2020 hat daher kaum jemanden wirklich überrascht. Das Gericht stellte fest, dass den Erfordernissen der nationalen Sicherheit der USA, des dortigen öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang gegenüber den Rechten der Europäer eingeräumt wird. Hieraus ergebe sich, dass hierzulande nicht zulässige Eingriffe in die Grundrechte der Personen ermöglicht werden, deren Daten in die Vereinigten Staaten übermittelt wurden.

Insbesondere seien die auf die amerikanischen Rechtsvorschriften gestützten Überwachungsprogramme nicht auf ein zwingend erforderliches Maß beschränkt. Überhaupt sei nach Ansicht des Gerichts hinsichtlich bestimmter Überwachungsprogramme nicht einmal erkennbar, dass für die darin enthaltenen Ermächtigungen gegenüber EU-Bürgern irgendwelche Einschränkungen bestehen. Auch würden diesen betroffenen Personen keine Rechte verliehen, die sie gegenüber den amerikanischen Behörden gerichtlich durchsetzen könnten.

Wacklige Klauseln

Neben dem Privacy Shield prüfte der EuGH in seiner Entscheidung auch die Standarddatenschutzklauseln (SDK) auf ihre Wirksamkeit. Diese stellen eine alternative Rechtsgrundlage zum transatlantischen Datenverkehr dar. Wer diese Vorgaben nutzen will, muss einige Klauseln, welche von der EU vorgegeben sind, mit seinem amerikanischen Partner vertraglich vereinbaren. Im Rahmen dieser

Vertragsbestandteile wird zwischen den Partnern ein datenschutzfreundlicher Umgang mit persönlichen Informationen vereinbart. In der Praxis sind solche SDK auch beim Transfer von Daten in andere außereuropäische Länder höchst relevant, etwa nach Indien.

Bei der Prüfung kam der EuGH immerhin zu dem Ergebnis, dass die SDK weiter zulässig bleiben. Voraussetzung sei jedoch, dass die Personen, deren Daten in andere Länder

übermittelt werden, ein Schutzniveau genießen müssen, „das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist“. Praktisch bedeutet dies, dass das Zielland geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe bieten muss.

Hier bringt der EuGH die lokalen Datenschutzbehörden im EU-Mitgliedsstaat ins Spiel. Diese hätten einen Datenexport zu verbieten, wenn sie der Auffassung sind, dass die SDK im betreffenden Land nicht eingehalten werden. Kritiker bezweifeln, dass Datenschutzbehörden SDK mit amerikanischen Partnern überhaupt zulassen dürfen. Denn die Klauseln hätten keinerlei Einfluss auf übertriebene Zugriffsmöglichkeiten von US-Behörden und den fehlenden Rechtsschutz. Allenfalls könnten sie technische Maßnahmen festlegen, die den Zugriff Dritter etwa durch Verschlüsselung erschweren.

Ob sich künftige Datenexporte in die USA allein per SDK absichern lassen, ist deshalb fraglich. Damit blieben nicht mehr viele Rechtsgrundlagen. Sehr eingeschränkt lassen sich Daten innerhalb eines Konzerns weitergeben. Als letzte Möglichkeit könnten Firmen explizite Einwilligungen jedes einzelnen Betroffenen einholen. Dazu müssten sie die Nutzer jedoch detailliert informieren, was mit ihren Daten in Übersee geplant ist und wer dort alles Zugriff hat.

Autonomes Europa

Bemerkenswert ist, wie unterschiedlich Datenschutzbehörden auf die Entscheidung reagieren. Ulrich Kelber, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), sieht in dem Urteil eine Stärkung der Rechte der Bürger. Der EuGH mache deutlich, „dass internationaler Datenverkehr weiter möglich ist“. Dabei müssten aber die Grundrechte der europäischen Bürgerinnen und Bürger beachtet und „besondere Schutzmaßnahmen ergriffen“ werden.

Strenger legt die Datenschutzbeauftragte Berlins, Maja Smolczyk, das Urteil aus. Sie

beschwört die digitale Eigenständigkeit Europas und fordert sämtliche Verantwortliche auf, „umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln“. Die Zeiten seien vorbei, in denen personenbezogene Daten aus Bequemlichkeit oder Kostenersparnissen in die USA übermittelt werden könnten. Bereits übermittelte Daten müssten „zurückgeholt werden“.

Dass es allerdings zu schnellen neuen Lösungen für den transatlantischen Datenverkehr kommt, ist derzeit unwahrscheinlich. Es ist kaum zu erwarten, dass eine Biden-Regierung den Bitten der Europäer nach mehr Datenschutz für die eigenen Bürger nachkommen wird. Europäische Firmen und Anwender

müssen sich auf einen längeren Zeitraum mit rechtlicher Ungewissheit bei der Zusammenarbeit mit US-Unternehmen einstellen. Umso wichtiger ist es, rechtssichere Alternativen voranzutreiben, die nicht auf ein Placet aus Washington angewiesen sind. In der Zwischenzeit bleiben nur alternative Vorgehensweisen, wie der folgende Artikel näher erklärt.

(anm) **ct**



Es gibt **10** Arten von Menschen.
iX-Leser und die anderen.



**3 x als
Heft**

Jetzt Mini-Abo testen:
3 Hefte + Bluetooth-Tastatur
nur 16,50 €

www.iX.de/testen



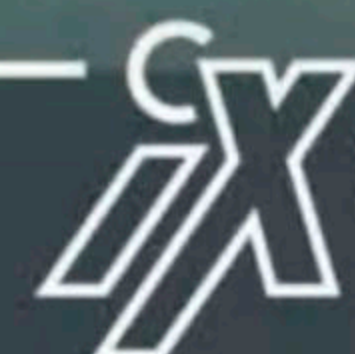
www.iX.de/testen



49 (0)541 800 09 120



leserservice@heise.de



MAGAZIN FÜR PROFESSIONELLE
INFORMATIONSTECHNIK

Alternativen zum Privacy Shield



Mit dem Wegfall des Privacy Shield entfällt über Nacht die zentrale Rechtsgrundlage für eine Übertragung personenbezogener Daten in die USA. Damit stellt sich die praxisrelevante Frage, ob und für wen es Alternativen dazu gibt.

Von Joerg Heidrich

Nachdem sich der Fallout und der Pulverdampf lichten, den das Urteil des Europäischen Gerichtshofs in Sachen „Schrems II“ hinterlassen hat, müssen die Unternehmen und ihre IT überlegen, wie sie mit der Entscheidung und ihren Auswirkungen umgehen. Der EU-US Privacy Shield jedenfalls ist auf Basis der Entscheidung unwirksam und nicht mehr anwendbar. Auch die Regelungen der Standardvertragsklauseln sind zumindest nicht mehr uneingeschränkt nutzbar – was übrigens auch für den Export von Daten in andere Länder als die USA wie etwa Indien oder China gilt (siehe Seite 108).

Keine Übergangsfristen

Auf der anderen Seite sind die allermeisten Unternehmen auf die Nutzung von US-Software angewiesen und es gibt keinesfalls immer eine adäquate europäische Alternative, auf die man schnell und unproblematisch umsteigen könnte. Tatsächlich besteht hierzulande eine Abhängigkeit von einer essenziellen US-Infrastruktur. Denn auch ein kleines Unternehmen wird es kaum schaffen, für den beruflichen Einsatz beispielsweise ein Smartphone ohne Apple oder Android zu finden. Schon die reine Nutzung des Internets dürfte ohne amerikanische Infrastruktur nicht möglich sein.

Doch welche Alternativen bleiben nach dem Fall des Privacy Shield konkret für die Unternehmen? Und welche Risiken sind damit verbunden?

Die schlechte Nachricht vorweg: Eine Übergangsfrist zur weiteren Nutzung des Privacy Shield gibt es nicht. Die Aussage der Datenschutzkonferenz (DSK), des Gremiums der deutschen Datenschutzbehörden, ist hier sehr eindeutig. Die Übermittlung personenbezogener Daten in die USA auf der Grundlage des Privacy Shield sei unzulässig und müsse unverzüglich eingestellt werden.

Auch ist realistischerweise nicht zu erwarten, dass sich die EU-Kommission und die amerikanische Regierung in absehbarer Zeit auf ein neues, ähnliches Abkommen verständigen können, das eine vergleichbar einfache Übermittlung von Daten zulässt. Hierfür sind auf der einen Seite die Anforderungen des Europäischen Gerichtshofs ebenso wie die der DSGVO zu hoch. Auf der anderen Seite ist kaum damit zu rechnen, dass die USA ihre großflächige Überwachung globaler Datenströme zugunsten der



Europäer in kurzer Zeit erheblich reduzieren, auch nicht unter einem Präsidenten Biden.

Schwierige Alternativen

In der Praxis relevant war neben dem Privacy Shield bislang die Nutzung der Standardvertragsklauseln der Europäischen Kommission. Dabei handelt es sich um vorgegebene Formulierungen für vertragliche Vereinbarungen zwischen dem europäischen und dem amerikanischen Partner. Der Grundgedanke dahinter ist, dass die Parteien untereinander die Einhaltung datenschutzrechtlicher Vorgaben vereinbaren und dann auch für diese Einhaltung sorgen. Das Problem dabei: Natürlich kann auch ein solcher Pakt amerikanische Behörden nicht davon abhalten, in den Daten der europäischen Nutzer herumzuschnüffeln. Das kann realistischere auch kein US-Unternehmen garantieren.

Diese Problematik hat auch der EuGH in seiner Entscheidung gesehen. Die Richter kamen dabei zu dem Ergebnis, dass diese Klauseln zwar grundsätzlich weiter genutzt werden können. Es müsse jedoch von den Beteiligten geprüft werden, ob bezüglich der Rechte der betroffenen Personen im Drittland, also insbesondere in den USA, ein gleichwertiges Schutzniveau wie in der Union herrscht. Dies sei in den Vereinigten Staaten grundsätzlich nicht der Fall, sodass die Vereinbarung der Standardvertragsklauseln allein nicht ausreicht. Es ist allerdings nach den Vorstellungen des Gerichts möglich, mit zusätzlichen Maßnahmen dieses Schutzniveau sicherzustellen.

Kreative technische Maßnahmen gefragt

Hier liegt eine Chance für kreative technische Maßnahmen. Diese müssen einen grenzenlosen Zugriff der US-Dienste zumindest wirksam eindämmen. Eine wichtige Rolle könnte hier der Kryptografie zukommen. So bietet beispielsweise ein Hersteller von Überwachungskameras an, die entstehenden Aufnahmen zum Abruf in eine US-Cloud zu legen. Dieses Geschäftsmodell wäre möglicherweise dadurch zu retten, dass die Aufnahmen nach Stand der Technik verschlüsselt werden und die Schlüssel dazu ausnahmslos beim Kunden liegen.

Allerdings sind hier die deutschen wie die europäischen Datenschutzbehörden nicht sehr gnädig. Kommt ein Unternehmen zu dem Schluss, dass keine ergänzenden Maßnahmen möglich sind, so sei kein angemessenes Schutzniveau gewährleistet. In diesem Fall fordert die Europäische Datenschutzkommission, die Übermittlung personenbezogener Daten in die USA sofort auszusetzen oder zu beenden. Wer trotzdem weiterhin persönliche Informationen übermitteln möchte, habe seine zuständige Aufsichtsbehörde zu benachrichtigen, hierzulande die Datenschutzbehörde des jeweiligen Bundeslands.

Ein ähnliches Schicksal droht auch den Nutzern der sogenannten Binding Corporate Rules (BCR; auf Deutsch verbindliche interne Datenschutzvorschriften) als Basis für eine Datenweitergabe. Auf Basis der BCR können multinationale Konzerne,

internationale Organisationen und Firmengruppen innerhalb ihrer Organisation personenbezogene Daten in Drittstaaten mit nicht angemessenem Schutzniveau transferieren. Hinsichtlich der USA reicht dies allein als Rechtsgrundlage

nach Ansicht der Europäischen Datenschutzkommission ebenfalls nicht mehr aus. Auch hier sind zusätzliche Maßnahmen nötig, um einen Zugriff der US-Behörden weitestgehend zu verhindern.

Einwilligung als Alternative?

Als eine der wenigen Alternativen zu den oben genannten Rechtsgrundlagen bleibt das Einholen von Einwilligungen der Betroffenen. Das klingt allerdings einfacher, als es in der Praxis ist. Denn eine solche Zustimmung kann nur freiwillig von einem informierten Nutzer erteilt werden. Das bedeutet, dieser muss vorab über die geplante Verarbeitung seiner Daten informiert werden. Auch über einen Transfer in die USA muss er natürlich informiert werden, ebenso wie über eine mögliche Nutzung seiner Daten durch amerikanische Dienste und Behörden.

Einen rechtswirksamen Informationstext zu formulieren, ist daher eine echte Herausforderung. Dennoch kann die Einwilligung in einigen Bereichen, bei denen der Nutzer ohnehin um seine Zustimmung gebeten wird, als Rechtsgrundlage dienen. Dies gilt zum Beispiel für Consent-Tools, also die ungeliebten Cookie-Banner, im Rahmen des Einholens von Einwilligungen für das Setzen von



Cookies (siehe Seite 132). Die dabei erlangten Informationen, namentlich die IP-Adressen, werden häufig in die USA exportiert, sodass es auch hierfür einer Rechtsgrundlage bedarf. Diese könnte in einem ergänzten Passus in dem Text des Consent-Tools bestehen.

Umstritten ist, ob Einwilligungen für die Nutzung ihrer persönlichen Daten in US-basierten Tools auch von Mitarbeitern innerhalb des Unternehmens eingeholt werden können. Da hier die Entscheidungsfreiheit der Beschäftigten in einem Arbeitsverhältnis eingeschränkt ist, wäre hierfür, soweit möglich, eine Betriebs- oder Dienstvereinbarung die wohl bessere Wahl.

Jenseits dieser Rechtsgrundlagen gibt es noch ein paar Ausnahmeregelungen, die einen Datentransfer in die USA ermöglichen. Sie sind in Art. 49 der DSGVO geregelt. Dieser erlaubt beispielsweise das Übermitteln von Informationen, die zur Erfüllung eines Vertrags notwendig sind. Das umfasst zum Beispiel Buchungsdaten für Hotelübernachtungen in den Staaten. Erlaubt ist der Datentransfer auch, wenn die Übermittlung aus wichtigen Gründen des öffentlichen Interesses oder für das Geltendmachen von Rechtsansprüchen notwendig ist. Diese Sonderfälle sind für den Alltag von Unternehmen allerdings nur selten relevant.

Die Rolle der Auftragsverarbeiter

Häufig findet innerhalb der Unternehmen der Datenexport in die USA nicht direkt statt, sondern es ist ein Auftragsverarbeiter dazwischengeschaltet (siehe auch Seite 72). Das ist in vielen Fällen die europäische Niederlassung eines US-Konzerns, meist mit Sitz in Irland. Bisher war ein Transfer über den Atlantik innerhalb des amerikanischen Konzerns relativ problemlos möglich.

Auch dies ändert sich nun. Ob eine solche Übertragung stattfindet, ergibt sich aus dem Vertrag, der mit dem Auftragsverarbeiter nach Artikel 28 DSGVO abzuschließen ist. Dort muss dokumentiert werden, ob Übermittlungen in ein Drittland erfolgen und auf welcher Rechtsgrundlage. Dies gilt auch für Subunternehmer, die Unterauftragsverarbeiter.

Sofern eine Weitergabe in die USA durch einen Dienstleister erfolgt, gelten die oben genannten

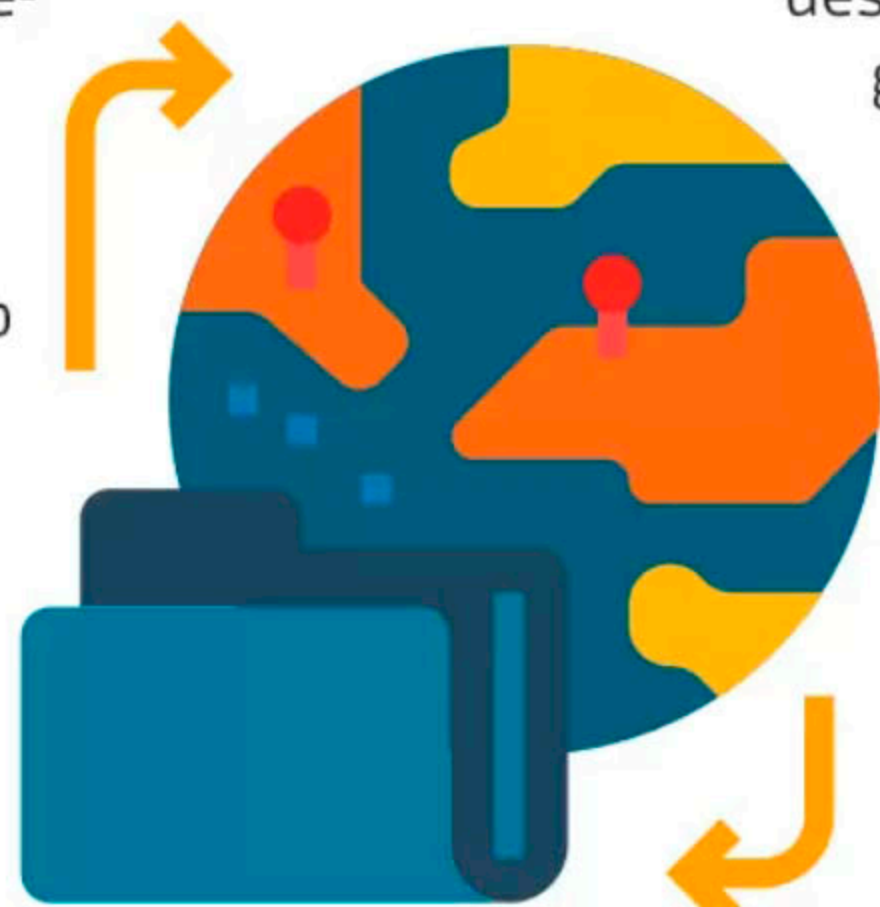
Vorgaben: Wenn nicht eine Ausnahmeregelung vorliegt, muss technisch durch zusätzliche Maßnahmen ein angemessenes Schutzniveau für die Daten hergestellt werden. Ist dies nicht möglich, so empfiehlt die Europäische Datenschutzkonferenz in einer FAQ, eine Änderungs- oder Ergänzungsklausel des Vertrags auszuhandeln, um Übertragungen in die USA zu verbieten. In diesem Fall sollen personenbezogene Daten nicht außerhalb des EWR-Gebiets (Europäischer Wirtschaftsraum) übertragen werden und alle Verarbeitungsaktivitäten sollten im EU-Gebiet stattfinden.

Was bei Nichtbeachtung droht

Die Entwicklungen nach dem Urteil zu ignorieren und weiter ohne Rechtsgrundlage Daten zu übermitteln, ist sicher keine gute Idee. Der EuGH hatte ausdrücklich betont, dass die Datenschutz-Aufsichtsbehörden verpflichtet seien, unzulässige Datenexporte zu verbieten. Zwar ist im Moment noch offen, wie die zuständigen Datenschutzbehörden auf die aktuellen Entwicklungen reagieren werden. Allerdings kündigten sie bereits an, keine Übergangsfrist zu gewähren. Zudem ist es häufig leicht herauszufinden, ob noch nach den Vorgaben des Privacy Shield Daten übermittelt werden. Nicht zuletzt steht das in vielen Fällen sogar immer noch in fahrlässigerweise nicht geänderten Datenschutzerklärungen.

Finanziell droht in diesem Fall ein Bußgeld, das – wie in der DSGVO üblich – bei bis zu 20 Millionen Euro oder 4 Prozent des weltweit erzielten Umsatzes des Unternehmens liegen kann. Wie hoch die geforderte Summe dann tatsächlich ist, ist immer vom Einzelfall abhängig und wird auf Basis einer Vorgabe der Behörden ermittelt (siehe Seite 62). Je nach Größe des betroffenen Unternehmens, der Menge der übertragenen Daten und deren Grad an Vertraulichkeit können hier aber leicht Bußgelder in sechs- oder siebenstelliger Höhe erreicht werden.

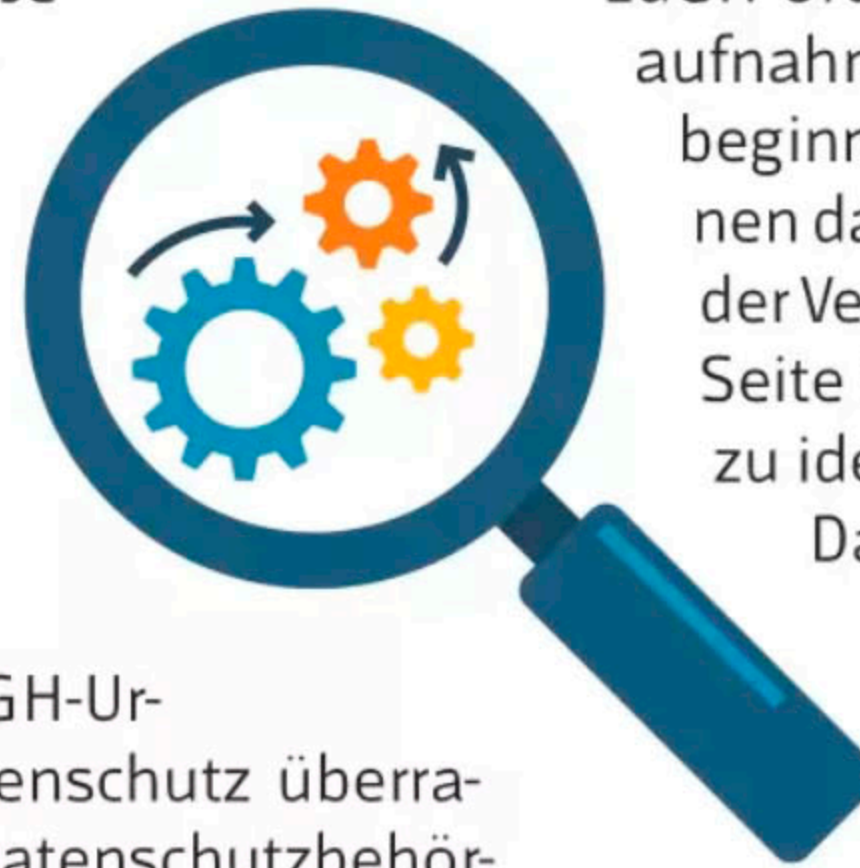
Zudem droht weiteres Ungemach, auf das auch die Berliner Datenschutzbeauftragte in ihrer Pressemeldung zu dem Urteil noch einmal explizit hinweist: Danach könnten betroffene Personen Schadensersatz für unzulässige Datenexporte verlangen. Dieser bezieht sich auf einen immateriellen Schaden und müsse nach dem europäischen Recht eine abschreckende Höhe aufweisen. Wer also Opfer eines unberechtigten Daten-



transfers außerhalb des EWR ist, kann möglicherweise ein Schmerzensgeld geltend machen. Dieses wäre zwar in jedem Einzelfall nur verhältnismäßig klein, vielleicht im unteren vierstelligen Bereich. Macht aber eine große Anzahl an Betroffenen solche Ansprüche geltend, kann dies für das verantwortliche Unternehmen schnell existenzbedrohend werden.

Was also jetzt tun?

Auch wenn das Ergebnis des EuGH-Urteils für keinen Experten im Datenschutz überraschend kommen konnte und die Datenschutzbehörden seit Jahren vor der Nutzung des Privacy Shield warnten: Patentrezepte für den Umgang mit der neuen Situation hat niemand. Und wenn, dann sehen diese das sofortige Abschalten aller US-Hard-



und Software vor, was aber nicht nur unrealistisch, sondern regelrecht weltfremd ist – zumindest, wenn das Unternehmen weiterarbeiten will.

In der wirklichen Welt sollte die Aufarbeitung des EuGH-Urteils zunächst mit einer internen Bestandsaufnahme der datenschutzrelevanten Prozesse beginnen. Datenschutzaffine Unternehmen können dabei auf ihr bereits bestehendes Verzeichnis der Verarbeitungstätigkeiten zurückgreifen (siehe Seite 50). Ziel sollte es dabei sein, alle Prozesse zu identifizieren, bei denen personenbezogene Daten insbesondere von Kunden direkt oder indirekt über Auftragsverarbeiter oder sonstige Dritte in die USA oder andere Drittstaaten übertragen werden.

Auf diese Liste gehören auch solche Applikationen, die personenbezogene Informationen von Mitarbeitern übertragen. Dabei müssen IT und Datenschutz eng zusammenarbeiten. Am Ende sollte ein Verzeichnis stehen, aus dem ersicht-

Back to BASIC

Exklusiv
im heise shop!

+ Nano-Axe-
Board mit
PICAXE-08M2



Make Picaxe Special

Noch einfacher als Arduino: Im neuen PICAXE Special der Make dreht sich alles um den Einstieg ins Programmieren mit BASIC. Dazu gibt es ein neuentwickeltes Programmierboard für den Einsatz von PICAXE-Chips, das Nano-Axe-Board mit USB-Anschluss. Damit können Sie sofort starten!

shop.heise.de/make-picaxe

24,95 € >

NEU

 **heise shop**

shop.heise.de/make-picaxe >

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

lich wird, bei welchen Prozessen welche Daten wohin außerhalb des EWR übertragen werden. Diese Bestandsaufnahme ist zugleich ein guter Weg, Schatten-IT – also nicht genehmigte Anwendungen und Speicherorte – innerhalb des Unternehmens zu identifizieren.

Im nächsten Schritt wären die Prozesse gemeinsam zu analysieren und zu gewichten. Gerade bei nicht zwingend notwendigen Anwendungen fällt es leichter, Alternativen zu finden. Hier ist es zum Beispiel häufig möglich, auf interne Lösungen zu setzen, die man bei dieser Gelegenheit einheitlich im Haus ausrollen kann. So ist es sinnvoll, einen internen Datenspeicher on Premises für alle zu betreiben und so dafür zu sorgen, dass wertvolle Firmeninformationen eben nicht in den diversen US-Clouds landen. Zugleich kann man in diesem Rahmen einen internen Wildwuchs beenden, etwa bei der Nutzung diverser Videokonferenzanbieter. Und im Zweifel müssen eben auch lieb gewordene „Nice-to-have“-Dienste einzelner Abteilungen einfach abgeschaltet werden, notfalls auch gegen den Willen der Mitarbeiter.

Den Rest muss die Technik richten

Allerdings lassen sich natürlich nicht alle Dienste abschalten oder durch europäische Angebote ersetzen. Ab einem bestimmten Punkt verbleiben auf der Liste nur „Must-have“-Prozesse mit amerikanischen Anbietern, direkt oder indirekt über Auftragsverarbeiter, von denen das Unternehmen abhängig ist. Dies sind in den meisten Fällen auch die Googles oder Microsofts. An der Stelle ist man dann auf die Kooperation mit diesen Anbietern angewiesen.

Diese Unternehmen sind im eigenen Interesse gezwungen, ihre Angebote so umzubauen, dass eine Zusammenarbeit mit ihnen weiter möglich ist. Dabei scheint eine Kombination aus dem Abschluss von Standardvertragsklauseln mit flankierenden technischen Maßnahmen erfolgversprechend. Letztere können etwa in der Verschlüsselung der Daten liegen, im Auslagern von Serverstandorten in von der EU als sicher definierte Länder oder auch in der Änderung technischer Prozesse, die eine Speicherung von Daten on Premises oder auf den Endgeräten der Nutzer vorsehen. Anregungen für mögliche technische Unterstützung durch Privacy-Maßnahmen bietet der Kasten „Mögliche technische Schutzmaßnahmen als Ergänzung“.

Verweigert ein Unternehmen die Umstellung oder bietet es keine unterstützenden technischen Maßnahmen an, so bleibt für die europäischen

Mögliche technische Schutzmaßnahmen als Ergänzung

- Transportverschlüsselung Ende-zu-Ende
- Verschlüsselung der abgelegten Daten
- alleinige Verwaltung der Schlüssel beim europäischen Unternehmen oder beim Nutzer
- E-Mail-Verschlüsselung
- Ablage von Daten on Premises oder auf den Geräten der Endbenutzer statt zentral in den USA
- Treuhandlösungen wie das inzwischen eingestellte Daten-Treuhand-Modell von Microsoft mit der Telekom
- exklusiv für den Auftraggeber gehostete Server
- Nutzung von Zwei-Faktor-Authentifizierung

Unternehmen mittelfristig keine andere Chance, als die Zusammenarbeit zu beenden oder mit dem Risiko eines hohen Bußgelds zu leben.

Fazit

Die Entscheidung des EuGH stellt jedes Unternehmen vor erhebliche Herausforderungen, die es unverzüglich angehen sollte. Allerdings sind die bestehenden Handlungsoptionen sehr eingeschränkt. In einigen Fällen, vor allem im Bereich Onlinewerbung und Tracking, kann die Nutzung von Einwilligungen eine Option sein. Einziges Mittel der Wahl ist in vielen Fällen nur noch die Nutzung von Standardvertragsklauseln, bei denen durch technische Maßnahmen das Risiko eines Zugriffs durch US-Behörden zumindest eingeschränkt wird.

Das stellt allerdings für alle Beteiligten eine große Herausforderung dar. Da kaum eine schnelle neue Lösung als Rechtsgrundlage für die Übermittlung von Daten über den Atlantik in Sicht ist, muss als langfristiges Ziel aber die Emanzipation von allzu datenhungrigen US-Angeboten und das Erreichen einer digitalen Souveränität hiesiger Unternehmen stehen. (anm) **ct**

Vernetzen, verstehen, umsetzen –

mit heise Security Pro
zu mehr IT-Sicherheit.

Nur 995 €
im Jahr

 heise Security **Pro**

heise Security Pro liefert Ihnen **Hintergründe, Analysen und vertiefendes Know-how** rund um IT-Sicherheit und **vernetzt IT-Security-Experten**. Werden auch Sie Teil dieser Community und sichern Sie sich jetzt das Profi-Paket für nur 995 € im Jahr*:

- | | |
|---|--|
|  Mindestens 4 Security Webinare |  Jährliche heise Security Konferenz |
|  1 Ticket für die secIT |  heise Security Expertenplattform |
|  Wöchentlicher Experten-Newsletter |  1 heise+ Lizenz |

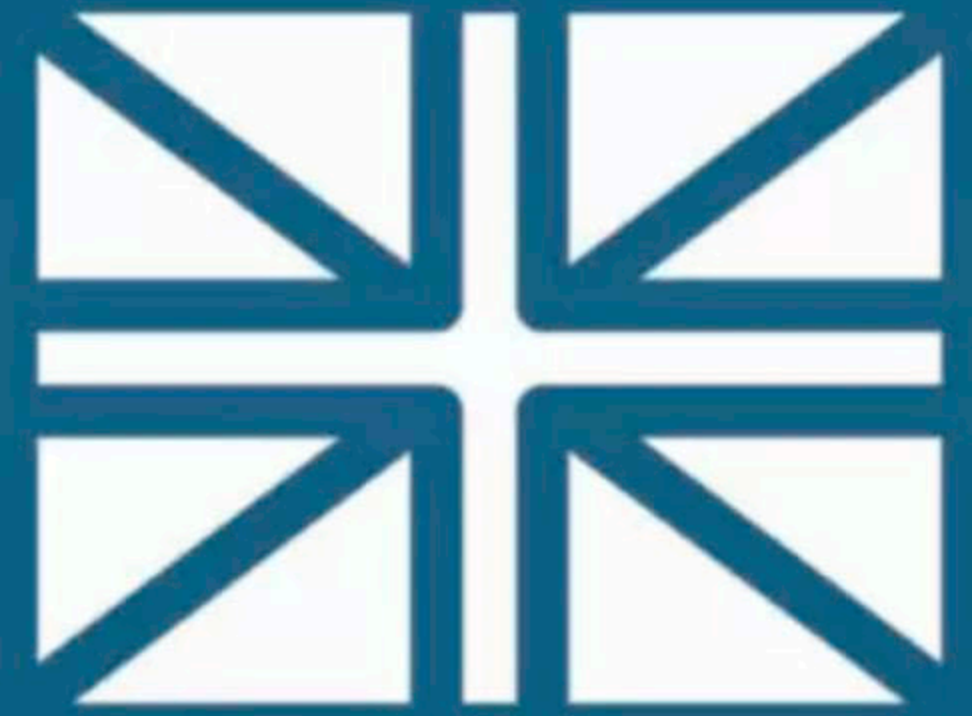
*Weitere Pakete auf Anfrage bei pro-service@heise.de.

JETZT TEIL DER
COMMUNITY WERDEN:

heise.de/heisec-pro



Der Brexit und seine Folgen



Den drohenden GAU im Datenverkehr zwischen der EU und Großbritannien konnte der Brexit-Vertrag gerade noch mal abwenden. Doch juristisch abgesichert sind künftige Übertragungen persönlicher Daten ins Vereinigte Königreich noch lange nicht. Firmen müssen deshalb jetzt vorbeugen.

Von Joerg Heidrich

Es war so eine Art Weihnachtswunder, die Vereinbarung zwischen der Europäischen Union und dem Vereinigten Königreich, die am 24. Dezember 2020 und damit wenige Tage vor dem Fristende am 31. Dezember geschlossen wurde. Durch das Handelsabkommen konnte der harte Brexit in letzter Minute erst einmal vermieden werden.

Ziel des Brexit-Vertrags ist nach Aussagen der EU-Kommission, „den digitalen Handel zu erleichtern, indem ungerechtfertigte Hindernisse beseitigt werden. Gleichzeitig sollen „hohe Standards für den Schutz personenbezogener Daten gewährleistet werden“.

Hätte es keine Regelung zum Export von Daten über den Ärmelkanal gegeben, so wäre Großbritannien aus Datenschutzsicht über Nacht zu einem unsicheren Drittstaat geworden (siehe Seite 108). Übermittlungen personenbezogener Daten wären dann nur noch unter sehr engen Voraussetzungen möglich gewesen.

Sechs Monate Frist

Die Übereinkunft legt fest, dass Großbritannien für eine Übergangsfrist nicht als unsicherer Drittstaat eingestuft wird. Voraussetzung ist, dass die Briten für diesen Zeitraum an ihren auf

der DSGVO basierenden nationalen datenschutzrechtlichen Regelungen festhalten. Eine Abweichung wäre nur mit Zustimmung der EU zulässig.

Bis Ende April kann der Datenverkehr also unverändert weiter fließen. Diese Übergangsfrist kann dann noch einmal um zwei Monate verlängert werden. Bis spätestens Ende Juni muss die EU-Kommission einen Angemessenheitsbeschluss mit dem Vereinigten Königreich vereinbaren. Die Verhandlungen dazu sollen unverzüglich beginnen.

Umstrittene Sonderregelung

Allerdings vertreten namhafte britische Juraprofessoren die Ansicht, dass das EU-Recht derartige Sonderregelungen wie im Brexit-Vertrag gar nicht erlaubt. Zudem stünde die Vereinbarung im Widerspruch zur DSGVO, welche den Datenexport außerhalb der EU regelt. Denn formal hat das Vereinigte Königreich zum 1. Januar 2021 die EU verlassen und ist kein Mitgliedsstaat mehr. Dagegen wird etwa argumentiert, dass es sich bei dem Übereinkommen um einen völkerrechtlichen Vertrag handelt, der dem EU-Recht vorgeht.

Kein Problem mit dem vereinbarten Sonderweg hat offenbar die Konferenz der hiesigen Datenschutzaufsichtsbehörden. Diese begrüßen in einer



Presseerklärung Ende Dezember ausdrücklich die beschlossene „vorläufige Rechtssicherheit für Datenübermittlungen in das Vereinigte Königreich“. Das Abkommen würde den „bisher befürchteten gravierenden Rechtsunsicherheiten“ vorbeugen. Die britische Datenschutzbehörde ICO lobte den Vertrag als „bestmögliche Regelung für UK-Organisationen, die personenbezogene Daten aus der EU verarbeiten“.

Sichere Drittstaaten

Endet die durch den Vertrag geschaffene Frist, stehen Ende Juni zwei Szenarien im Raum: Die beiden bislang arg zerstrittenen Parteien einigen sich auf den Angemessenheitsbeschluss. Einigt man sich nicht, folgt der harte Datenschutz-Brexit mit Verspätung.

Einigt man sich, könnte vom Sommer 2021 an auch das Vereinigte Königreich als sicherer Drittstaat eingeordnet werden. Entsprechende Verhandlungen sollen nach Aussage der zuständigen EU-Kommission bereits seit einigen Monaten laufen. Experten bezweifeln allerdings, dass eine dafür nötige Vereinbarung in einem derart kurzen Zeitraum erreicht werden kann. Die Verhandlungen mit Japan dauerten etwa weitaus länger.

Und auch inhaltlich gibt es Zweifel, dass in UK tatsächlich von einem mit der EU vergleichbaren Datenschutzniveau auszugehen ist. Kritisch gesehen wird dabei vor allem die starke Rolle der Geheimdienste. Diese sind eng mit den amerikanischen Diensten vernetzt und auch Teil der „Five Eyes“-Gemeinde. Zu diesem elitären Kreis von überwachungsfreundlichen Staaten gehören neben den USA und Großbritannien auch Australien, Kanada und Neuseeland. Zumindest bei den beiden letztgenannten Ländern stand dies allerdings einer Anerkennung als sicherer Drittstaat nicht im Wege.

Unsichere Drittstaaten

Kommt es bis Ende Juni zu keiner Einigung, würde auch Großbritannien in die Einordnung als unsicherer Drittstaat fallen, in der sich bereits China, Indien, Russland sowie die USA finden. Eine Weitergabe von Informationen in diese Länder ist zwar nicht grundsätzlich verboten. Allerdings gibt es einige rechtliche

Hürden, die vor der ersten Übertragung geklärt werden müssen.

Für solche Staaten gelten die strengen Vorschriften der Art. 44 ff. DSGVO. Praktisch relevant ist hierbei vor allem der Abschluss von Standard-datenschutzklauseln (SDK, siehe Seite 112). Allerdings arbeitet die EU-Kommission derzeit an Neuformulierungen der Klauseln, die vermutlich Anfang 2021 fertig werden.

Zudem sind nach der Rechtsprechung des EuGH meist noch zusätzliche technische und organisatorische Schutzmaßnahmen zu ergreifen, insbesondere um die EU-Bürger vor dem allzu leichtfertigen Zugriff fremder Geheimdienste zu schützen. Zu diesen Schutzmaßnahmen gehören zum Beispiel die Anonymisierung und Verschlüsselung von Daten.

Eine Datenübertragung in ein Drittland kann zudem auch durch eine Einwilligung der jeweiligen Betroffenen legitimiert werden (siehe Seite 116).

Auf den Ernstfall vorbereiten

IT-Unternehmen sind gut beraten, die drohenden Gefahren ernst zu nehmen und den Aufschub zu gründlichen Vorbereitungen auf den möglichen „Datenschutz-Brexit“ zu nutzen. Hierzu gehört es zunächst, die eigene Abhängigkeit von UK-Unternehmen zu analysieren und Ausschau nach möglichen Alternativen zu halten.

Für wichtige und unverzichtbare Partner, zum Beispiel im Bereich IT, Personalwesen oder Finanzen, empfiehlt es sich, rechtzeitig ein Szenario ohne Angemessenheitsbeschluss zu planen.

Dazu werden vor allem Standard-datenschutzklauseln das Mittel der Wahl sein. Wer diese bis Ende Juni vorbereitet, kann Mitte des Jahres im Notfall schnell umsteigen. Dafür ist es wichtig, zusätzliche technische und organisatorische Maßnahmen zum Schutz der Daten der EU-Bürger zu definieren und vorzubereiten.

Anders als bei der vergleichbaren Rechtslage in den USA nach dem Schrems-II-Urteil im vergangenen Jahr ist kaum damit zu rechnen, dass die hiesigen Datenschutzbehörden bei Verstößen gegen die strengen DSGVO-Vorgaben zum Datentransfer nach UK Milde walten lassen werden. (anm) 





Ohne IT-Sicherheit kein Datenschutz

Ganz besonders wirkt sich die neue Rechtslage auf die IT-Sicherheit aus, die nun mit der DSGVO elementarer Bestandteil des Datenschutzes ist. Vernachlässigt man die Pflichten, in der technischen Praxis wie im Umgang mit Daten, drohen hohe Bußgelder.

Von Joerg Heidrich

Das Thema IT-Sicherheit hat in der DSGVO einen überragend hohen Stellenwert erhalten. Zwar kannte auch das alte Recht schon den Bereich der Datensicherheit. Die neuen Regelungen erweitern jedoch die gesetzlichen Anforderungen an die Technik so erheblich, dass die IT-Sicherheit elementarer Bestandteil des Datenschutzes wird.

Von zentraler Bedeutung sind dabei Begriffe wie Vertraulichkeit, Integrität, Verfügbarkeit und die Belastbarkeit der IT-Sicherheitssysteme. Was hier zu beachten ist, regelt Art. 5 DSGVO. Danach müssen

personenbezogene Daten „in einer Weise verarbeitet werden, die eine angemessene Sicherheit“ der Daten gewährleistet, „einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“. Konkreter wird hier Art. 32, der die technischen Anforderungen an die Verarbeitung von persönlichen Daten definiert. Diese kann man sich wie eine Waage vorstellen: Auf der einen Seite stehen die zu schützenden Daten, auf der anderen die zu ergreifenden Maßnahmen. Zu berücksichtigen sind danach unter an-

derem Faktoren wie der Stand der Technik, die Implementierungskosten, die unterschiedlichen Eintrittswahrscheinlichkeiten sowie die Schwere des Risikos für die Betroffenen.

Wichtig ist, dass die Risikobewertung aus dem Blickwinkel der einzelnen Kunden und Mitarbeiter zu erfolgen hat – nicht aus der des Unternehmens. Es kommt also primär nicht darauf an, welche Schäden, etwa im Bereich der Reputation, ein Unternehmen oder ein Freiberufler durch eine Datenpanne aufweisen könnte. Entscheidend ist vielmehr, was den Inhabern der Daten – in der Regel Kunden und Mitarbeitern – beispielsweise durch ein Datenleck drohen könnte, also etwa durch den Abfluss sensibler Krankendaten oder von Kreditkartennummern.

Backups werden verpflichtend

Von diesem Risiko für die Betroffenen ausgehend, müssen die für die Datenverarbeitung Verantwortlichen „geeignete technische und organisatorische Maßnahmen“ ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Als zu ergreifende Maßnahmen nennt das Gesetz sogar ein paar konkrete Methoden:

- Die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Praktisch bedeutet das nichts weniger, als dass die Verpflichtung zum regelmäßigen Einspielen von Backups (siehe Seite 140) ebenso gesetzliche Pflicht wird wie die regelmäßige Evaluierung der eigenen IT-Infrastruktur, etwa durch Pentesting. Die oben genannten Maßnahmen sind eher beispielhaft zu verstehen. Es ist also nicht zwingend erforderlich, alle

umzusetzen. Ausreichend ist ein überzeugendes Konzept zur IT-Sicherheit, das diese Teile enthalten kann und sollte, aber nicht zwingend muss, sofern das Konzept als Ganzes überzeugt.

Stand der Technik

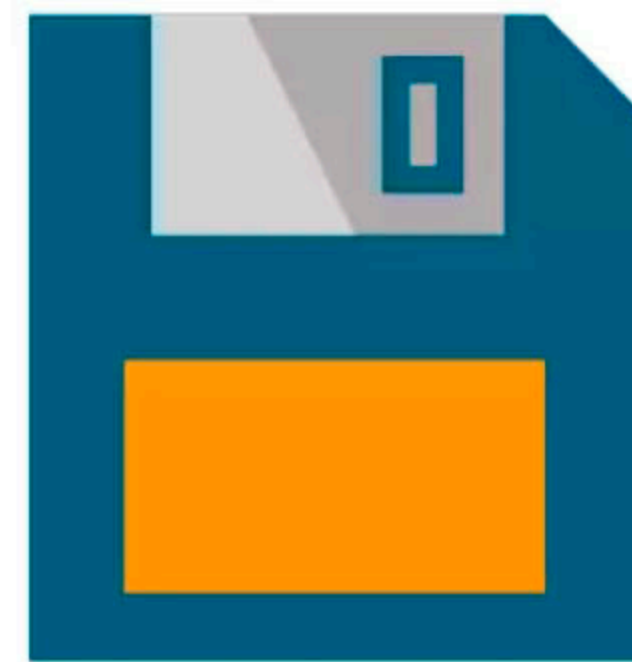
Ebenfalls neu im Bereich des Datenschutzes sind die Anforderungen, bei der Konzeption des Schutzes der jeweils verarbeiteten Daten den Stand der Technik zu berücksichtigen. Darunter versteht man solche technischen Maßnahmen, die schon zur Verfügung stehen und die sich in der Praxis als geeignet und effektiv bewährt haben. Nicht gemeint sind dagegen die neuesten technischen Entwicklungen aus den Laboren. Der Stand der Technik ist nicht statisch, sondern muss immer wieder auf neue Entwicklungen geprüft werden, um die Datensicherheit gewährleisten zu können.

Daraus ergibt sich aber natürlich nicht, dass sich jedes kleine Unternehmen eine den neuesten und teuersten Anforderungen genügende IT-Infrastruktur einrichten muss. Denn der hier relevante Art. 32 DSGVO sieht unter anderem die Berücksichtigung der Implementierungskosten vor, also letztlich ein Gebot der Verhältnismäßigkeit. Hierbei ist hinsichtlich der Auswahl von Hard- und Software eine Abwägung vorzunehmen, die auch zu dokumentieren ist. Sehr hilfreich zur Bestimmung der technischen Aspekte des Themas sind Vorgaben zum Stand der Technik wie die des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder die „Handreichung zum Stand der Technik“ des Tele-Trust-Vereins (siehe [ct.de/wjdh](https://www.ct.de/wjdh)).

Als praktisches Beispiel für den Stand der Technik hat etwa das Landgericht Würzburg in einer der ersten Entscheidungen zur DSGVO (Az.: 11 O 1741/18 UWG) vom September 2018 ausgeführt, dass beim Erheben von Daten über ein Kontaktformular „zwingend auch eine Verschlüsselung der Homepage erforderlich“ sei. Gemeint ist hier offenbar die SSL/TLS-Verschlüsselung für Websites und insbesondere für Formulare, die laut Gericht stets vorliegen muss.

TOMs: Die technischen und organisatorischen Maßnahmen

Die von dem Verantwortlichen festzulegenden technischen und organisatorischen Maßnahmen (TOM, siehe Seite 50) spielen eine zentrale Rolle



bei der Beurteilung der im Unternehmen vorhandenen IT-Sicherheit. Sie dokumentieren, wie die Daten der Betroffenen konkret geschützt und abgesichert sind. Erreicht werden muss nach Art. 32 DSGVO ein „dem Risiko angemessenes Schutzniveau“.

Dieses wird ermittelt durch eine Schutzbedarfsfeststellung, bei der zunächst die Schutzbedürftigkeit der jeweiligen Daten ermittelt wird. Hierbei betrachtet man insbesondere typische Schadensszenarien und leitet daraus die notwendige Absicherung ab. Hilfreich ist dabei die Einteilung der Daten in Schutzbedarfskategorien. So kennt etwa der BSI-Standard 100-2 die Kategorien „normal“, „hoch“ und „sehr hoch“, an die dann unterschiedliche Anforderungen hinsichtlich des Schutzes zu stellen sind (siehe Seite 128).

Besonders wichtig sind die TOMs, wenn es etwa bei einem Datenverlust zu einem meldepflichtigen Verstoß kommt (siehe Seite 144). Denn dann muss das Unternehmen mithilfe der TOMs und dem Verzeichnis der Verarbeitungstätigkeiten nachweisen, dass es tatsächlich auch angemessene Maßnahmen zum Schutz der jeweiligen vorhandenen Daten getroffen hat. Daher ist auch in diesem Bereich eine ausführliche Dokumentation der getroffenen Maßnahmen im Bereich der IT-Infrastruktur unerlässlich. Fehlte eine solche Dokumentation, so dürfte die Wahrscheinlichkeit eines hohen Bußgeldes für Verstöße gerade bei IT-Unfällen erheblich ansteigen.

Im Hamsterrad der IT-Sicherheit

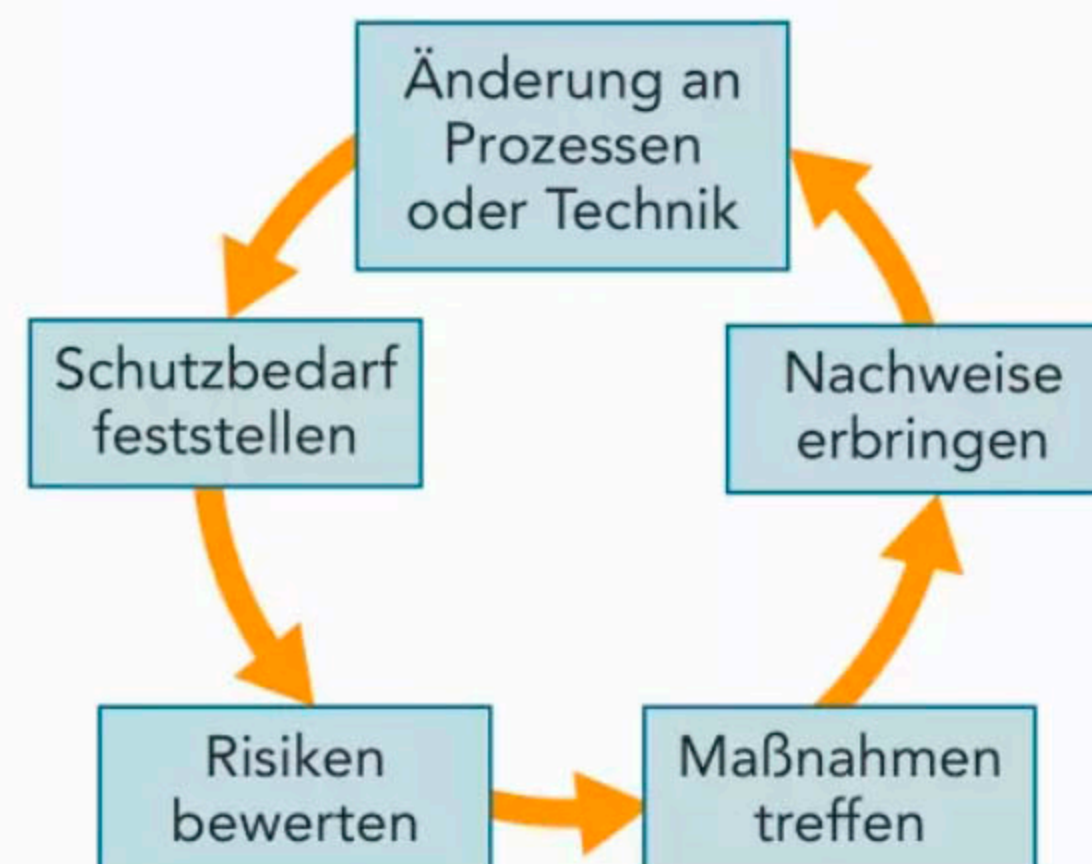
Hieraus ergibt sich für die Verantwortlichen ein niemals endender Kreislauf: Ausgangsbasis ist dabei die Bestandsaufnahme der eigenen Infrastruktur und der vorhandenen Schutzmaßnahmen für die gespeicherten Daten. Dem stellt man die Bewertung der Sensibilität der vorhandenen Informationen entgegen. So haben einfache Kundendaten wie Namen und Postanschrift natürlich einen weitaus niedrigeren Schutzbedarf als die Patientendatenbank eines Onkologen.

Als Ergebnis dieser Risikobewertung ist dann ein Katalog mit den dafür angemessenen technischen und organisatorischen Schutzmaßnahmen zu erstellen und umzusetzen. Wichtig: Das Ergebnis muss stets dokumentiert werden, schon um im Fall eines Databreaches nachweisen zu können, alles Notwendige unternommen zu haben.

Allerdings ist es mit einem solchen einmaligen Prozess nicht getan. Notwendig ist ein Verfahren zur

IT-Sicherheit in der DSGVO

Unternehmen müssen fortlaufend den Schutzbedarf ermitteln und ihre Maßnahmen entsprechend anpassen.



„regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit“ der getroffenen Maßnahmen. Dies bedeutet eine regelmäßige und nachweisbare Überprüfung, je nach Sensibilität der vorgehaltenen Daten auch durch Externe.

In welcher Häufigkeit solche Neubewertungen vorzunehmen sind, steht nicht explizit im Gesetz. Fest steht, dass dies immer bei Einführung wichtiger neuer technischer oder organisatorischer Maßnahmen der Fall ist oder auch bei der Nutzung von neuer sicherheitsrelevanter Hard- und Software. Darüber hinaus dürfte je nach Größe des Unternehmens und der Art der gespeicherten Daten ein Zeitraum zwischen einem Quartal und einem Jahr angemessen sein. Mit jeder Evaluation beginnt dann der Vorgang von Neuem – das Hamsterrad der IT-Sicherheit. (keh) **ct**

Infos zum Stand der Technik:

[ct.de/wjdh](https://www.ct.de/wjdh)

Das Krea-Tief überwinden!

NEU
im heise shop

Auch als
PDF zum
Download!



Mac & i EXTRA Workshops

für Mac und Windows

**ERFOLG
MIT
SOCIAL
MEDIA**

**MÖBEL
ENTWERFEN
IN 3D**

**WORD-
PRESS-
TUNING**

**LOGO
ERSTELLEN**

**KRIMI
SCHREIBEN**

**GOOGLE
OPTIMIERUNG**

**FILM
DREHEN**

**FOTOS
AUFBESSERN**

**WISSENS-
DATEN-
BANK**

TYPOGRAFIE

Mac & i Extra Workshops 2020

In 13 neuen Profi-Workshops zu den Themen Krimi schreiben, Möbel konstruieren, dem eigenen Spielfilm, Bilder verbessern und Vielem mehr, greifen die Autoren den Lesern hilfreich unter die Arme.

Dieses Mac & i Extra ist ein Muss für alle, die kreativ arbeiten und sich ausprobieren wollen.

shop.heise.de/mac-workshops20

10,90 € >

 **heise shop**

shop.heise.de/mac-workshops20 >

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

Risiken richtig abschätzen



Bei der Verarbeitung von personenbezogenen Daten können immer erhebliche Risiken für die Rechte der davon betroffenen natürlichen Personen auftreten, selbst dann, wenn diese grundsätzlich rechtmäßig durchgeführt wird. Um diese Risiken in einem speziellen Projekt oder Verfahren zu erfassen und zu minimieren, enthält die DSGVO das in dieser Form neue Instrument der Datenschutz-Folgenabschätzung.

Von Joerg Heidrich

Die DSGVO basiert in wesentlichen Punkten auf einem risikobasierten Ansatz. Das bedeutet: Ausgehend von der Gefahr, die den Betroffenen durch die Verarbeitung ihrer Daten jeweils droht, ist ein angemessenes Schutzniveau zu ermitteln und technisch und organisatorisch umzusetzen. Ganz praktisch heißt das, dass die Anforderungen an die Sicherheit von Daten mit deren Sensibilität steigt. Bei der Analyse der Risiken und der Festlegung von Risiken spielt die Datenschutz-Folgenabschätzung (DSFA) eine wichtige Rolle. Sie ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken „für die Rechte und Freiheiten der natürlichen Personen“ bei der Verarbeitung ihrer Daten. Hierbei müssen im Rahmen einer der eigentlichen Prüfung vorangestellte Schutzbedarfsfeststellung typische Schadensszenarien und daraus abgeleitet der Schutzbedarf der Daten überprüft und dokumentiert werden.

Wann ist eine DSFA durchzuführen?

Eine DSFA ist nach Art. 35 DSGVO durchzuführen, wenn die Form der Verarbeitung, „insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung“ voraussichtlich ein hohes Risiko zur Folge hat. Auszugehen ist dabei von einzelnen, konkreten Verarbeitungsvorgängen, die auch in den Verarbeitungsverzeichnissen (siehe dazu Seite 42) festzuhalten sind.

Wichtig ist: Es dreht sich dabei nicht um die Risiken des die Daten verarbeitenden Unternehmens oder der Verwaltung, sondern um die der betroffenen natürlichen Personen, deren Daten verarbeitet werden. Konkret ermittelt man die Risiken mit einer sogenannten Schwellwertanalyse vor Beginn der Verarbeitung der Daten oder bei der Planung von neuen Maßnahmen. Kommt man dabei zu dem Ergebnis, dass das geplante Vorhaben mit einem hohen Risiko für die Rechte und Freiheiten dieser Betroffenen verbunden ist, so wird es ernst und es ist vorab eine „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen“.

Kommt man im Rahmen der Schwellwertanalyse zu dem Ergebnis, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, ist die DSFA nicht zwingend erforderlich, schadet aber natürlich auch nicht. In jedem Fall ist nach Vorgabe der Datenschutzbehörden die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA inklusive von Ausführungen zu den maßgeblichen Gründen schriftlich zu dokumentieren.

Typische Risikokategorien

Die inzwischen umgetaufte Art. 29-Datenschutzgruppe der EU hat einfache Kriterien zur Einordnung von Verarbeitungsvorgängen dargelegt, die typische Risikogruppen darstellen. Erfüllt ein Verarbeitungsvorgang zwei oder mehr dieser Kriterien, so wird

Die Aufsichtsbehörden der Länder veröffentlichen Muss-Listen mit Verarbeitungsvorgängen, für die eine DSFA durchzuführen ist, wie in diesem Ausschnitt beispielhaft gezeigt.

7	Verarbeitung von umfangreichen Angaben über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die betroffenen Personen ergeben, oder diese in andere Weise erheblich beeinträchtigen	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Beschäftigten erzeugen Geolokalisierung von Beschäftigten	Zentrale Aufzeichnung des Internetverkehrs und der Aktivitäten am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen. Ein Unternehmen lässt Bewegungsprofile von Beschäftigten erstellen (per RFID, Handy-Ortung oder GPS) zur Sicherung des Personals (Wachpersonal, Feuerwehrleute), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (LKW mit Ladung, Geldtransport) oder zur Koordination von Arbeitseinsätzen im Außendienst.
---	--	---	---

Quelle: Landesbeauftragte für Datenschutz Schleswig-Holstein, ULID

vielfach ein hohes Risiko gegeben sein (siehe Kasten unten). In diesem Fall hat der Verantwortliche eine DSFA durchzuführen.

Allerdings ist diese Liste nicht zwingend. Insbesondere kann es in Einzelfällen auch vorkommen, dass zwar nur eines der genannten Kriterien erfüllt wird und dennoch aufgrund eines hohen Risikos des Verarbeitungsvorgangs eine DSFA notwendig ist. Die DSGVO nennt hier in Art. 35 Abs. 3 beispielsweise die „systematische umfangreiche Überwachung öffent-

lich zugänglicher Bereiche“ – also Videoüberwachung in großem Stil (siehe auch Seite 82). Gerade in diesem Bereich der Videoüberwachung kam es in Österreich zu dem ersten bekannten Bußgeld aufgrund eines Verstoßes gegen das neue Datenschutzrecht. Seitdem gibt es solche Strafen in diesem Bereich in schöner Regelmäßigkeit.

Ebenfalls notwendig ist eine Folgenabschätzung bei der Nutzung von besonderen personenbezogenen Daten, die in großem Umfang verarbeitet wer-

Risikokategorien zur Durchführung einer DSFA

- Bewerten oder Einstufen von Personen, z. B. im Rahmen von Scoring oder Profiling
- Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- Systematische Überwachung
- Vertrauliche oder höchstpersönliche Daten, z. B. Verwendung von besonderen personenbezogenen Daten im Sinne von Art. 9 DSGVO
- Datenverarbeitung in großem Umfang
- Abgleichen oder Zusammenführen von Datensätzen
- Daten zu schutzbedürftigen betroffenen Personen, z. B. von Arbeitnehmern oder Kindern
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen, z. B. Biometrie
- Betroffene Personen werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert



den oder beim Zusammenführen und Kombinieren von Daten, etwa bei Big-Data-Prozessen. Je größer der Umfang der verarbeiteten Daten auf der einen und das Risiko für die Betroffenen auf der anderen Seite, desto wahrscheinlicher ist die Erforderlichkeit dieser Einschätzung.

Die Muss-Liste

Die Aufsichtsbehörden haben ferner Muss-Listen mit Beispielen veröffentlicht, bei denen zwingend eine Datenschutz-Folgenabschätzung durchzuführen ist (siehe [ct.de/w37z](https://www.ct.de/w37z)).

Eine DSFA durchführen

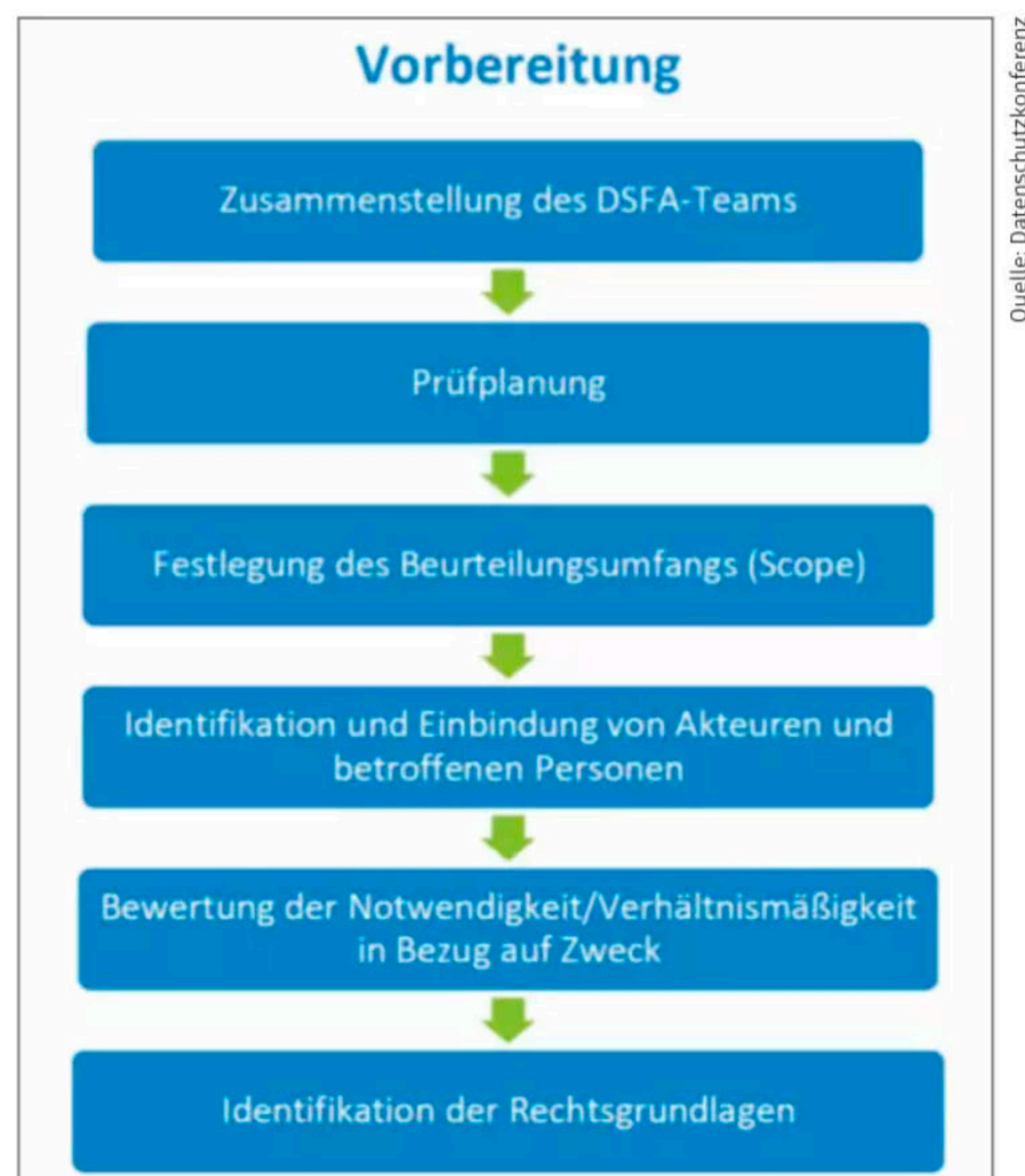
Eine DSFA führt man idealerweise in einem interdisziplinären Team durch, in dem neben Juristen und Technikern auch die jeweiligen Fachabteilungen und natürlich der zuständige Datenschutzbeauftragte beteiligt sind. Inhaltlich identifiziert man im ersten Schritt die Risikoquelle und bestimmt die damit verbundenen Eintrittswahrscheinlichkeiten. Für die so ermittelten Risiken muss man geeignete Abhilfemaßnahmen finden und auf den jeweiligen Sachverhalt anpassen.

Die zu treffenden Maßnahmen können dabei technischer oder organisatorischer Art sein. So können Risiken bei Daten etwa dadurch minimiert werden, dass Daten pseudonymisiert oder verschlüsselt werden oder man den Zugriff auf sie technisch oder physikalisch beschränkt.

Eine solche Folgenabschätzung ist in vielen Fällen gerade im technischen Bereich aufwendig und kann von einem Mehrseiter bis hin zum Umfang eines Wälzers von Buddenbrooks-Format. Diese Dokumentationen müssen den jeweiligen Aufsichtsbehörden, also den Datenschützern der Länder, spätestens dann vorgelegt werden, wenn es zu einem Verstoß gegen die Gebote des Datenschutzes gekommen ist. Hat man dann keine derartige Abschätzung vorzuweisen, so dürfte als Folge ein empfindliches Bußgeld drohen.

Dauerhafter Prozess

Die Überwachung des Risikos bei der Verarbeitung personenbezogener Daten ist ein dauerhafter Prozess, der keinesfalls mit der Erstellung von technischen und organisatorischen Maßnahmen (TOMs) und der Durchführung von ein paar kurzen DSFA abgeschlossen ist. Bei größeren Unternehmen ist zur



Bereits die Vorbereitung einer Datenschutz-Folgenabschätzung erfordert mehrere Schritte.

Überwachung dieser Prozesse die Einführung eines Datenschutzmanagementsystems unumgänglich.

Kommt man bei der Überwachung der laufenden oder neuen Prozesse zu dem Ergebnis, dass sich das daraus resultierende Risiko für die betroffenen natürlichen Personen ändert, so ist nämlich erneut eine DSFA durchzuführen und die Ergebnisse müssen erneut dokumentiert werden. Dies kann sich zum Beispiel ergeben, wenn in einen bestehenden Prozess neue Arten von Daten hinzukommen oder der Umfang der Verarbeitung erheblich ausgeweitet wird.

Zu hohes Risiko

Kommen die Verantwortlichen bei einer DSFA zu dem Ergebnis, dass die geplante Datenverarbeitung ein zu hohes Risiko für die Betroffenen beinhaltet und dies auch nicht mit wirksamen technischen und organisatorischen Maßnahmen einzugrenzen ist, so müssen sie gemäß Art. 36 DSGVO die Aufsichtsbehörde konsultieren. Diese untersucht dann die geplanten Vorhaben. Erkennt sie dabei, dass die geplante Verarbeitung nicht gesetzeskonform und

hinlänglich sicher ist, unterbreitet sie dem Verantwortlichen innerhalb eines Zeitraums von im Normalfall bis zu acht Wochen nach der Anfrage schriftliche Empfehlungen. Weiterhin kann sie ihre in Art. 58 DSGVO genannten, weitreichenden Befugnisse ausüben. Hierunter fallen eine vorübergehende oder endgültige Beschränkung oder gar ein Verbot der geplanten Verarbeitung.

Praktisch bedeutet dies: Findet man bei der DSFA erhebliche Risiken für die Betroffenen, aber keine geeigneten technischen oder organisatorischen Maßnahmen, stoppt das Projekt ganz oder zumindest in den betroffenen Teilen, bis die Aufsichtsbehörde über den weiteren Fortgang entschieden hat. Diese unterbreitet dann nach zwei Monaten oder auch einem längeren Zeitraum einen Vorschlag zur weiteren Durchführung des Projekts. Inwieweit diese Vorgehensweise nicht zuletzt angesichts der in vielen

Bundesländern äußerst dünnen Personaldecke der Datenschutzbehörden realistisch ist, bleibt abzuwarten.

Riskante Ignoranz

Die Datenschutz-Folgenabschätzung ist eines der zentralen Elemente des risikobasierten Ansatzes der DSGVO und wohl in dieser Form auch eine der wichtigsten Neuerungen. In der Praxis wird sie vor allem jenseits der großen Unternehmen häufig noch weitgehend ignoriert. Dies wird sich spätestens dann rächen, wenn innerhalb eines Meldeprozesses, zum Beispiel bei einer Datenpanne, auf Nachfrage der Behörden keine Dokumentation von offensichtlich notwendigen DSFAs vorgelegt werden kann. Gerade in diesem Bereich sind hohe Bußgelder mehr als wahrscheinlich. (keh) **ct**

Orientierungshilfen
und Software zur
DSFA:

ct.de/w37z



24. – 25. März 2021

ONLINE

- Die Konferenz zum Internet der Dinge erstmals online
- Alle Vorträge im Livestream
- Videos und Präsentationen im Nachgang verfügbar
- Video- und Textchat für individuelle Fragen

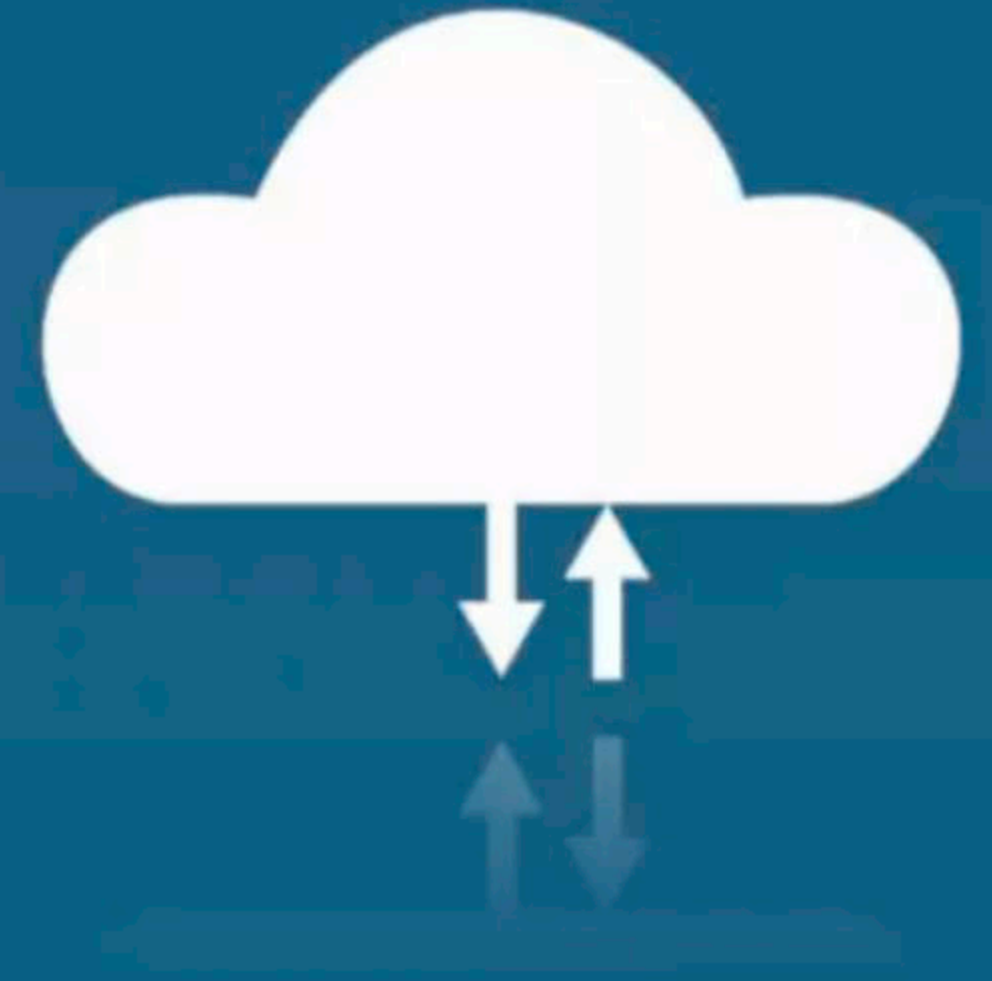
www.buildingiot.de



@ heise Developer

dpunkt.verlag

Cloud Computing beim Dienstleister



Viele Unternehmen verwenden Cloud-Lösungen. Wer beim Hosting oder bei der Verarbeitung von Daten auf die Unterstützung von Cloud-Computing-Anbietern setzt, muss dabei einige rechtliche Vorgaben beachten. Auch die Cloud-Dienstleister selbst haben dabei Rechte und Pflichten.

Von Joerg Heidrich

Daten auf fremde Rechner zu transferieren, die irgendwo im Ausland stehen und bei denen man bisweilen nicht einmal genau weiß, wem sie gehören und wer dafür verantwortlich ist, ist eine Technik, die vor allem den Juristen unter den Datenschützern nicht sehr geheuer ist. Allerdings liegt es auf der anderen Seite nahe, dass Informationen auf den gut geschützten Cloud-Rechnern großer oder spezialisierter Anbieter zumindest sicherer liegen dürften als auf den Servern von kleinen Unternehmen oder Freiberuflern ohne eigene IT-Abteilungen. Auch um dies zu gewährleisten, stellen die DSGVO und das BDSG bei der Verlagerung personenbezogener Daten in die Cloud besondere Anforderungen an die Sicherheitsvorkehrungen.

Für Anbieter sowie Nutzer von Cloud-Angeboten bringt die DSGVO gleich mehrere entscheidende Änderungen mit sich. Sie betreffen das Auswählen eines Dienstleisters ebenso wie das Abschließen von Verträgen. Hier können DSGVO-konforme Zertifizierungen bei der Entscheidung für einen Anbieter helfen, die für die nächste Zeit angekündigt sind. Rechtlich bedeutsam ist ebenfalls die Mithaftung des Cloud-Hosters bei Datenpannen, die auch direkt gegenüber den einzelnen Betroffenen besteht. Ein großes Problem für die gesamte Branche dürfte allerdings in den strengen Löschanforderungen lie-

gen, die in der Praxis gerade in der Cloud nur schwer umzusetzen sein werden.

Auswahlkriterien für Cloud-Anbieter

Juristisch wird das Verarbeiten von Daten in der Cloud als Auftragsverarbeitung eingestuft (siehe Seite 56). Typischerweise setzt der Auftraggeber für die Verarbeitung auf Dienstleister, kontrolliert jedoch die Nutzung der Daten weitgehend selbst und verantwortet sie auch.

Die Voraussetzungen für ein solches Verfahren finden sich in Art. 28 DSGVO. Diesem zufolge darf man nur mit solchen Cloud-Anbietern zusammenarbeiten, die „hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“

Die technischen und organisatorischen Anforderungen an den Cloud-Anbieter sind dabei hoch. So muss er unter anderem unter Berücksichtigung des Stands der Technik und der Schwere des Risikos für die Rechte und Freiheiten der betroffenen natürlichen Personen „geeignete technische und organi-

satorische Maßnahmen“ ergreifen. Ziel ist ein dem jeweiligen Risiko der Datenverarbeitung angemessenes Schutzniveau.

Um diesen Anforderungen zu entsprechen, ist vorab das Risiko zu bestimmen, das durch das Weitergeben der jeweiligen Daten in die Cloud entsteht (siehe S. 128). Entscheidend ist dabei die Perspektive: Das Risiko bestimmt sich nämlich nicht wie bisher aus der Sicht des Auftraggebers und dessen IT-Sicherheit, sondern aus der der betroffenen natürlichen Personen.

Folglich erhöhen sich die Anforderungen an die IT-Sicherheit in den Fällen ganz erheblich, in denen vertrauliche oder besonders geschützte personenbezogene Daten in der Cloud gespeichert werden sollen. Dabei kann es im Einzelfall sogar möglich sein, dass ein Verlagern dieser Informationen bei einem besonders hohen Risiko für die Betroffenen gar nicht zulässig ist. Auf der anderen Seite sind die technischen Anforderungen bei der Verarbeitung von beispielsweise reinen Adressdaten, die auch öffentlich vorhanden sind, erheblich niedriger.

Spezialverträge für Auftragsverarbeitung

Wie in allen anderen Bereichen des Datenschutzes wird durch die DSGVO die IT-Sicherheit bei der Datenverarbeitung in der Cloud ein elementarer Bestandteil des Umgangs mit vertraulichen Informationen. Hieraus resultieren aktive Prüf- und Kontrollpflichten für den Auftraggeber bei seinem Dienstleister. Neben den Vorgaben der IT-Sicherheit muss er sich unter anderem auch darüber informieren, ob eine Datenübermittlung in Staaten außerhalb der EU vorgesehen ist und wie in diesem Fall das erforderliche Datenschutzniveau eingehalten werden soll (siehe Seite 116). Schließlich muss der Cloud-Hoster den Auftraggeber explizit informieren, wenn er Subunternehmen und weitere Auftragsverarbeiter einsetzt.

Die hierfür notwendigen Vereinbarungen müssen in einem gesonderten Dokument festgehalten werden, dem Auftragsverarbeitungsvertrag (siehe Seite 56). Dieser definiert unter anderem ausführlich die Pflichten des Cloud-Anbieters, dessen Haftung sowie den Einsatz von Subunternehmen. Auch die technischen und organisatorischen Maßnahmen

können im Detail angegeben werden. Muster für solche Vertragszusätze sind im Internet vielfach erhältlich, beispielsweise von Branchenverbänden wie Bitkom oder Datenschutzvereinigungen wie der GDD.

Das goldene Zeitalter der Zertifizierung

In der Regel ist es für einen Auftraggeber schwer möglich, tatsächlich die technischen und organisatorischen Sicherheitsmaßnahmen seines Dienstleisters zu überprüfen. Um hier mehr Sicherheit für den Auftraggeber zu erreichen, setzt die DSGVO verstärkt auf Zertifizierungsverfahren. So kann im Cloud-

Bereich die Einhaltung eines genehmigten Zertifizierungsverfahrens ein entscheidender Faktor für den Nachweis von ausreichendem Datenschutz und hinreichender IT-Sicherheit auf Seiten des Anbieters sein und entsprechende detaillierte Unterlagen ersetzen.

Es ist also zu erwarten, dass solche Gütesiegel im gesamten IT-Bereich erheblich an Bedeutung gewinnen werden. Speziell für Cloud-Angebote gibt es bereits eine Fülle an Zertifizierungsverfahren. Zu den bekannten zählen das Gütesiegel SaaS von Euro-Cloud, CSA STAR oder

TÜV Trust IT. Die bisherigen Zertifizierungen bezogen sich allerdings nicht unmittelbar auf die Anforderungen der DSGVO. Allerdings wird wohl der Markt in absehbarer Zeit auch geeignete und angemessene Zertifizierungen für Cloud-Hoster anbieten.

Verschiebung der Verantwortung

Früher sah Paragraph 11 des Bundesdatenschutzgesetzes (BDSG-alt) den Auftraggeber nach außen als allein verantwortliche Stelle für die von ihm initiierte Datennutzung vor. Dies galt sogar dann, wenn der Cloud-Dienstleister sich rechtswidrig verhielt oder gegen Weisungen verstieß. Eine wesentliche Neuerung der DSGVO im Bereich der Cloud-Dienste ist die Ausweitung der Verantwortlichkeiten für die Rechtmäßigkeit der Datenverarbeitung und der daraus entstehenden Schäden auf den Hoster. Dieser haftet nach Artikel 82 DSGVO gemeinsam mit dem Verantwortlichen gegenüber den Betroffenen für materielle sowie immaterielle Schäden, also beispielsweise auch für Schmerzensgeld.





I. Kategorisierung der Daten

- Festlegung, welche Daten in die Cloud gestellt werden sollen:
Einteilung beispielsweise in: kein Personenbezug / Personenbezug / besondere Kategorien von personenbezogenen Daten
- Festlegung der Dauer der Speicherung:
nur vorübergehend / dauerhaft / zu Archivierungszwecken
Je länger die Speicherung erfolgt, desto höher sind die Anforderungen an die IT-Sicherheit.
- Anzahl der übertragenen Datensätze:
Je größer die Datenmenge, desto höher sind die Anforderungen etwa an die IT-Sicherheit und die Datenschutzorganisation.
- Festlegen eines Löschkonzepts



II. Auswahl des Cloud-Anbieters und -Modells

- Festlegung des Cloud-Modells
Einteilung On-Premise / private / private-public / public
- Auswahl des Cloud-Anbieters
Art. 32 DSGVO stellt hohe Anforderungen an die Technikgestaltung. Danach sind bei der Bewertung der zu ergreifenden Maßnahmen folgende Umstände zu berücksichtigen:
Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Auf Basis dieser Analyse sollten der Verantwortliche und der Auftragsverarbeiter „geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Als mögliche technische und organisatorische Maßnahmen nennt die DSGVO etwa: Verschlüsselung, Pseudonymisierung, Löschkonzept, Wiederherstellungskonzepte / Backups, Evaluierungsverfahren zur Wirksamkeit der getroffenen Maßnahmen
- Dokumentation der getroffenen Maßnahmen



III. Physikalischer Standort der Server

- unproblematisch: innerhalb Deutschlands / innerhalb der EU / innerhalb der sicher klassifizierten Drittstaaten (u. a. Japan, Argentinien, Kanada, Israel, Neuseeland, Schweiz, Uruguay)
- Ein Datenexport auf Server in den USA ist nur sehr eingeschränkt erlaubt (siehe Seite 116).
- Erforderlich: Zustimmung aller Betroffenen / Vereinbarung von vorgegebenen Vertragsklauseln (EU-Standardvertragsklauseln) mit ergänzenden technischen und organisatorischen Maßnahmen / Sonderregelungen bei Datenweitergabe in Konzernen.



IV. Vertragliche Vereinbarung

- wichtig unter anderem: SLA-Agreement und – bei ausländischen Unternehmen – Gerichtsstand und Rechtswahl



V. Auftragsverarbeitung

- Es muss ein zusätzlicher Vertrag zur Auftragsverarbeitung zwischen den Parteien geschlossen werden. Im Rahmen dieses Vertrags hat der Cloud-Anbieter unter anderem die von ihm getroffenen technischen und organisatorischen Maßnahmen (TOM) darzulegen.



VI. Durchführung einer Datenschutzfolgenabschätzung

- Bei umfangreichen oder potenziell riskanten Datenverarbeitungen muss bereits im Vorfeld geprüft werden, ob ein besonderes Risiko für die Rechte der Betroffenen besteht. Die Datenschutzfolgenabschätzung (DSFA) ist eine Bestandsaufnahme, auf deren Basis beurteilt werden kann, ob die geplante Nutzung der personenbezogenen Daten zulässig ist. Vor Durchführung umfangreicher Cloud-Projekte wird meist eine solche Abschätzung durchzuführen sein.

Dies ist insofern bemerkenswert, als dass es sich bei Kunden oder Mitarbeitern des Auftraggebers um Personen handelt, mit denen der Cloud-Anbieter im Normalfall selbst keine vertragliche Beziehung hat und die er nicht einmal kennt. Dennoch kann eine betroffene Person nach Art. 79 DSGVO nun rechtlich gesehen auch direkt gegen den Auftragsverarbeiter vorgehen, wenn sie der Ansicht ist, dass „die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden“. Die Verantwortung des Cloud-Anbieters erhöht sich damit gegenüber den Regelungen des BDSG-alt enorm.

Dies gilt etwa für Schadensersatzzahlungen bei massenhaften Rechtsverletzungen, die je nach Anzahl der Betroffenen leicht auch schwindelerregende Höhen erreichen können (siehe Seite 72).

Löschen von Daten

Die Pflichten zum Löschen von Daten werden durch die DSGVO erheblich erweitert (siehe Seite 32), was vor allem die Nutzer von Cloud-Angeboten vor große Probleme stellen wird. Grundsätzlich müssen nach Art. 17 DSGVO personenbezogene Informationen unverzüglich gelöscht werden, wenn der Zweck für ihre Nutzung entfallen ist, der Betroffene eine erteilte Einwilligung widerruft oder die Nutzung der Daten zu Unrecht erfolgt ist. Ausnahmen von diesen Verpflichtungen sieht das Gesetz in Fällen vor, in denen ein übergeordnetes Interesse am Vorhalten der Daten besteht, etwa bei der Ausübung des Rechts auf Presse- oder Meinungsfreiheit oder zu Zwecken der Forschung.

Es gehört damit zu den zentralen Aufgaben in Unternehmen, Löschkonzepte zu entwickeln, die festlegen, wann welche Informationen zu entsorgen sind. Die maximalen Aufbewahrungsfristen für die einzelnen Daten zu bemessen, kann im Einzelfall äußerst kompliziert sein. Dies gilt umso mehr, wenn Löschpflichten mit Verpflichtungen zur Aufbewahrung kollidieren, etwa im Bereich der E-Mail-Archivierung. Art. 17 DSGVO verlangt auch die Löschung von Datenkopien sowie von Links auf Daten und Kopien. Dies dürfte nicht nur für langfristige Backups schwierig werden, gerade in der Cloud.

Natürlich gelten diese Verpflichtungen auch für das rückstandslose Entfernen personenbezogener

Daten aus Cloud-Angeboten, also aus einem System, das mangels Transparenz nur bedingt darauf eingerichtet ist. Viele Unternehmen wissen überhaupt nicht, wohin die zu löschenden Daten physisch übertragen worden sind. Die Ausarbeitung belastbarer Löschkonzepte dürfte daher zu den dringendsten Aufgaben von Cloud-Anbietern und ihren Kunden gehören.

Dabei stellt sich auch die Frage, wie Daten in der Cloud überhaupt rechtssicher gelöscht werden können. Da eine physische Vernichtung der Datenträger in aller Regel auszuschließen ist, bliebe allenfalls ein Überschreiben gemäß den Vorgaben des BSI. Es darf allerdings bezweifelt werden, ob sich gerade internationale Unternehmen diesen rigiden Vorgaben anschließen.

Ob ein Verschlüsseln von Daten in der Cloud bei gleichzeitigem Vernichten des Schlüssels einem

Löschen der Daten entspricht, wird derzeit in Fachkreisen diskutiert. Das wäre ein recht eleganter Weg, den Anforderungen des Art. 17 DSGVO zu genügen. Dabei wird dergestalt argumentiert, dass Daten ohne den Schlüssel nicht mehr oder nur mit erheblichem Aufwand wiederhergestellt werden können und daher als gelöscht angesehen werden dürfen. Dieser Ansicht halten Kritiker des Konzepts, vor allem aus den Reihen der Datenschutzbehörden, entgegen, dass es nur eine Frage der Zeit sei, bis neue, wirkungsvolle Rechner die bisherige Verschlüsselung knacken könnten.

Schließlich spielt auch der Standort der Server der Cloud eine große Rolle bei der Auswahl eines Anbieters. Sofern die Rechner in Deutschland oder innerhalb des Gebiets der Europäischen Union stehen, gibt es keine Besonderheiten. Dies ändert sich aber dann, wenn die Informationen in Staaten außerhalb der EU exportiert werden, insbesondere in die USA. Dies ist zwar rechtlich nicht ausgeschlossen, es gilt jedoch eine Reihe von zusätzlichen Anforderungen zu beachten (siehe Seite 116). (keh) **ct**



**Umsetzungshinweise
Cloud Computing:**

[ct.de/wa75](https://www.ct.de/wa75)

Daten rechtssicher löschen



Daten nicht nur zu erfassen, zu verarbeiten und weiterzugeben, sondern diese auch rechtskonform zu löschen, ist eine der großen Herausforderungen der DSGVO. Solche Verpflichtungen können auf „Zuruf“ des Betroffenen ebenso entstehen wie durch Zeitablauf gesetzlicher Speicher- und Aufbewahrungspflichten.

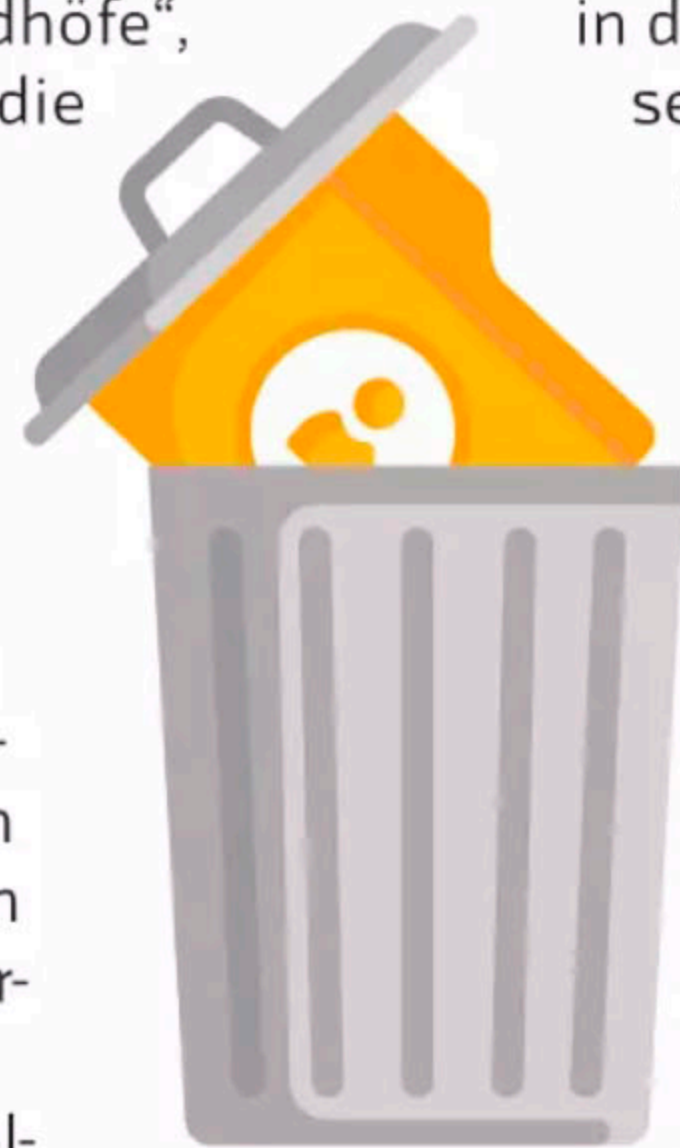
Von Joerg Heidrich

Die Datenschutzbeauftragte Berlins, Maja Smoltczyk, nennt sie „Datenfriedhöfe“, die Sammlungen von Daten, die eigentlich nie erfasst oder zumindest längst gelöscht gehören. Die Brisanz solcher Missstände wird immer dann offensichtlich, wenn es „etwa durch Cyberangriffe zu missbräuchlichen Zugriffen auf die massenhaft gehorteten Daten gekommen ist“. Doch auch ohne solche schwerwiegenden Folgen können bei derartigen Sammlungen drastische Verstöße gegen die Grundsätze des Datenschutzes vorliegen.

Wie eklatant die Berliner Behörde solche Fehler einschätzt, zeigte sich jüngst im Fall des Bußgeldbescheids gegen den Immobilienkonzern Deutsche Wohnen SE. Nicht weniger als die Zahlung von 14,5 Millionen Euro verlangt das Amt von dem Unternehmen. Anlass dafür ist unter anderem die Tatsache, dass für die Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendet wurde, welches keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen.

Teure Datenfriedhöfe

Der Fall aus Berlin ist exemplarisch für die Probleme, die viele Unternehmen bei der Speicherung von



Daten immer noch haben. Dabei hat sich auch in diesem Bereich durch die europäische Gesetzgebung nicht viel verändert – Löschanprüche und -pflichten kannte auch schon das alte BDSG. Die DSGVO regelt diese Problematik schwerpunktmäßig in Art. 17. Danach hat der Betroffene ein Recht auf Löschung, wenn die Speicherung seiner Daten gegen die DSGVO oder anderes Recht verstößt, dem der Verantwortliche für das Vorhalten der Informationen unterliegt. Insbesondere hat er einen Anspruch darauf, dass seine personenbezogenen Daten gelöscht und nicht mehr verarbeitet werden, wenn diese für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden. Gleiches gilt für die Fälle, in denen der Betroffene seine Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Nutzung der Daten eingelegt hat.

Löschen auf Zuruf

Auf dieser Basis müssen zwei unterschiedliche Pflichten zur Löschung von Daten unterschieden werden: Das Löschen „auf Zuruf“ durch den Betroffenen auf der einen und durch Wegfall des Rechtsgrunds auf der anderen Seite. Im ersten Fall wendet sich eine Privatperson an die Stelle, die seine Daten speichert und verlangt die Löschung dieser Angaben.

Faktisch und rechtlich unproblematisch ist dies in den Fällen, in denen der Betroffene zuvor eine Einwilligung erteilt hat, die er nun widerruft. Dies gilt beispielsweise für solche Informationen, die ein Website-Betreiber im Rahmen eines Newsletter-Versands oder der Anmeldung zu einem kostenlosen Forum mitgeteilt hat. Diese Daten müssen von dem Verantwortlichen zeitnah und restlos gelöscht werden. Praktische Voraussetzung zur Umsetzung dieser Vorgaben ist natürlich eine IT-Infrastruktur, die eine solche Löschung auch ermöglicht.

Löschen nach Zeitablauf

Auf der anderen Seite sind Daten auch dann zu löschen, wenn die Rechtsgrundlage für ihre Speicherung wegfällt – und zwar automatisch und ohne Aufforderung durch den Betroffenen. Hierfür sind entsprechende Löschkonzepte unumgänglich. Häufigster Fall hierbei ist die Aufbewahrungspflicht auf Basis gesetzlicher Vorgaben, etwa für Handelsbriefe, Rechnungen oder geschäftsrelevante E-Mails. Die unterschiedlichen Längen für das Vor-

halten der Unterlagen dauern dabei von sechs bis zu 30 Jahren, etwa im Bereich der Fertigung von Röntgenaufnahmen (siehe Tabelle S. 138: Verzeichnis der wichtigsten Aufbewahrungsfristen). Die Aufbewahrungsfristen beginnen mit dem Ende des Kalenderjahres, in dem das Dokument erstellt oder empfangen worden ist und enden nach Ablauf der Frist mit dem Ende des Kalenderjahres. Größere „Löschorgien“ bieten sich daher zum Jahresende an.

Höchst problematisch wird es, wenn Löschwünsche und Speicherpflichten zusammentreffen. In der Praxis führt dies häufig zu Konflikten, wenn ein Unternehmen einem Kunden erklären muss, dass es seine Daten zwar gerne löschen möchte, dies aber auf Basis von gesetzlichen Aufbewahrungsvorschriften, etwa aus der Abgabenordnung (AO), nicht darf. Hier bleibt meist nur, dem Kunden geduldig die Rechtslage zu erklären. Gleiches gilt auch für die Ausnahmen der Löschpflichten, welche die DSGVO festlegt (siehe Kasten unten).

Backups und Archive

Große Probleme gibt es in der Praxis regelmäßig dann, wenn sich die zu löschenden Daten zusätzlich in Backups oder Archiven befinden. Tatsächlich kennt die DSGVO hier keine Sonderregelung für diese Arten der Speicherung. Das bedeutet: Grundsätzlich sind auch personenbezogene Daten aus solchen Sammlungen zu löschen. Dieses Vorgehen muss zentraler Bestandteil eines Löschkonzepts sein, welches die Entfernung der Informationen regelt.

Schwierig bis kaum möglich stellt sich dies allerdings beim „Löschen auf Zuruf“ dar. Denn vor allem Archive sehen überhaupt keine Möglichkeiten für ein vorzeitiges Entfernen einzelner Datensätze vor. Zudem gibt es hier auch einen Konflikt mit den gesetzlichen Anforderungen zur Archivierung, die zum Beispiel im Rahmen der Abgabenordnung (AO) gefordert wird. Erleichterungen kennt das Gesetz hier nur für den Bereich der „nicht automatisierten Datenverarbeitung“, also für die händische Sortierung. Im Normalfall überwiegt die Pflicht zur Führung eines vollständigen Archivs die Löschfristen, so dass eine Löschung erst nach Fristablauf zu erfolgen hat. Hier bleibt aber erhebliche Rechtsunsicherheit, so dass die Entscheidungen der Gerichte abgewartet werden müssen.

Auch bei der Löschung aus Backups gibt es keine gesonderte Regelung. Hier sieht allerdings Art. 32

Ausnahmen von den Löschpflichten

Art. 17 Absatz 3 DSGVO und Erwägungsgrund 65 nennen einige Ausnahmen von den Löschpflichten. Danach dürfen Daten erhalten bleiben, soweit deren Verarbeitung erforderlich ist:

- Für die Ausübung des Rechts auf freie Meinungsäußerung und Information
- Zur Erfüllung einer rechtlichen Verpflichtung
- Für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde
- Aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke
- Zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken
- Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

DSGVO vor, dass Unternehmen „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“ aufweisen müssen. Dies stellt de facto eine Verpflichtung zur Durchführung von Backups dar, die der Löschpflicht gegenübersteht.

Hieraus lässt sich die Möglichkeit ableiten, löschpflichtige Daten zumindest über einen gewissen Zeitraum weiter speichern zu dürfen, um den IT-Pflichten des Unternehmens zu genügen. Wie lange diese Frist dauert, ist noch völlig offen, viele Monate oder gar Jahre erfasst sie sicher nicht. Eine Frist über einige Wochen bis zur Löschung dürfte damit allerdings zu rechtfertigen sein. Auch wenn die DSGVO im Gegensatz zu der alten Rechtslage dies nicht explizit vorsieht, sollten die zur Löschung vorgesehen Daten zwingend markiert und soweit möglich für eine weitere Nutzung gesperrt werden.

Was ist eigentlich Löschen?

Eine Definition des Begriffs „Löschen“ kennt die DSGVO nicht. Sie unterscheidet aber in Art. 4 Abs. 2 zwischen Löschen und Vernichtung. Entscheidend ist, dass die Verarbeitung und Nutzung der personenbezogenen Daten der betroffenen Person nicht mehr möglich und der Prozess auch nicht revidierbar ist. Dies ist unzweifelhaft der Fall, wenn der entsprechende Datenträger physisch zerstört wird oder die Informationen auf Datenträgern dauerhaft gelöscht werden, zum Beispiel durch entsprechende Software.

Nach einer Entscheidung der Datenschutzbehörde Österreichs (GZ: DSB-D123.270/0009-DSB/2018 vom 5.12.2018) steht dem Verantwortlichen hinsichtlich der Mittel, also der Art und Weise der Löschung, ein Auswahlermessen zu. Soweit sichergestellt wird, dass „weder der Verantwortliche selbst noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann“, reiche auch eine Entfernung des Personenbezugs („Anonymisierung“).

Daher war es in dem behandelten Fall zulässig, die Daten eines Betroffenen durch die eines „Dummy Kunden“ zu ersetzen. Im nächsten Schritt wurde diese Attrappe mit einem weiteren, nicht zuordenbaren Eintrag zusammengelegt, wodurch auch der Änderungsverlauf nachhaltig nicht mehr rekonstruierbar ist. Diese Entfernung des Personenbezugs stelle bereits eine Löschung dar.

Fazit

Nicht nur der Fall der Deutschen Wohnen zeigt, dass die rechtskonforme Löschung von Daten einen zentralen Punkt der DSGVO darstellt und Fehler in diesem Bereich mit hohen Bußgeldern belegt werden können. Daher ist es unerlässlich, ein Löschkonzept vorzuhalten, dass sowohl die Datenentfernung nach Wegfall der Rechtsgrundlage, aber auch das Löschen auf Zuruf beinhaltet. (keh) 

Gesetzliche Aufbewahrungspflichten (Auswahl)	
Abrechnungsbelege	10 Jahre
An-, Ab- und Ummeldungen der Krankenkassen	6 Jahre
Angebotsunterlagen, die zum Auftrag geführt haben	6 Jahre
Arbeitsunfähigkeitsbescheinigungen (Krankmeldung)	5 Jahre
Ausgangsrechnungen	10 Jahre
Bankauszüge, Bankbelege	10 Jahre
Beitragsabrechnungen zur Sozialversicherung	10 Jahre
Bewertungsunterlagen	10 Jahre
Bilanzen	10 Jahre
Buchungsanweisungen, Buchungsbelege	10 Jahre
Debitorenbuchhaltung, Debitorenlisten	10 Jahre
E-Mails mit steuerrelevantem Inhalt	10 Jahre
Eingangsrechnungen	10 Jahre
Frachtbriefe	6 Jahre
Gehaltslisten	10 Jahre
Geschäftsberichte	10 Jahre
Geschäftsbriefe	6 Jahre
Gewinn- und Verlustrechnungen	10 Jahre
Handelsbriefe	6 Jahre
Inventare, Inventarnachweise	10 Jahre
Jahresabschluss	10 Jahre
Kontoauszüge, Kontenregister	10 Jahre
Kreditorenbuchhaltung	10 Jahre
Lohnlisten	10 Jahre
Lohnsteuer-Jahresausgleichsunterlagen für Mitarbeiter	10 Jahre
Quittungen, wenn Buchungsunterlagen	10 Jahre
Rechnungen und Rechnungsunterlagen	10 Jahre
Reisekostenabrechnungen	10 Jahre
Schriftwechsel	6 Jahre
Schriftwechsel innerhalb des Unternehmens	6 Jahre
Steuerunterlagen	10 Jahre
Versand- und Frachtunterlagen	10 Jahre
Werbekostenbelege	10 Jahre



Gute Aussichten für Fotobegeisterte.

Sparen Sie 35% und sammeln wertvolles Know-how:

- **2 Ausgaben** kompaktes Profiwissen für 14,60 € (Preis in DE)
- **Workshops und Tutorials**
- **Tests und Vergleiche** aktueller Geräte



Inklusive Geschenk nach Wahl

z. B. Kamera-Reinigungsset

Jetzt bestellen:

www.ct-foto.de/miniabo

ct Fotografie

☎ +49 541/80 009 120

✉ leserservice@heise.de

Backup und Archivierung

Das Verarbeiten und Speichern der Daten von Kunden und Mitarbeitern ist für Unternehmen essenziell. Dem Wunsch, auch persönliche Informationen beliebig lange zu speichern und lückenlos auszuwerten, stehen jedoch die strengen Vorgaben des Datenschutzes entgegen. Um sie einzuhalten, braucht man rechtssichere Speicher-, Backup- und Löschkonzepte. Die dabei entstehenden Probleme zeigen sich exemplarisch an den Pflichten zur Archivierung von E-Mails.

Von Joerg Heidrich

Sei es als vorübergehendes Backup von Logfiles oder als Langzeitspeicherung wie bei der E-Mail-Archivierung: Die Sicherung von Daten ist für Unternehmen in vielen Bereichen nicht nur sinnvoll, sondern sogar rechtlich zwingend vorgeschrieben. Allerdings hat diese „private Vorratsdatenspeicherung“ auch rechtliche Grenzen. Diese beziehen sich sowohl darauf, was gespeichert werden soll und muss, als auch vor allem auf die Frage, wie lange die Informationen auf den eigenen Systemen vorgehalten werden dürfen.

Rechtliche Vorgaben gibt es vor allem bei personenbezogenen Daten wie Informationen über Endkunden und die eigenen Mitarbeiter sowie bei E-Mails. Informationen ohne Personenbezug wie technische Daten, Konstruktionspläne oder Maschinenauswertungen kann man dagegen aus juristischer Sicht in den allermeisten Fällen unbeschränkt speichern und vorhalten. Allerdings können sich auch in solchen Archiven Löschpflichten verstecken, etwa wenn Lizenzvereinbarungen auslaufen oder nach Vertragsende Daten eines Vertragspartners zwingend gelöscht werden müssen.

Erlaubnis benötigt

Handelt es sich aber um personenbezogene Daten – dafür reichen auch einzelne Informationen in einer

größeren Datensammlung –, sind die rechtlichen Vorgaben der DSGVO und des BDSG zu beachten. Danach dürfen solche Informationen grundsätzlich nur verarbeitet und gespeichert werden, wenn dafür eine Einwilligung aller Betroffenen oder eine gesetzliche Erlaubnis vorliegt.

Einwilligungen sind bei dauerhaften Speicherungen eher selten, wenn auch rechtlich möglich. Voraussetzung ist allerdings, dass der Nutzer vor der Erhebung über das Schicksal seiner Daten informiert wird und in diesem Kenntnis der Speicherung der Daten zustimmt.

Wer zum Beispiel in die Zusendung eines Newsletters einwilligt, stimmt damit zugleich der zeitlich unbegrenzten Speicherung seiner Mailadresse zu. Diese Erlaubnis gilt im Zweifelsfall so lange, bis der Nutzer sein Abonnement abbestellt, der Speicherung seiner Daten explizit widerspricht oder bis das Projekt eingestellt wird. In diesen Fällen muss allerdings gewährleistet sein, dass die Informationen über diesen Nutzer vollständig gelöscht werden – und zwar auch aus etwaigen Backups, was in der Praxis häufig vernachlässigt wird.

Im Regelfall gilt es jedoch eine Rechtsgrundlage zu finden, auf deren Basis die Daten verarbeitet werden können. Solche Erlaubnistatbestände finden sich zahlreich in den unterschiedlichen Gesetzen selbst. So regelt im BDSG, dass die Vorgaben der



DSGVO erweitert, der Paragraph 26 die „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“.

Danach ist in einem Arbeitsverhältnis die Nutzung von Mitarbeiterdaten erlaubt, sofern diese „für Zwecke des Beschäftigungsverhältnisses verarbeitet werden“, insbesondere wenn dies unter anderem „für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung“ erforderlich ist.

Beispiel E-Mail-Archivierung

Die Langzeitspeicherung solcher Informationen kann dann im Einzelfall sogar zwingend vorgeschrieben sein, etwa im Bereich der Gehaltszahlungen. Nach dem Ende des Beschäftigtenverhältnisses fällt diese Rechtsgrundlage wieder weg. An ihre Stelle können allerdings andere gesetzliche Erlaubnisse oder sogar Anforderungen zur Speicherung treten, etwa aus dem Steuerrecht oder zur Berechnung der Rente.

Welche praktischen Schwierigkeiten sich bei der praktischen Umsetzung juristischer Vorgaben ergeben können, zeigt seit vielen Jahren die Pflicht zur E-Mail-Archivierung. Diese findet ihre Grundlage in den Vorgaben der Abgabenordnung (AO) und des Handelsgesetzbuches (HGB). Danach müssen sämtliche steuerlich relevanten Daten in maschinell auswertbarer Form für die Dauer von bis zu zehn Jahren aufbewahrt und für einen Prüfbzugriff durch die Steuerbehörden aufbereitet werden. Zu diesen aufbewahrungspflichtigen Handelsbriefen gehören auch E-Mails und ihre Dateianhänge, soweit sie „ein Handelsgeschäft betreffen“. Hierunter fallen zum Beispiel Bestellungen, Buchungen, Aufträge oder Rechnungen. Welche formalen technischen Voraussetzungen zu erfüllen sind, regeln die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD), die vor allem für die gefürchteten Steuerprüfungen relevant sind.

Damit fangen die rechtlichen Probleme allerdings erst an. Denn die Regelungen geben zwar ein verbindliches Speichern von Handelsbriefen in Form von E-Mails vor. Gleichzeitig verbieten aber Datenschutz und Arbeitsrecht zwingend die Archivierung rein privater Mails von oder an die Mitarbeiter. Zumindest in den Fällen, in denen den Mitarbeitern die private

Nutzung der Mailzugänge gestattet ist, müssen solche persönlichen Nachrichten vor dem Archivieren zwingend von den Handelsbriefen getrennt werden. Dies ist, wenn überhaupt, nur mit einigem technischen oder tatsächlichen Aufwand möglich – zumindest, wenn man den strengen Vorschriften der GoBD genügen will.

Nur zweckgebundene Speicherung

Eine weitere Hürde ist der eherne rechtliche Grundsatz der Zweckbindung. Danach dürfen Daten nur für den Zweck genutzt werden, zu dem sie erfasst oder gespeichert wurden. Für die steuerrechtlich begründete Archivierung von Handelsbriefen bedeutet dies, dass man eine solche Datensammlung eben nur für diesen Zweck benutzen darf. Die in vielen Unternehmen praktizierte zusätzliche Nutzung als E-Mail-Archiv und kurzfristiges Daten-Backup ist rechtlich unzulässig.

Ein anderer typischer Bereich für eine möglichst dauerhafte Speicherung von Daten betrifft die Backups, etwa von Logfiles. Im Regelfall werden hier in Form von IP-Adressen auch personenbezogene Daten erfasst. Rechtsprechung und gesetzliche Vorgaben sehen für die Speicherung und Aufbewahrung dann eine Erlaubnis vor, soweit dies zu Zwecken der IT-

Sicherheit erfolgt und ebenso erforderlich ist. Das bedeutet zunächst, dass „Nice to have“-Datensammlungen ebenso unzulässig sind wie eine Protokollierung zu Zwecken beispielsweise des Marketings. Auch eine spätere Nutzung dieser Informationen zu ganz anderen Zwecken, etwa im Rahmen von Big Data, ist auf Basis der strengen Vorgaben der Zweckbindung kaum zulässig.



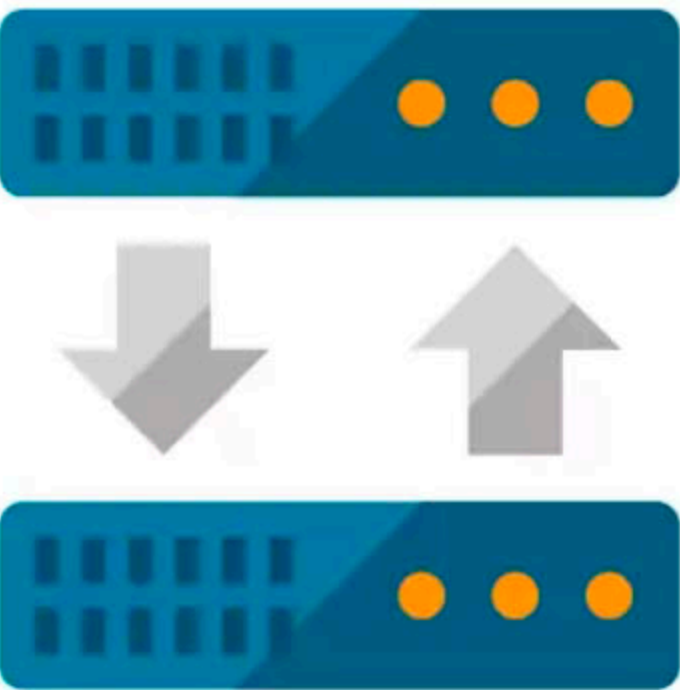
Umgang mit Logfiles

In der Praxis stellt sich immer wieder die Frage, wie lange die Speicherung von Logfiles erlaubt ist. Explizite gesetzliche Vorgaben dazu gibt es nicht. Der Bundesgerichtshof hat hierzu im Jahr 2014 ein Urteil gefällt, wonach ein Access-Provider im Rahmen der Gewährung der IT-Sicherheit seine Logfiles für eine Dauer von sieben Tagen speichern darf. Diese äußerst kurze Frist lässt sich zwar nicht eins zu eins auf andere Anbieter wie Website-Betreiber übertragen. Hieraus ergibt sich aber, dass ein allzu langes Vorhalten von Logfiles, selbst in Backups, klar gegen den Datenschutz verstößt.

Zulässig dürften Speicherfristen zwischen einer Woche und einem Monat sein. Die Praxis, solche Informationen über Monate zu speichern, ist daher eindeutig rechtswidrig. Um dieser Problematik zu entgehen, bietet es sich an, in den Logfiles zumindest bei langfristigem Vorhalten nur gekürzte IP-Adressen zu speichern. Diese sind dann zwar noch für die allermeisten Zwecke der IT-Sicherheit nutzbar. Einer Person zuzuordnen sind sie durch die Kürzung jedoch nicht mehr, sodass sie dann nicht mehr als personenbezogen zu betrachten sind und nicht in den Anwendungsbereich von DSGVO & Co fallen.

Immer mehr Daten werden in die Cloud exportiert, gerade im Bereich von Backups und Archivierung. Dies gilt natürlich auch bei Backup oder Archivierung. Soweit hierfür unternehmenseigene Server zum

Einsatz kommen, entstehen aus juristischer Sicht keine Komplikationen. Anders sieht es allerdings aus, wenn Unternehmen personenbezogene Daten an Dienstleister geben und deren Rechner sich außerhalb der EU befinden (siehe Seite 108 bis 123).



Löschpflichten

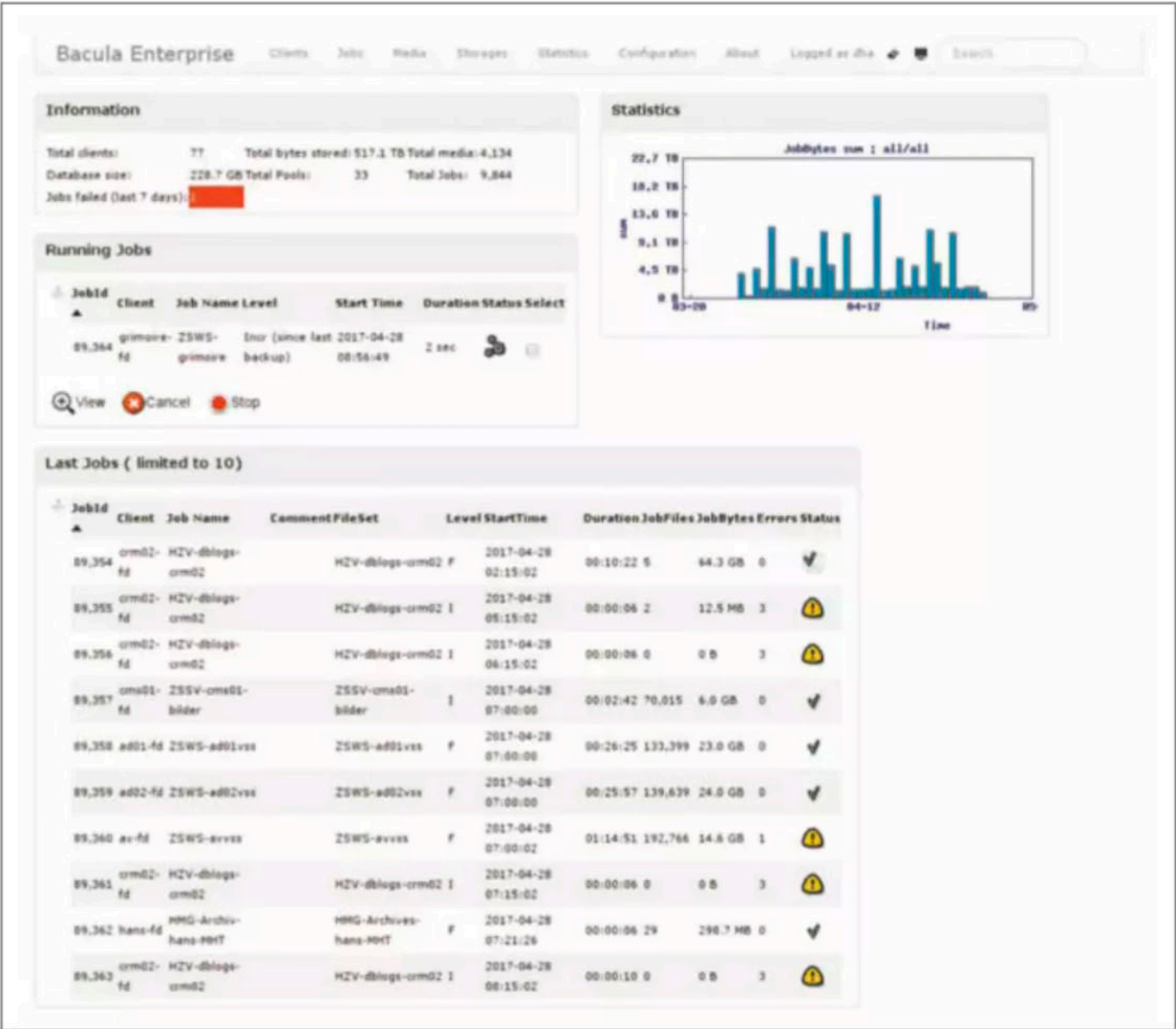
Wann aber müssen gespeicherte Daten zwingend gelöscht werden? Hauptgründe hierfür sind der Wegfall der Rechtsgrundlage oder ein expliziter Löschungswunsch durch den Betroffenen. Fällt der Grund für das Vorhalten der Informationen ersatzlos weg, sind die Daten zu löschen oder in ein Archiv zu überführen. Dies gilt beispielsweise nach dem Ende von Vertragsverhältnissen oder wenn das ursprüngliche Angebot eingestellt wird. Auch der Ablauf einer gewissen Zeitspanne kann hier ein Grund sein, beispielsweise am Ende von gesetzlichen Aufbewahrungsfristen. Das Löschen muss nach dem Wegfall dieser Gründe unverzüglich erfolgen. Selbstverständlich umfasst diese Verpflichtung auch Backups der erfassten Informationen.

Zudem kann ein Betroffener aktiv das Löschen seiner personenbezogenen Daten verlangen. Auch in diesem Fall hat ein unverzügliches und restloses Entfernen, etwa aus dem CRM, zu erfolgen. Problematisch sind dabei die Fälle, in denen eine Löschungsaufforderung mit gesetzlichen Speicherungspflichten kollidiert. So verlangen zum Beispiel ehemalige

Kunden regelmäßig die Löschung ihrer Daten. Dies ist dann nicht möglich, wenn das innerhalb der steuerrechtlichen Aufbewahrungsfristen erfolgt, die meist zwischen sechs und zehn Jahren liegen. In diesen Fällen ist lediglich eine Einschränkung der Verarbeitung der Daten möglich, da die Pflichten zum Vorhalten der steuerlichen Informationen den Datenschutz in der Regel überwiegen.

Gute Konzepte gesucht

Die längerfristige Speicherung von Daten ist ein juristischer Drahtseilakt. Auf der einen Seite stehen zwingende gesetzliche Aufbewahrungspflichten neben Anforderungen aus dem Compliance-Bereich. Auf der anderen Seite gebietet der Datenschutz ein möglichst kurzes und streng zweckgebundenes Vorhalten persönlicher Informationen. Um diesen Zielkonflikt zu entschärfen, empfiehlt es sich, entsprechende Speicher- und Löschkonzepte zu entwickeln, die neben den juristischen Vorgaben auch die Interessen aller Beteiligten berücksichtigen. (keh) **ct**



Ob für die Langzeitarchivierung oder gegen Datenverluste: Ein Backup ist das A und O für jeden, der mit Daten arbeitet. Aber Vorsicht, auch bei dieser „privaten Vorratsdatenspeicherung“ ist rechtlich nicht alles erlaubt.

EGAL WO... SPACE FASZINIERT!

DAS IST SPACE

Vollgepackt mit informativen Artikeln und atemberaubenden Fotos berichtet Space über die Technik der Weltraumfahrt, ebenso wie über Astronomie und kosmische Phänomene.



Testen Sie 2× Space mit 30% Rabatt!

Nur 11,90 €* statt 17,00 €* im Handel!

Zusätzlich digital als PDF im Kundenaccount verfügbar.

Jetzt bestellen unter:

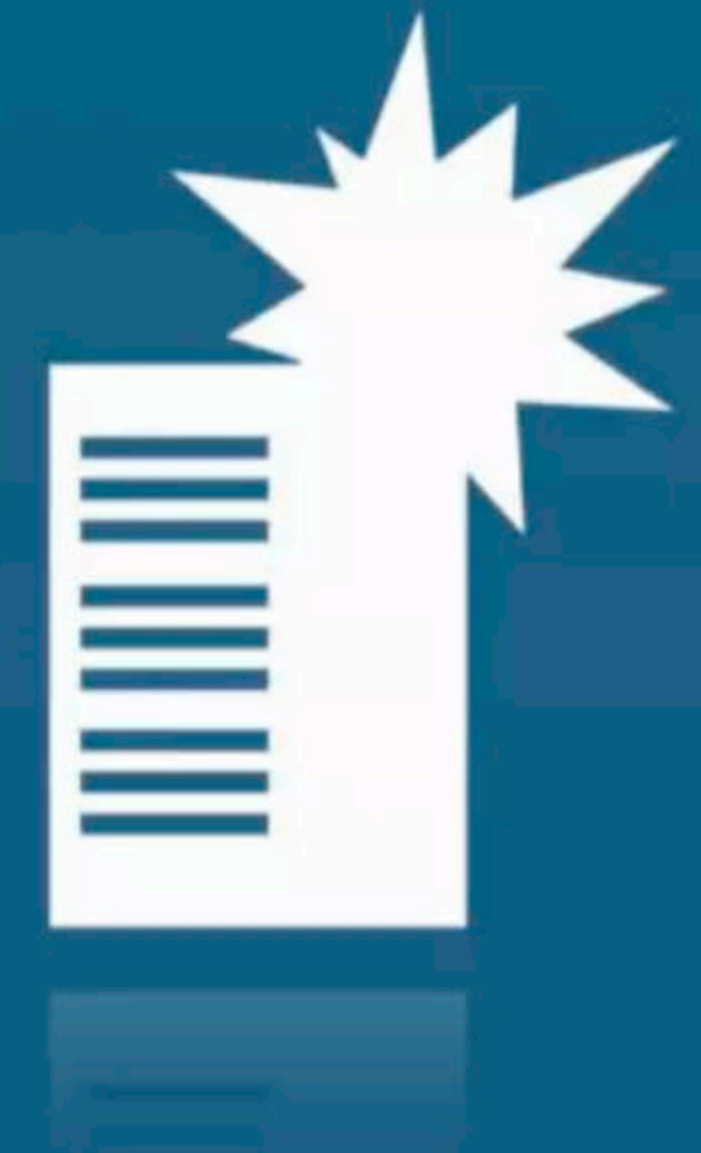
www.emedia.de/space-mini

☎ 0541 80 009 126 ✉ space-abo@emedia.de

✉ eMedia Leserservice, Postfach 24 69, 49014 Osnabrück

*Preise in Deutschland.

Meldepflichten bei Datenpannen



Trotz aller Sorgfalt kann es vorkommen, dass personenbezogene Daten unbeabsichtigt Dritten zugänglich werden, etwa durch Verlust eines Speichermediums, einen Malware-Angriff oder eine fahrlässige Datenpanne. Solch ein „Data Breach“ muss innerhalb kürzester Zeit umfänglich bei den Behörden und im Extremfall sogar den Betroffenen gemeldet werden – sonst drohen Bußgelder. Allerdings sind die Anforderungen an eine solche Meldung durchaus hoch.

Von Joerg Heidrich

Die Regelungen in der DSGVO zum Umgang mit Datenpannen stellen eine ganz erhebliche Verschärfung im Vergleich zur früheren Rechtslage dar. Damit werden diese Vorschriften mit zu den wichtigsten, aber gleichwohl eher unbekannten Neuregelungen. Kommt man diesen Anforderungen nicht oder nur teilweise und fehlerhaft nach, drohen erhebliche Bußgelder. Jedes Unternehmen tut also gut daran, sich rechtzeitig auf die Folgen eines Datenlecks vorzubereiten und entsprechende Notfallpläne aufzustellen.

Auch nach dem alten BDSG gab es bereits die Verpflichtung, den Verlust personenbezogener Daten anzuzeigen. Dies galt allerdings nur dann, sofern „schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen“ drohten. Weitergeben musste man daher Fälle mit ganz erheblichen Auswirkungen wie den Verlust von Aufzeichnungsbändern in Krankenhäusern.

Die Art. 33 und 34 DSGVO weiten diese Meldepflichten nun erheblich aus und senken die Voraussetzungen erheblich nach unten. Zukünftig sind Verletzungen des Schutzes personenbezogener Daten bereits dann zu melden, wenn diese zu „einem Risiko für die Rechte und Freiheiten natürlicher Per-

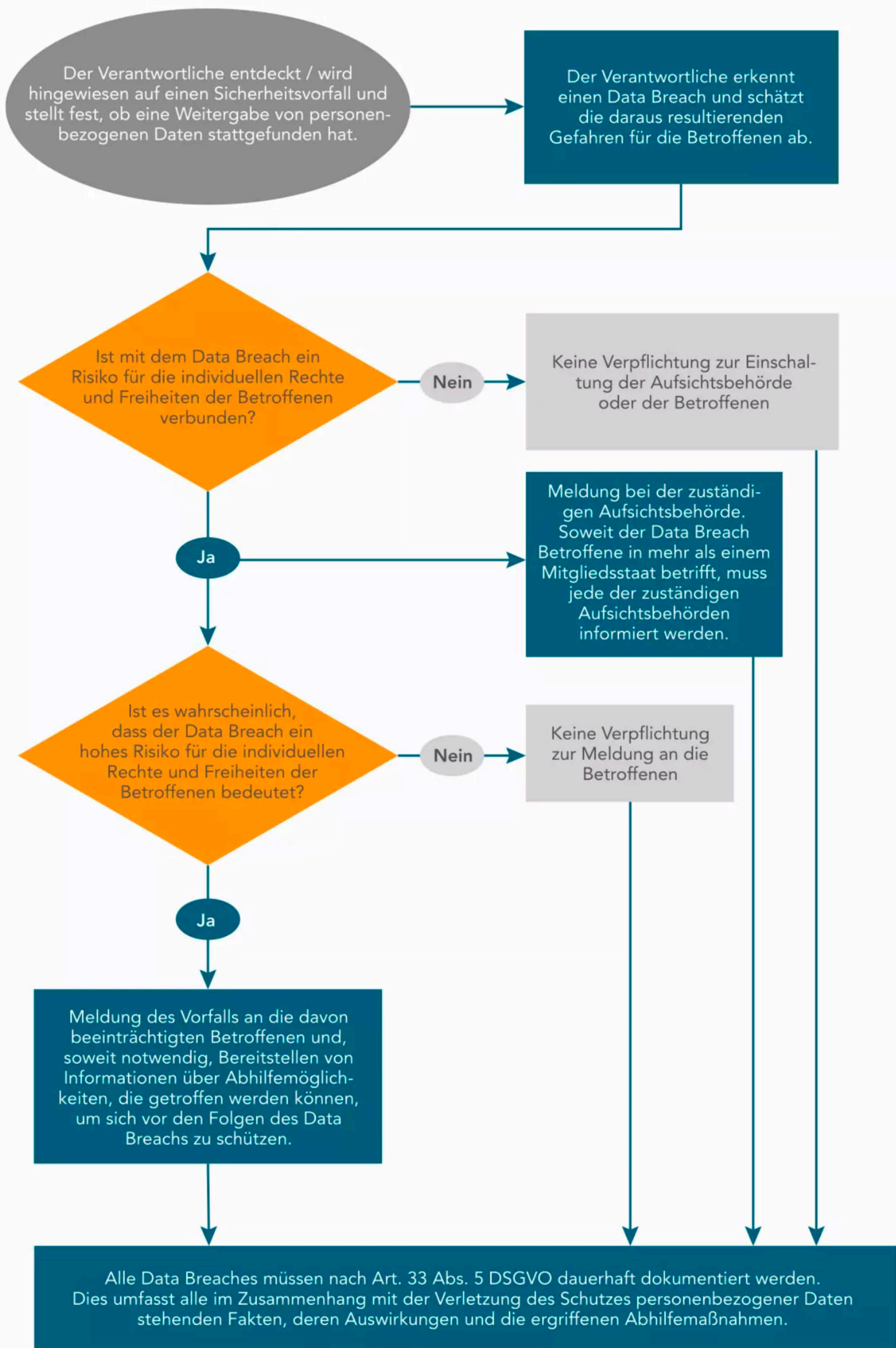
sonen“ führen. Damit beschränken sich die Anforderungen also nicht auf besonders schwere Datenlecks, sondern umfassen ohne größere Einschränkung nahezu jeden Verlust persönlicher Informationen im Unternehmen oder in der Verwaltung.

Freiheitsrisiken

Was damit genau gemeint ist, zeigt ein Leitfaden der Artikel-29-Datenschutzgruppe, dem früheren Zusammenschluss der europäischen Datenschutzbehörden, aus dem Herbst 2017 (siehe [ct.de/w5hs](https://www.ct.de/w5hs)). Das Papier enthält Beispiele für Vorgänge, die zu einer Mitteilungspflicht führen können:

- Entwendung von Login-Daten und Kaufhistorien von einem internationalen Online-Anbieter
- Als Ergebnis eines Online-Angriffs kann ein Krankenhaus für 30 Stunden nicht mehr auf Gesundheitsdaten zugreifen.
- Personendaten von über 5000 Studierenden werden an die falsche Mailingliste mit hundert von Empfängern geschickt
- Marketing-E-Mails werden in größerem Umfang so versandt, dass sämtliche Empfänger erkennbar sind

Ablaufdiagramm zur Meldepflicht



Quelle: Arbeitsgruppe Artikel 29, übersetzt

Noch weiter geht die niedersächsische Datenschutzbehörde, die in einem Online-Formular zur Meldung von Datenschutzverstößen auch Vorgänge wie die unrichtige Entsorgung personenbezogener Daten auf Papier, das Anzeigen der Daten falscher Betroffener in einem Kundenportal oder die mündliche Bekanntgabe personenbezogener Daten an die falsche Person aufweist.

Theoretisch ist damit auch jeder Verlust von Smartphones, Tablets oder Laptops sowie USB-Sticks anzuzeigen, sofern sich darauf personenbezogene Daten befinden – etwa von Kunden oder Mitarbeitern. Noch ungeklärt ist dabei die Frage, ob dies auch dann gilt, wenn das Gerät oder zumindest die Daten verschlüsselt sind. Es spricht einiges dafür, dass in diesem Fall nicht von einer Meldepflicht auszugehen ist, da kein relevantes Risiko für die Betroffenen besteht.

Zeitkritisch

Die Meldung muss unverzüglich, und zwar „möglichst binnen 72 Stunden“ ab Kenntnis des Data Breach erfolgen. Diese Frist ist extrem kurz und lässt Unternehmen kaum ausreichend Zeit für eine entsprechende Aufarbeitung der Geschehnisse.

Denn zumindest einige Datenschutzbehörden interpretieren „möglichst binnen 72 Stunden“ nicht als wünschenswerten Mindestwert, sondern knallhart als Höchstgrenze, die im Regelfall nicht zu überschreiten ist.

Formvollendet

Welche Inhalte die zu übermittelnde Meldung aufweisen muss, regelt Art. 33 Abs. 3 der DSGVO. Danach sind folgende Informationen Pflicht:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen

zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Weiterhin müssen die „Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen“ von dem Verantwortlichen dokumentiert werden. Faktisch ist also ein umfangreiches Protokoll der Geschehnisse sowie der ergriffenen Maßnahmen anzufertigen. Ziel ist es, der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen von Art. 33 zu ermöglichen.

Meldepflichten an Kunden und Mitarbeiter

Doch die Verpflichtungen des für die Datenverarbeitung Verantwortlichen können sogar noch weiter gehen. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein „hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen“ zur Folge, sind die betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen. Da hier ein hohes Risiko erforderlich ist, greift diese Pflicht erst bei etwas gravierenderen Auswirkungen der Datenpanne als bei der Meldepflicht an die Behörden.

Die Benachrichtigung sollte nach Erwägungsgrund 86 eine in klarer und einfacher Sprache verfasste Beschreibung der Art der Datenverletzung sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen des Data Breach enthalten. Die inhaltlichen Anforderungen an die Meldung entsprechen den oben genannten bei den Aufsichtsbehörden.

Solche Benachrichtigungen der betroffenen Person sollten stets „unverzüglich“, also so rasch wie möglich, in Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen.

Eine längere Benachrichtigungsfrist kann dann gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.

Ausnahmen der Benachrichtigungspflichten

Hierunter fällt etwa eine dem Stand der Technik entsprechende Verschlüsselung der Daten. Ebenfalls entfällt die Meldepflicht dann, wenn der Verantwortliche durch nachträglich getroffene Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht. Dies könnte etwa der Fall sein, wenn die Daten auf einem verlorenen Smartphone nachträglich über eine Remote-Steuerung gelöscht werden konnten.



Gleiches gilt auch dann, wenn ein Hinweis mit einem unverhältnismäßig hohen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden. Zu denken wäre hierbei an Hinweise auf der Website oder in extremen Fällen auch an Anzeigen in Tageszeitungen, wie sie schon das alte BDSG kannte. In jedem Fall ist es wichtig, sich auf solche Notfälle angemessen vorzubereiten. Hierzu gehört es insbesondere, ein interdisziplinäres Team ins Leben zu rufen, das kurzfristig verfügbar ist und auf solche Datenpannen reagieren kann. (keh) **ct**

Profis hinzuziehen

Eine Data-Breach-Meldung nach Art. 33 und 34 DSGVO kann eine hochgradig herausfordernde Angelegenheit sein, bei der man als Unternehmen ohne entsprechendes Know-How sehr viel falsch machen kann. Hinzu kommt der immense Zeitdruck von 72 Stunden, in deren Rahmen die Meldung zu erfolgen hat. Zwar dürfte auch ein mäßig begabter Datenschutzbeauftragter mithilfe von entsprechenden Vorlagen bei einem einfachen Vorfall wie dem Verlust eines USB-Sticks oder eines Notebooks klarkommen. Bei komplizierteren Vorfällen insbesondere im Online-Bereich empfiehlt es sich aber im Zweifelsfall, externe Kompetenz im Bereich Recht und Technik hinzuzuziehen.

Dies gilt je nach vorhandener Kompetenz zunächst einmal für kompetente Techniker, die bei der Aufarbeitung des Falls ebenso behilflich sein können wie bei der Beschreibung und der zeitnahen Umsetzung von Abhilfemaßnahmen. Bei solchen komplizierten Fällen sollte zudem auch ein IT-Anwalt hinzugezogen werden, der bei diesen Punkten ebenso nützlich sein kann

wie bei der Formulierung der zu übermittelnden Meldung an die Aufsichtsbehörden.

Spätestens dann, wenn auch Pflichten zu einer Mitteilung des Datenschutzes an die jeweiligen Betroffenen besteht, sollte der Vorgang auch unter PR-Gesichtspunkten wahrgenommen werden. In einem solchen Fall kann ein Unternehmen durch unbedachte Kommunikation regelrechte Desaster in der öffentlichen Wahrnehmung erleben, wie dies schon einige Provider feststellen mussten, die in diese unschöne Lage gerieten. Neben der technischen und juristischen Bewältigung einer solchen Krise kann es sich dann empfehlen, auch für diesen Bereich entsprechende Fachleute hinzuzuziehen, die eine angemessene Ansprache für solche Vorfälle formulieren können.

In jedem Fall ist es ebenso hilfreich wie empfehlenswert, die Kontaktdaten solcher Profis für alle Fälle in den (offline) Unterlagen vorzuhalten, um im Ernstfall nicht auch noch auf die Suche gehen zu müssen.

**Guidelines und FAQ
zu Meldepflichten:**

[ct.de/w5hs](https://www.ct.de/w5hs)



DSGVO für Website-Betreiber

Betreiber einer Website müssen etliche Regelungen der DSGVO berücksichtigen. Wir zeigen, wie Sie Ihren Internetauftritt datenschutzkonform gestalten und welche Informationen gemäß dem Datenschutz weder fehlen noch falsch sein dürfen.

Von Nicolas Maekeler

Nicht nur Unternehmens-Websites oder Onlineshops müssen den Anforderungen der DSGVO genügen, sondern in den allermeisten Fällen auch Blogs oder Internetseiten von Vereinen. Denn ohne die Verarbeitung personenbezogener Daten, also Informationen jeglicher Art, die sich auf eine zumindest theoretisch identifizierbare natürliche Person beziehen, lässt sich keine Website betreiben.

Erwägungsgrund 30 der DSGVO stellt klar, dass auch IP-Adressen als „Online-Kennungen“ und damit als personenbezogene Daten zu werten sind. Dies deckt sich auch mit der Rechtsprechung des Bundesgerichtshofs (BGH), der bereits im Mai 2017 entschied, dass es sich auch bei dynamisch vergebenen

IP-Adressen um personenbezogene Daten handelt. Da der Browser selbst bei einem reinen Lesezugriff auf eine Website die IP-Adresse übermittelt, ist allein schon deswegen der Anwendungsbereich der DSGVO eröffnet.

Wer seine Website nicht datenschutzkonform einrichtet, muss damit rechnen, von Mitbewerbern abgemahnt zu werden oder ins Visier der Datenschutzbehörden zu geraten.

Datenschutzerklärung

Website-Betreiber müssen ihre Besucher mit einer Datenschutzerklärung (auch „Privacy Policy“) über alle Vorgänge aufklären, bei denen sie personen-

bezogene Daten verarbeiten. Eine solche Erklärung war auch schon lange vor Wirksamwerden der DSGVO obligatorisch.

Die Datenschutzerklärung muss etwa die konkrete Rechtsgrundlage für die Datenverarbeitung aus Artikel 6 der DSGVO nennen. Rechtsgründe für die Verarbeitung können zum Beispiel die Bearbeitung eines Kaufvertrages in einem Onlineshop sein, aber auch berechnigte Interessen des Website-Betreibers (siehe Seite 16).

Im letzten Fall ist dann auch das konkret verfolgte Interesse zu formulieren. Bei Website-Betreibern kann das beispielsweise das Interesse an der Betriebssicherheit ihrer Homepages sein. Um Angriffe erkennen und abwehren zu können, dürfen sie dafür die IP-Adressen der Besucher für maximal 14 Tage speichern. Darauf muss in der Datenschutzerklärung hingewiesen werden. Ob und wie lange IP-Adressen der Nutzer gespeichert werden, erfährt man beim Webhoster seines Vertrauens.

Website-Betreiber sollten die Besucher darüber informieren, wo auf Besucher beziehbare Daten erhoben und verarbeitet werden. Neben Logfiles zählen auch Geolokalisierungsfunktionen dazu, Registrierungsmöglichkeiten, Kommentarfunktionen, das Abonnement von Newslettern, die Verwendung von Cookies, die Nutzung von Social-Sharing-Funktionen und die Verwendung von Analyse- und Trackingdiensten.

Website-Betreiber müssen auf Basis der DSGVO die Besucher ihrer Site ausführlich über ihre Rechte aufklären. Neben der Pflicht, sie über deren Rechte auf Auskunft, Löschung, Berichtigung von Daten und Widerruf zu informieren, verlangt die DSGVO die Information über das Recht auf Einschränkung der Verarbeitung, das Widerspruchsrecht, das Beschwerderecht bei einer Aufsichtsbehörde sowie das Recht auf Datenübertragbarkeit.

Informationen zum Widerspruchsrecht müssen sogar optisch hervorgehoben werden, etwa durch Fettdruck oder eine Umrahmung. Hat das Unternehmen einen Datenschutzbeauftragten, müssen dessen Kontaktdaten hinterlegt werden.

Die wichtigsten allgemeinen Pflichtangaben können den Checklisten für die Datenschutzerklärung auf Seite 46 entnommen werden.

Richtet sich die Website an eine internationale Klientel, so sollte die Datenschutzerklärung nicht

nur in deutscher Sprache vorliegen, sondern auch in allen infrage kommenden Übersetzungen.

Letztlich muss die Privacy Policy „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ bereitgestellt werden. Bei umfangreichen Datenschutzerklärungen bietet es sich an, Details auszugliedern und über Links an separater Stelle verfügbar zu machen.

Wer für diese anspruchsvolle Aufgabe nicht gleich einen Datenschutzrechtler beauftragen möchte, kann einen Online-Generator nutzen. Mithilfe dieser Tools kann man sich die DSGVO-konforme Datenschutzerklärung in wenigen Schritten zusammenklicken. Empfehlenswert ist der Datenschutzgenerator von Rechtsanwalt Thomas Schwenke (siehe ct.de/wy9s).

Webformulare verschlüsseln

Bietet die Website Nutzern die Möglichkeit, ihre personenbezogenen Daten in Webformulare einzugeben – zum Beispiel in einem Onlineshop während des Bestellprozesses –, muss dieser Vorgang verschlüsselt ablaufen. Das folgt aus dem in der DSGVO geregelten Grundsatz der Integrität und Vertraulichkeit, wonach personenbezogene Daten in einer Weise verarbeitet werden müssen, „die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung [...]“.

Webmaster dürfen nach dem Grundsatz der Datenminimierung nur die Daten anfordern, die sie für die jeweilige Aufgabe benötigen (siehe Seite 16). Bei Newsletter-Anmeldungen sollten sie beispielsweise nicht das Geburtsdatum oder die postalische Adresse abfragen. Wie man die Versendung von Newslettern DSGVO-konform gestalten kann, erfahren Sie in dem Artikel auf Seite 154.

Der Einsatz von Cookies sorgt schon länger für Verunsicherung bei Website-Verantwortlichen. Viele Sites weisen durch Banner oder Popup-Fenster Besucher darauf hin, dass sie Cookies verwenden, wobei diese Hinweisschilder in vielen Fällen rechtlich nicht einwandfrei gestaltet sind. Da die



nötigen (siehe Seite 16). Bei Newsletter-Anmeldungen sollten sie beispielsweise nicht das Geburtsdatum oder die postalische Adresse abfragen. Wie man die Versendung von Newslettern DSGVO-konform gestalten kann, erfahren Sie in dem Artikel auf Seite 154.

Cookies unerwünscht

Der Einsatz von Cookies sorgt schon länger für Verunsicherung bei Website-Verantwortlichen. Viele Sites weisen durch Banner oder Popup-Fenster Besucher darauf hin, dass sie Cookies verwenden, wobei diese Hinweisschilder in vielen Fällen rechtlich nicht einwandfrei gestaltet sind. Da die

Cookie-Thematik sehr komplex ist, klären wir auf Seite 158 alle Detailfragen.

Vorsicht bei Plugins

Soll eine Website Social-Media-Plugins wie den Facebook-Like-Button einsetzen, werden die Nutzer hierin einwilligen müssen. Denn diese Tools übertragen auch ohne einen Klick auf „Gefällt mir“ oder „Teilen“ ungefragt Informationen an die entsprechenden Anbieter. Das entspricht deutscher Rechtsprechung nach dem alten BDSG. So hat das Landgericht Düsseldorf mit Urteil vom 9.3.2016 (Aktenzeichen 12 O 151/15) entschieden, dass die Einbindung derartiger Facebook-Tools ohne Zustimmung nicht erlaubt ist. Im Rahmen der erwähnten Interessenabwägung wird sich der Einsatz solcher Buttons also nicht legitimieren lassen.

Website-Betreiber sollten deswegen auf die mittlerweile weit verbreitete Shariff-Lösung von c't zurückgreifen, die dafür sorgt, dass soziale Netzwerke erst dann Daten von Nutzern abfragen können, wenn diese auf den entsprechenden Button klicken (siehe ct.de/wy9s). Das ändert aber nichts an dem Umstand, dass der Nutzer beim Klick auf einen Button weiterhin nicht weiß, welche konkreten Daten Facebook erhält und was mit diesen passiert.

Auch für externen Social-Media-Content gibt es mittlerweile eine Lösung. Das c't-Projekt „Embetty“ ermöglicht es, YouTube-Videos, Vimeo-Videos, Facebook-Videos und Tweets datenschutzfreundlich einzubinden. Die Videos kommen zwar noch vom jeweiligen Webdienst, nicht aber das Vorschau-Bild. Der Browser spricht den externen Dienst erst an, wenn der Nutzer den entsprechenden Inhalt angeklickt hat (siehe ct.de/wy9s). Den Quellcode beider Tools hat c't auf Github veröffentlicht. Was im Übrigen beim Einsatz von Social-Media-Diensten, insbesondere beim Betrieb einer Facebook-Fanpage, in datenschutzrechtlicher Hinsicht zu berücksichtigen ist, können Sie auf Seite 152 nachlesen.

Vorsichtig sollte man auch beim Einsatz anderer Plugins oder Templates sein. Überlegen Sie, ob Sie alle Funktionen ihres modularen Website-Baukas-

tens benötigen. Einzelne Tools müssen auf ihre Datenschutzkonformität hin geprüft werden. Problematisch ist es zum Beispiel, wenn ein Plug-in zur Spamvermeidung bei Kommentarfunktionen Daten aus den Eingabefeldern zum Spam-Abgleich mittels Big Data an Server in die USA überträgt.

Webhosting und Webhousing

Ein Website-Betreiber darf nicht ohne Weiteres personenbezogene Daten auf einem von Dritten bereitgestellten Webspace speichern. Beauftragt er einen Dienstleister mit dem Hosting seiner Seiten, muss er dafür die Einwilligung der Besucher einholen oder eine andere Rechtsgrundlage schaffen.

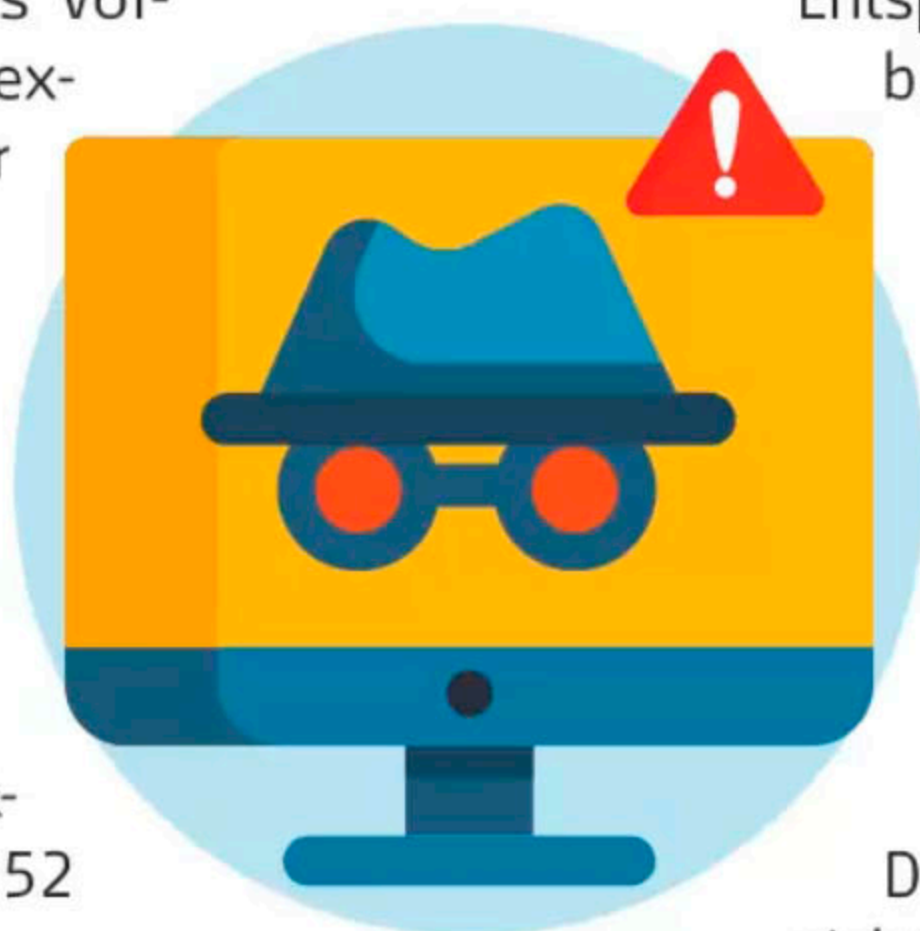
Da es unrealistisch ist, jeden einzelnen Besucher nach seiner Einwilligung zu fragen, ist es sinnvoll den Hoster mit einer Auftragsverarbeitung (vormals Auftragsdaten-

verarbeitung) nach Artikel 28 DSGVO einzubinden. Diese erlaubt dem Webhoster personenbezogene Daten „gemäß den Weisungen des für die Verarbeitung Verantwortlichen“ – also des Website-Betreibers zu verarbeiten. Im Rahmen dieses Konstrukts gilt der Webhoster rechtlich nicht mehr als außenstehender Dritter, es bezieht ihn in den Verantwortungsbereich des Website-Betreibers ein. Der bleibt damit also selbst „Herr der Daten“.

Mietet der Website-Betreiber nur Server in einem Rechenzentrum an, ohne dass der Hoster selbst die Daten verarbeitet (Housing), benötigt er keine derartige Vereinbarung. Etliche Webhoster bieten eigene Formulare für die Auftragsverarbeitung an.

Entsprechende Vereinbarungen kann man bequem auf elektronischem Weg abschließen, sogar mit Firmen, die außerhalb der EU ihren Sitz haben. Weitere Details zur Auftragsverarbeitung erfahren Sie in dem Artikel auf Seite 56. Wer seine Website bei einem US-amerikanischen Hoster unterbringen will, sollte sich bewusst sein, dass die Datenübertragung in ein unsicheres Drittland erfolgt. Was dabei zu berücksichtigen ist erfahren Sie im Kapitel ab

Seite 108–123. Website-Verantwortliche sollten die Beauftragung eines amerikanischen Webhosters jedenfalls gründlich überlegen.



Datenschutzgenerator, Shariff-Lösung, Embetty

ct.de/wy9s



FAQ

? Wo platziere ich am besten die Datenschutzerklärung auf meiner Website?

! Der Website-Besucher muss die Datenschutzerklärung einfach finden können, Sie sollten sie daher nicht irgendwo auf der Site verstecken. Der Link zur Erklärung gehört direkt auf die Startseite. Idealerweise platziert man ihn im Footer, sodass die Informationen auch von jeder Unterseite aus mit einem Klick erreichbar sind. Der Linktext sollte aussagekräftig sein, zu empfehlen sind Formulierungen wie „Datenschutz“, „Datenschutzhinweis“ oder am besten „Datenschutzerklärung“. In das Impressum gehört die Datenschutzerklärung nicht. Für beide Pflichtinformationen sollte man jeweils eine einzelne Seite anlegen. Da fehlende oder versteckte Datenschutzerklärungen zu den meist verbreitetsten Abmahngründen in Bezug auf Datenschutzverletzungen von Website-Betreibern gehören, sollten diese Grundsätze zwingend berücksichtigt werden. Denken Sie auch daran, einen Link zur Datenschutzerklärung in den geschäftlich genutzten Social Media-Profilen zu platzieren.

? Benötige ich für meine private Website auch eine Datenschutzerklärung?

! Lediglich Webangebote, die ausschließlich familiären oder persönlichen Zwecken dienen, sind vom Anwendungsbereich der DSGVO ausgenommen (siehe Seite 12). Das trifft etwa auf private Social Media Profile zu. Für öffentlich zugängliche Websites dürfte das Haushaltsprivileg in der Regel jedoch nicht

zur Geltung kommen. Denkbar wäre aber beispielsweise ein Archiv von Bildern der eigenen Katzen für Freunde und Verwandte. Aber Vorsicht: Es genügt, auf derartigen Seiten Bannerwerbung zu schalten oder Affiliate-Links zu verwenden, um die Grenze zur kommerziellen Nutzung zu überschreiten und den Vorschriften der DSGVO zu unterliegen.

? Reicht es aus, wenn ich bei Formularfeldern auf meiner Website einen Link zur Datenschutzerklärung setze?

! Überall dort, wo Website-Besucher aktiv personenbezogene Daten eingeben können, wie bei Kontaktformularen, Online-Bestellungen oder im Rahmen von Registrierungsfunktionen, sollten Sie neben dem Link zur Datenschutzerklärung auch einen erläuternden Hinweis zur jeweiligen Datenverarbeitung hinzufügen. Als Faustformel gilt: Eine Verlinkung ist immer nur dann ausreichend, wenn der Nutzer mit der entsprechenden Datenverarbeitung rechnen darf. Im Umkehrschluss bedeutet dies, dass die Datenschutzerklärung keine überraschenden Verarbeitungsvorgänge enthalten darf. Da die Abgrenzung schwierig ist, sollten Sie lieber einmal zu viel Informationen bereitstellen als zu wenig. Insbesondere wenn Einwilligungen auf der Website eingeholt werden, reicht ein einfacher Link zur Datenschutzerklärung nicht aus. Wie ein Hinweistext beispielsweise im Falle einer Newsletter-Anmeldung aussehen sollte, erfahren Sie auf Seite 154.

? Ich habe auf meiner Website ein Kontaktformular. Benötige ich die Einwilligung des Nutzers, damit ich ihm antworten kann?

! Immer wieder finden sich bei Kontaktformularen auf Websites kleine Checkboxes, die man anklicken muss, um eine datenschutzrechtliche Einwilligung zur Beantwortung des Anliegens zu erteilen. Dies ist allerdings unnötig. Man sollte sogar darauf verzichten. Das Problem ist, dass eine Einwilligung jederzeit widerrufbar ist, erst ab dem 16. Lebensjahr wirksam erteilt werden kann und vom Verantwortlichen dokumentiert werden muss. Die Beantwortung einer Nutzeranfrage wird entweder durch eine (vor-)vertragliche Beziehung oder durch die berechtigten Interessen des Website-Betreibers legitimiert. Weil der Nutzer eine Verarbeitung seiner Daten zum Zwecke der Beantwortung erwartet, reicht insoweit ein kurzer Hinweis mit Verweis auf die Datenschutzerklärung aus. (keh) 

Facebook & Datenschutz



Soziale Netzwerke haben den mehr als berechtigten Ruf, große Datenkraken zu sein. Zur Pflege des Kundenkontakts sind diese Dienste für Unternehmen jedoch von großer Bedeutung. Allerdings ist Vorsicht geboten: Sie sind für die Datenverarbeitung der Social-Media-Anbieter teils mitverantwortlich und haften unter Umständen auch.

Von Nicolas Maekeler

Wenn es um die Außendarstellung geht, kommt kaum ein Unternehmen mehr ohne Facebook, Google, Twitter und Co. aus. Gerade für kleinere Firmen oder Selbstständige ist der Betrieb einer sogenannten Facebook-Fanpage ein kostengünstiger und einfacher Weg, um mit Kunden in Kontakt treten zu können.

Besucherstatistiken

Neben den normalen Funktionen eines eigenständigen Facebook-Profiles stehen Administratoren einer Fanpage verschiedene Statistiken rund um die Seite zur Verfügung. Die Daten aus diesen Insight-Statistiken, wie Alter der Besucher, Geschlecht, Interaktion mit Beiträgen etc., können Fanpage-Betreiber nutzen, um Werbung und Inhalte gezielt an den Besuchern auszurichten. Diese Form der Datennutzung war den Datenschutzbehörden schon lange ein Dorn im Auge. Ein bereits im Jahr 2011 angestoßenes Verfahren vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) gegen einen Fanpage-Betreiber mündete in einem Urteil des Europäischen Gerichtshofs (EuGH, Urteil vom 05.06.2018, Aktenzeichen: C-2210/16, „Wirtschaftsakademie“). Dieser entschied, dass Fanpage-Betreiber für die Verarbeitung von Daten der Besucher mitverantwortlich sind. Der Grund: Mithilfe der bereitgestellten Filter könne der Fanpage-Betreiber selbst Kriterien festlegen, nach denen Insight-Statistiken erstellt werden. Er könne sogar Kategorie von Personen bezeichnen, deren personenbezogene Daten Facebook auswertet. Dadurch

trage er zur Verarbeitung dieser Daten der Nutzer bei, schlussfolgerte das Gericht. Laut EuGH hilft dem Seitenbetreiber auch nicht, dass er die von Facebook erstellten Besucherstatistiken in anonymisierter Form erhält. Diese Statistiken beruhen dem Gericht zufolge auf einer Erhebung und Verarbeitung personenbezogener Daten der Seitenbesucher für eben diese statistischen Zwecke, die bereits zu einem Zeitpunkt erfolgt, wenn der Nutzer die Fanpage aufruft.

Weitreichende Folgen

Obwohl die Entscheidung noch vor Wirksamwerden der DSGVO gefällt wurde, hat sie aktuelle Auswirkungen, da sich an der Definition des „Verantwortlichen“ nichts Wesentliches geändert hat. Nach Art. 4 Nr. 7 DSGVO ist „Verantwortlicher“ die Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Gemeinsam mit Facebook für Datenverarbeitungsvorgänge verantwortlich zu sein, hat allerdings weitreichende Folgen für Seitenbetreiber. Sie sind zum Beispiel zur Auskunft verpflichtet und müssen Informationspflichten erfüllen. Wenn sich herausstellt, dass Facebook auf den Seiten Datenschutzverstöße begeht, sind die Betreiber – zumindest im Rahmen ihrer Fanpage-Nutzung – zunächst in vollem Umfang mit haftbar. Auch, wenn im Falle von Bußgeldern oder Schadensersatzforderungen eine Rückzahlung des auf Facebook entfallenden Teils der Kosten von Facebook verlangt werden kann.

Weitere Hinweise:

[ct.de/w1bg](https://www.ct.de/w1bg)

Joint Controller Agreement

Um die gemeinsame Verantwortlichkeit zu regeln, muss nach Art. 26 DSGVO eine Vereinbarung zwischen den Parteien getroffen werden (Joint Controller Agreement). In dieser wird festgelegt, wer welche Verpflichtungen gemäß der DSGVO erfüllt. In Reaktion auf das Urteil des EuGH hat Facebook seine AGB um eine solche Vereinbarung namens „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“, ergänzt (siehe [ct.de/w1bg](https://www.facebook.com/ct.de/w1bg)). Diese Vereinbarung macht deutlich, dass auch der Fanpage-Betreiber gewisse Verpflichtungen übernimmt: „Du solltest sicherstellen, dass du auch eine Rechtsgrundlage für die Verarbeitung der Insights-Daten hast.“

Zudem bedarf es eigener Datenschutzhinweise, die über den Punkt „Datenrichtlinie“ im Infobereich der Fanpage hinterlegt werden können. Diese sollten die notwendigen Informationen des Art. 13 DSGVO beinhalten und zusätzlich auf die Seiten-Insights-Ergänzung verlinken.

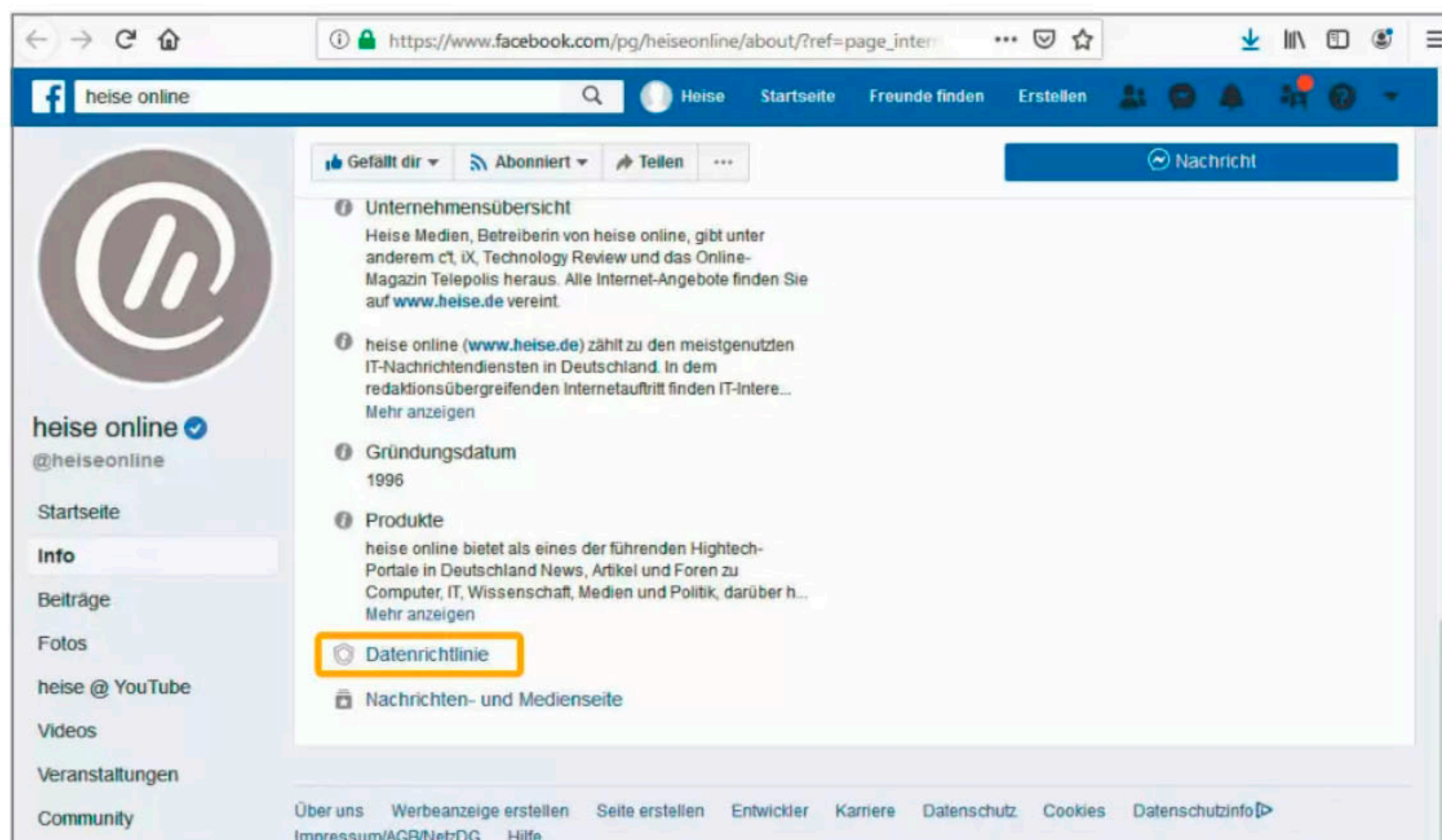
Die Datenschutzbehörden sind allerdings der Ansicht, dass kein datenschutzkonformer Betrieb einer Fanpage möglich ist. Der Datenschutzkonferenz (DSK) genügen die seitens Facebook bereitgestellten Informationen nicht. Sie seien nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten ihrer Besucher zu ermöglichen. Im November 2019 machte Facebook transparent, dass keine Daten von Nichtmitgliedern für Insight-Statistiken verarbeitet werden. Dies dürfte ein wichtiges Argument der Behörden gegen den Betrieb von Fanpages entkräften.

Gleichwohl können die Datenschutzbehörden weiterhin direkt gegen Fanpagebetreiber vorgehen und sie zur Deaktivierung der Seite verpflichten, wenn sie die Datenverarbeitung als rechtswidrig einstufen. Dieses Vorgehen sei nämlich effektiver, als sich an Facebook zu wenden, wie sich aus einer Entscheidung des Bundesverwaltungsgerichts (BVerwG Urteil. v. 11.09.2019, Az. 6 C 15.18) ergibt.

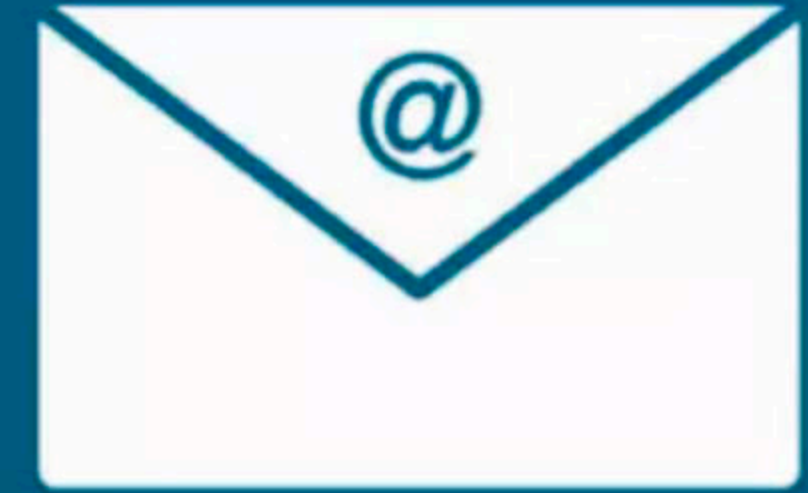
Trend zur Mithaftung

Auch bei der „Gefällt mir“-Schaltfläche (Like-Button), die Website-Betreiber auf ihren Homepages einbinden können, um ihre Inhalte zu verbreiten, sieht der EuGH eine arbeitsteilige Datenverarbeitung zwischen Facebook und dem Seitenbetreiber. Dies folgt aus einer konsequenten Entscheidung des obersten europäischen Gerichts (EuGH, Urteil vom 29.07.2019, Aktenzeichen: C-40/17, „Fashion ID“). Ausgangspunkt des Falls war eine Klage der Verbraucherzentrale Nordrhein-Westfalen gegen einen Online-Händler, der einen Facebook-Like-Button in seine Website eingebunden hatte. Durch den Button werden bei Aufruf der Website die IP-Adresse des Website-Besuchers, die aufgerufenen Inhalte sowie browser-spezifische Informationen an Facebook übermittelt, ohne dass der Nutzer die Schaltfläche betätigt. Laut EuGH reicht es aus, wenn ein Beteiligter aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt, nach dem Motto: Wäre der Like-Button nicht eingebunden, könnte Facebook auch keine Daten sammeln. Die gemeinsame Verantwortung erstreckt sich nur auf die Phase der Datenerhebung und -übermittlung an Facebook. Für alles Weitere ist Facebook allein verantwortlich.

Die Rechtsprechung des EuGH gibt Anlass, generell von Drittanbietern eingebundene Dienste auf eine gemeinsame Verantwortlichkeit hin zu überprüfen. Das Problem: In den allermeisten Fällen bieten Plattformbetreiber keine Standardvereinbarung nach Art. 26 DSGVO an. An dieser fehlt es auch im Falle des Like-Buttons. Die Nutzung wäre damit datenschutzrechtlich unzulässig. Darüber hinaus ist in vielen Fällen bei der Verwendung von Social-Plugins die Einwilligung der Nutzer einzuholen. Hintergründe hierzu finden Sie im Artikel auf Seite 158. Datenschutzfreundliche Lösungen bieten die im Artikel DSGVO für Website-Betreiber vorgestellten Lösungen „Shariff“ und „Embeddy“ des c't Magazins ab Seite 148. Im Übrigen sollte auf den Einsatz von Social-Plugins verzichtet werden, wenn sie keine messbaren wirtschaftlichen Vorteile bringen. (keh) 



E-Mail-Marketing



Die DSGVO enthält keine Sonderregeln für das Versenden von Newslettern oder E-Mail-Werbung. Der rechtliche Rahmen ist dennoch eindeutig.

Von Nicolas Maekeler

Der Versand von Newslettern ist nach wie vor ein beliebtes Marketinginstrument. Selbstverständlich sind auch hierbei rechtliche Vorgaben zu beachten. Da in aller Regel personenbezogene Daten verarbeitet werden, benötigt der Versender beim E-Mail-Versand eine in der DSGVO geregelte Rechtsgrundlage. Ob der Versender dabei eine Einwilligung benötigt oder ob eine andere Rechtsgrundlage greift, hängt von der Art des Newsletters ab. Nimmt er ohne kommerzielles Interesse Kontakt zum Empfänger auf, wird sich der Versender auf sein „berechtigtes Interesse“ berufen können. Diese Rechtsgrundlage erlaubt laut DSGVO eine Datenverarbeitung, wenn keine überwiegenden entgegenstehenden Interessen des Betroffenen bestehen und dieser der Datenverarbeitung nicht bereits per Opt-out widersprochen hat (siehe auch Seite 16).

Beispiele für berechtigtes Interesse sind hier der Versand des Gemeindebriefs einer Kirche, die Einladung zur Veranstaltung einer gemeinnützigen Organisation und andere nicht werbliche Informationsbriefe. Auch Pressemitteilungen per Mail fallen darunter, weil man bei empfangenden Journalisten ein Interesse vermuten darf. Selbst für Werbesendungen benötigen Absender aus rein datenschutzrechtlicher Sicht nicht zwingend eine Einwilligung der Empfänger, denn gemäß Erwägungsgrund 47 DSGVO kann die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.



Wettbewerbsrecht verhindert Spam

Doch auch wenn das Versenden DSGVO-konform wäre, gilt es das Wettbewerbsrecht zu beachten: Nach Paragraph 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) gilt es als unzumutbare und damit unzulässige Belästigung, Werbe-Mails ohne vorherige ausdrückliche Einwilligung des Adressaten zu versenden. Diese Regelung hat nichts mit Datenschutz zu tun, sondern dient in erster Linie der Vermeidung von Spam. Mit der DSGVO hat sich diesbezüglich nichts geändert.

Eine Ausnahme vom generellen Einwilligungsvorbehalt sieht Paragraph 7 UWG nur im Rahmen der Ähnlichkeitswerbung vor. Die Voraussetzungen dafür sind jedoch sehr streng geregelt: Der Versender muss die E-Mail-Adresse des Empfängers im Zusammenhang mit dem Verkauf von Waren oder Dienstleistungen erhalten haben, er darf nur ähnliche Produkte bewerben und der Kunde muss bei Erhebung der Daten sowie in jedem Mailing auf sein Widerspruchsrecht hingewiesen werden. Letzteres kann in der Datenschutzerklärung der Website geschehen (siehe Kasten rechts). Dann muss der Versender bei der Erhebung der E-Mail-Adresse darauf hinweisen und in jeder Mail einen Optout-Link platzieren.

Für alle anderen Fälle der werblichen Ansprache per E-Mail bedarf es einer zu dokumentierenden Einwilligung, die den Anforderungen des Artikels 7 DSGVO entspricht. Der Empfänger muss sie freiwillig,

für einen konkreten Fall, in informierter Weise und unmissverständlich in Form einer Erklärung oder einer sonstigen eindeutigen Handlung abgeben. Das heißt: Ein schlichtes „Ja, ich möchte einen Newsletter erhalten“ reicht nicht aus.

Pflichtinformationen

Der Einwilligungstext muss alle datenschutzrechtlichen Pflichtinformationen enthalten. Damit er dennoch einigermaßen kurz und verständlich bleibt, setzt man am besten einen Link zur ohnehin notwendigen Datenschutzerklärung der eigenen Website. Dort muss dann ein ausführlicher Passus zum Newsletter-Versand enthalten sein.

Im Einwilligungstext selbst muss erkennbar sein, welcher Inhalt zu erwarten ist. Der Versender sollte das nicht zu eng, aber auch nicht zu weit fassen. Zum Beispiel kann ein „Newsletter für Gewinnspiele“ nicht für Produktwerbung verwendet werden. Die Formulierung „Newsletter für Werbebotschaften“ wäre hingegen zu weitreichend und damit unzulässig. Wichtig ist der Hinweis auf die Widerrufsmöglichkeit (siehe Formulierungsbeispiel für einen Einwilligungstext auf Seite 156).

Wenn Sie neben der E-Mail-Adresse zur Personalisierung des Newsletters auch den Namen abfragen, sollten Sie den Grund hierfür ebenfalls kurz im Einwilligungstext erwähnen. Die Erhebung weiterer Daten lässt sich mit dem Grundsatz der Datenminimierung jedoch nicht mehr vereinbaren.



Erfasst die Newsletter-Software nicht pseudonymisiert, wann der Empfänger die Mail öffnet und wann er welchen Link darin anklickt, muss der Versender auf dieses Tracking im Einwilligungstext hinweisen. Viele Datenschützer sind sogar der Ansicht, dass es dafür eine eigene Checkbox geben muss: Der Nutzer soll entscheiden dürfen, ob er den Newsletter mit oder ohne Tracking abonnieren möchte. Ansonsten läge – so die Rechtsmeinung – auch hier ein Verstoß gegen das Kopplungsverbot vor (siehe Seite 16).

Zustimmung per Double-Opt-in

Die DSGVO bestimmt, dass der Verantwortliche die Einwilligung in die Verarbeitung personenbezogener Daten nachweisen können muss. Das Double-Opt-in-Verfahren ist daher obligatorisch.

Weil der Newsletter-Versand erst startet, wenn der Link in einer Bestätigungs-Mail geklickt wurde, kann der Absender insbesondere verhindern, dass ein unbefugter Dritter die E-Mail-Adresse im Anmeldeformular angegeben hat. Die Bestätigungsmail selbst darf noch keine Werbung enthalten. Dagegen sollte aber der Einwilligungstext wiederholt werden.

Das gesamte Verfahren ist zu dokumentieren. Das bloße Abspeichern der IP-Adresse eines Newsletter-Abonnenten und die Behauptung, dass eine Einwilligung von diesem vorliege, reicht nach Ansicht des Bundesgerichtshofs dabei nicht aus (Urteil vom 10.02.2011, I ZR 164/09).

Beispiel für Erklärung der Ähnlichkeitswerbung

Wenn Sie bei uns Waren oder Dienstleistungen erwerben und hierbei Ihre E-Mail-Adresse angeben, behalten wir uns vor, diese für den Versand von Newslettern mit Direktwerbung für eigene ähnliche Waren oder Dienstleistungen zu verwenden. Dies dient der Wahrung unserer im Rahmen einer Interessensabwägung überwiegenden berechtigten Interessen an einer werblichen Ansprache unserer Kunden.

Sie können dieser Verwendung Ihrer Daten jederzeit durch eine Nachricht an [Adresse, E-Mail-Adresse] oder über den Abmeldelink in der Werbe-Mail widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen. Soweit der Newsletter-Versand aufgrund des Verkaufs von Waren oder Dienstleistungen erfolgt, berufen wir uns auf § 7 Abs. 3 UWG.

Newsletter

Anmelden

Bitte geben Sie Ihre E-Mail-Adresse ein, um diesen Newsletter zu abonnieren. Wir senden Ihnen daraufhin eine E-Mail zu. Um Missbrauch auszuschließen, wird die Zusendung des Newsletters erst dann freigeschaltet, wenn Sie unsere E-Mail bestätigt haben.

E-Mail-Adresse: (Pflichtfeld)

Anrede:

Bitte auswählen ▼

Vorname:

Nachname:

☒ Newsletter heise Download

Ich willige ein, dass mich Heise Medien per E-Mail über die von ihr angebotenen Zeitschriften, Online-Angebote, Produkte des heise Shops, Veranstaltungen und Software-Downloads informiert. Meine Daten werden ausschließlich zu diesem Zweck genutzt. Eine Weitergabe an Dritte erfolgt nicht. Ich kann die Einwilligung jederzeit per E-Mail an datenservice@heise.de, per Brief an Heise Medien GmbH & Co. KG, Vertrieb & Marketing, Karl-Wiechert-Allee 10, 30625 Hannover oder durch Nutzung des in den E-Mails enthaltenen Abmeldelinks widerrufen. Es gilt die Datenschutzerklärung von Heise Medien.

Anmelden



FAQ

Verfallsdatum?

? Wie lange ist eine erteilte Einwilligung für den Empfang von Newslettern gültig?

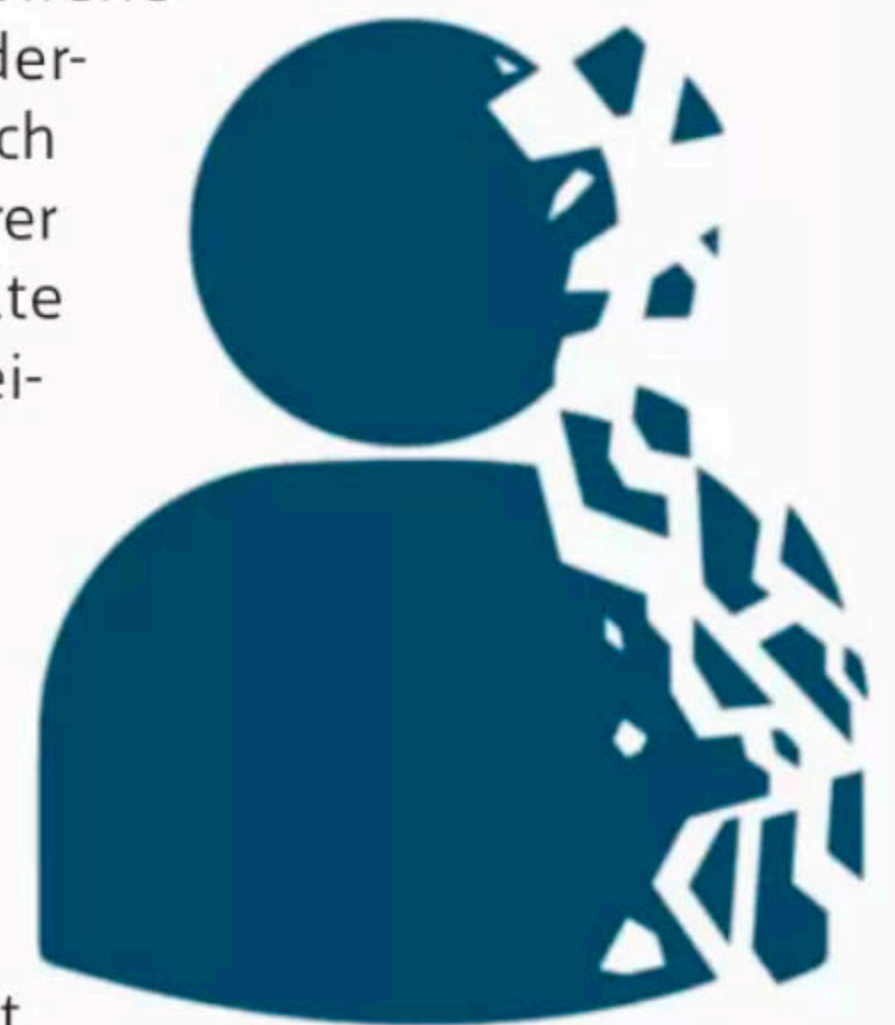
! Newsletter-Versender möchten zuweilen einen seit längerer Zeit nicht mehr genutzten Werbekanal reaktivieren. Aufgrund der Verunsicherung, ob die vormals eingeholte Einwilligung noch wirksam ist, versuchen sie die Empfänger durch einen Re-Opt-in „zurückzugewinnen“. Die Verunsicherung ist durchaus berechtigt, denn in der Rechtsprechung gibt es hierzu unterschiedliche Ansichten. Grundsätzlich ist eine erteilte datenschutzrechtliche Einwilligung solange gültig, bis der Betroffene sie widerruft. Das hat das Amtsgericht Bonn allerdings nicht davon abgehalten zu entscheiden, dass eine ungenutzte Einwilligung ihre Wirksamkeit verliert, wenn zwischen der Erteilung und der ersten Werbenachricht vier Jahre vergangen sind (AG Bonn, Urteil vom 10.05.2016, 104 C 227/15). Glücklicherweise wurde im Februar 2018 höchstrichterlich genau das Gegenteil entschieden. Der Bundesgerichtshof urteilte, dass eine Einwilligung nicht allein durch Zeitablauf erlischt (BGH, Urteil vom 01.02.2018, III ZR 196/17). Newsletter-Opt-ins haben somit kein Verfallsdatum.

Lösch mich!

? Ein Newsletter-Abonnent hat seine Einwilligung widerrufen und fordert mich gleichzeitig zur Löschung seiner E-Mail-Adresse auf. Muss ich diese auch aus der Blacklist löschen?

! Um zu gewährleisten, dass ein Widerspruch oder der Widerruf einer Einwilligung auch tatsächlich berücksichtigt wird, sollte man betroffene E-Mail-Adressen nicht nur aus dem Verteiler löschen, sondern diese gleichzeitig in einer Werbsperrdatei speichern. Da diese Blacklist zur Sicherstellung des geltend gemachten Rechtsanspruchs benötigt wird, ist das Führen dieser Liste auch datenschutzrechtlich zulässig. Über deren Sinn und Zweck sollten die Betroffenen in der Datenschutzerklärung unterrichtet werden.

Soweit eine betroffene Person neben dem Widerruf der Einwilligung auch explizit die Löschung ihrer Daten verlangt, sollte man sie darauf hinweisen, dass sie bei einem künftigen, rechtlich zulässigen Einsatz von Daten gegebenenfalls wieder Werbung erhalten könnte. Diese Vorgehensweise empfiehlt zumindest die Datenschutzkonferenz (DSK) in ihrer Orientierungshilfe zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung (siehe [ct.de/w2w7](https://www.ct.de/w2w7)).



Checkbox

? Ich möchte ein Newsletter-Abonnement in den Kaufprozess meines Onlineshops integrieren. Wie löse ich das rechtlich sauber?

! Wenn der Versender die Einwilligung während anderer Vorgänge einholt, etwa beim Abschluss eines Kaufvertrags in einem Online-Shop, muss das separat mit einer nicht vorausgefüllten Checkbox erfolgen. Nur so wird das Kriterium der „eindeutigen Handlung“ erfüllt. Die Erklärung darf auch nicht mit dem Abhaken der Allgemeinen Geschäftsbedingungen kombiniert werden. Unzulässig ist es auch, den Kunden den gesamten Bestellprozess des Online-Shops durchlaufen zu lassen und ihm ohne abgegebene Werbeeinwilligung den Kauf zu verwehren – das wäre ein Verstoß gegen das Kopplungsverbot des Art. 7 Abs. 4 DSGVO. Die Einwilligung wäre in diesem Fall nicht freiwillig erteilt worden. (keh) **ct**

DSK-Hilfe zur Direktwerbung und Beispiele Ähnlichkeitswerbung und Newsletter:

[ct.de/w2w7](https://www.ct.de/w2w7)

Cookies



Opt-In oder Opt-Out? Wie soll ich das Cookie-Banner gestalten? Das sind Fragen, die sich Website-Betreiber stellen, wenn sie sich mit dem datenschutzkonformen Einsatz von Cookies beschäftigen. Entscheidungen der obersten Gerichte bringen Licht ins Dunkel.

Von Nicolas Maekeler

Seit dem Start der DSGVO greift das Phänomen der Cookie-Hinweise immer weiter um sich. Kaum ein Webauftritt, bei dem nicht auf der Startseite ein Banner aufpoppt, das häufig schnell weggeklickt wird, weil es meist die Inhalte der Seite überdeckt. Warum ist es überhaupt erforderlich, mit Hinweistexten, Schaltflächen und Auswahlmenüs, den Einsatz von Cookies auf Websites zu steuern?

Datenpakete voller Informationen

Cookies sind nicht per se datenschutzrechtlich bedenklich. In vielen Fällen ist ihr Einsatz für grundlegende Funktionen der Website erforderlich oder zumindest nützlich, etwa um die bevorzugte Sprache, Seiteneinstellungen oder – im Falle eines Onlineshops – den Inhalt eines Warenkorb zu speichern. Darüber hinaus werden Cookies aber auch für die Website-Analyse verwendet. So ist es Website-Betreibern möglich, wiederkehrende Besucher zu erkennen und typische Klickpfade zu verfolgen.

Einen eher schlechten Ruf haben Cookies im Zusammenhang mit Online-Werbung. Mithilfe der kleinen Datenpakete tracken Werbetreibende Internetnutzer über viele Websites hinweg und legen von ihnen individuelle Profile an, um so gezielt personalisierte Werbung anzeigen zu können. Neben Informationen zur verwendeten Hard- oder Software können Cookies auch Informationen enthalten, die

einen Website-Besucher identifizierbar machen: IP-Adresse, E-Mail-Adresse, Name, Telefonnummer oder eine „unique user ID“.

An dieser Stelle kommt der Datenschutz ins Spiel: Die DSGVO regelt in Art. 4, dass auch Online-Kennungen, über die Personen identifiziert werden können, als personenbezogene Daten anzusehen sind. Für den Datenschutz nicht relevant sind somit technisch notwendige Cookies, die keine Wiedererkennung eines Website-Besuchers ermöglichen. Bei der Verwendung von Cookies, die einen Nutzer beispielsweise als „unique user“ identifizieren, ist hingegen der Anwendungsbereich der DSGVO eröffnet.

Rechtsgrundlage für Cookies

Für die Verwendung derartiger Cookies muss daher ein Erlaubnistatbestand des Artikel 6 DSGVO vorliegen. Es kommt mittlerweile dafür regelmäßig nur noch eine Einwilligung der Website-Besucher in Betracht.

Angesichts der undurchsichtigen Rechtslage nutzen viele Website-Betreiber noch vor geraumer Zeit auch die umstrittenen Marketing-Cookies wie gewohnt ohne Einwilligung mittels einer Opt-Out-Lösung. Insbesondere um den Einsatz von Webseitenanalyse-Cookies, etwa bei Google Analytics, machte man sich wenig Sorgen. Man berief sich auf die Rechtsgrundlage des Art. 6 Abs. 1 lit. f) DSGVO (Datenverarbeitung zur Wahrung berechtigter Interessen).

Tracking von Nutzern

Allerdings hatte sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) bereits im April 2018 in einem Positionspapier (siehe [ct.de/w54s](https://www.ct.de/w54s)) zu der Thematik geäußert. In dem Papier, das sich mit den rechtlichen Anforderungen an das Tracking von Nutzern auf Websites

beschäftigt, positionieren sich die Datenschützer eindeutig: „Es bedarf jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, und bei der Erstellung von Nutzerprofilen.“ Vor dem Verwenden von Analysewerkzeugen wie Google Analytics oder von Werbetrackern müsse daher vorab eine informierte

Checkliste Cookie-Banner & Consent-Tools

Folgende Punkte sind zu berücksichtigen, wenn mittels Cookie-Banner eine Einwilligung zur Nutzung von einwilligungsbedürftigen Cookies oder anderer Verfahren zur Verfolgung der Nutzer (Zählpixel, Browserfingerprinting usw.) eingeholt werden soll:

- Das Cookie-Banner muss beim erstmaligen Öffnen der Website erscheinen, zum Beispiel als eigenes HTML-Element. Es sollte eine Übersicht aller einwilligungsbedürftigen Verarbeitungsvorgänge enthalten.
- Über folgende Punkte sollte das Banner informieren:
 - Art und Funktionsweise der jeweiligen Cookies
 - Lebensdauer
 - Identität der Dienstleister, die die Cookies verarbeiten
- Auswahlmöglichkeiten dürfen nicht voreingestellt sein, sondern müssen vom Nutzer aktiviert werden.
- Während das Banner angezeigt wird, müssen alle Technologien, die potenziell Nutzerdaten erfassen, deaktiviert sein.
- Der Zugriff auf Impressum und Datenschutzerklärung darf durch das Banner nicht verhindert werden. Auf die Datenschutzerklärung sollte bestenfalls innerhalb des Banners verlinkt werden.
- Es muss technisch sichergestellt sein, dass die Datenverarbeitung erst stattfindet, wenn der Nutzer seine Einwilligung(en) durch das Setzen von Häkchen oder das Betätigen einer Schaltfläche abgegeben hat.
- Damit die Entscheidung des Nutzers berücksichtigt wird und das Banner nicht erneut erscheint, kann das Ergebnis auf dem Endgerät des Nutzers gespeichert werden, allerdings ohne Verwendung einer User-ID.
- Es muss eine Möglichkeit zum Widerruf implementiert werden. Der Widerruf muss so einfach möglich sein wie die Erteilung der Einwilligung.

Die DSK macht sehr konkrete Angaben, wie eine notwendige Einwilligung für den Einsatz von Cookies technisch einzuholen sei. Die Aussagen der DSK sind zwar nicht rechtlich bindend, machen jedoch deutlich, wie die Datenschutzbehörden das europäische Datenschutzrecht auslegen und anwenden werden.

Einwilligung eingeholt werden. Nur wenn der Einsatz von Cookies unbedingt erforderlich sei, um dem Nutzer den angefragten Online-Service zur Verfügung stellen zu können, soll man sich auf andere Rechtsgrundlagen berufen können.

Mitte April 2019 legte die DSK ergänzend eine „Orientierungshilfe für Anbieter von Telemedien“ vor (siehe [ct.de/w54s](https://www.ct.de/w54s)), in der sie ihre Position ausführlicher darlegt und begründet. Bei „Tracking“ handle es sich um „Datenverarbeitungen zur – in der Regel Website-übergreifenden – Nachverfolgung des individuellen Verhaltens von Nutzern“.

Planet49-Entscheidung des EuGH

Weitaus mehr Gewicht für die Frage wann und wie eine Einwilligung für die Nutzung von Cookies eingeholt werden muss, haben Entscheidungen des Europäischen Gerichtshofs (EuGH Urteil vom 01.10.2019, Az. C-673/17 „Planet49“) und des Bundesgerichtshofs (BGH Urteil vom 28.05.2020, Az. I ZR 7/16, siehe [ct.de/w54s](https://www.ct.de/w54s)). Die Gerichte hatten über eine Klage des Bundesverbandes der Verbraucherzentralen gegen den Glücksspielanbieter Planet49 zu entscheiden. Dieser hatte im Rahmen einer Gewinnspielregistrierung die Einwilligung zum Setzen und Auswerten von Cookies verlangt. Allerdings war der Text der Einwilligungserklärung mit einem voreingestellten Häkchen bereits angewählt und musste von den Teilnehmern erst deaktiviert werden. Der EuGH urteilte, dass eine wirksame Einwilligung ein aktives Verhalten des Nutzers voraussetzt, was durch eine voreingestellte Opt-Out-Funktion nicht ermöglicht werde.

Das Gericht stellte auch klar, dass neben Cookies auch vergleichbare Technologien dem Einwilligungsvorbehalt unterfallen, selbst wenn keine personenbezogenen Daten verarbeitet werden. Der BGH schloss sich diesen Einschätzungen an. Dies bedeutet jedoch nicht, dass nun für jedes Cookie eine Einwilligung eingeholt werden muss. Ausgenommen sind die Arten von Cookies, die unbedingt erforderlich sind, damit der Anbieter seine Dienste zur Verfügung stellen kann. Dies ist dann der Fall, wenn die Speicherung von Informationen technisch notwendig ist, wie etwa bei Warenkorb- und Session-Cookies.

Unwirksame Einwilligung

Die Vorgaben der Datenschutzbehörden und die durch die jüngste Rechtsprechung entwickelten Grundsätze sind mittlerweile hinreichend konkret.

Beispiel für Cookie-Banner

Cookie-Banner lassen sich auf unterschiedlichste Weise gestalten. Möchte man alles richtig machen, nehmen die Hinweise und Schaltflächen einen Großteil des Bildschirms ein. Der Berliner Rechtsanwalt Dr. Thomas Schwenke zeigt auf seiner Website datenschutz-generator.de, wie man es machen sollte. Bereits im ersten Layer des Banners hat man mit einem Klick die Möglichkeit, alle nicht notwendigen Cookies loszuwerden. Die bereitgestellten Informationen sind umfangreich. Es wird sogar auf die Datenverarbeitung in den USA und die damit verbundenen Risiken hingewiesen.



Cookie-Einstellungen

Hinweis auf den Einsatz von Cookies: Wir setzen auf unserer Website Cookies ein. Einige von ihnen sind notwendig (z.B. für den Warenkorb), während andere uns helfen unser Onlineangebot zu verbessern und wirtschaftlich zu betreiben. Sie können die nicht notwendigen Cookies akzeptieren oder per Klick auf die Schaltfläche "Nur notwendige Cookies akzeptieren" ablehnen sowie diese Einstellungen jederzeit aufrufen und Cookies auch nachträglich jederzeit abwählen (z.B. im Fußbereich unserer Website).

Hinweis auf Verarbeitung Ihrer auf dieser Webseite erhobenen Daten in den USA durch Google, Facebook, LinkedIn, Twitter, Youtube: Indem Sie auf "Ich akzeptiere" klicken, willigen Sie zugleich gem. Art. 49 Abs. 1 S. 1 lit. a DSGVO ein, dass Ihre Daten in den USA verarbeitet werden. Die USA werden vom Europäischen Gerichtshof als ein Land mit einem nach EU-Standards unzureichendem Datenschutzniveau eingeschätzt. Es besteht insbesondere das Risiko, dass Ihre Daten durch US-Behörden, zu Kontroll- und zu Überwachungszwecken, möglicherweise auch ohne Rechtsbehelfsmöglichkeiten, verarbeitet werden können. Wenn Sie auf "Nur essenzielle Cookies akzeptieren" klicken, findet die vorgehend beschriebene Übermittlung nicht statt. ([Erläuterungen zu dem Hinweis auf die US-Transfers](#))

Weitere Hinweise erhalten Sie in unserer [Datenschutzerklärung](#)

Hinweis: Wir nutzen das Cookie-Opt-In-Plugin für Wordpress von [BORLABS](#).

☒ Essenziell ☒ Marketing

Ich akzeptiere

Nur essenzielle Cookies akzeptieren

[Individuelle Cookie-Einstellungen](#)

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

Der Cookie-Banner des Berliner Rechtsanwalts Dr. Thomas Schwenke zeigt, wie es richtig geht.

Eine wirksame Einwilligung setzt demnach voraus, dass der Website-Besucher aktiv die Wahl haben muss, zu entscheiden, ob er Cookies zulassen will oder nicht. Er muss zudem auswählen können, welche Arten von Cookies er zulassen will oder nicht. Etliche Cookie-Hinweise verdecken in Form eines großen Layers fast die gesamten Inhalte einer Website und bieten lediglich die Möglichkeit, mittels eines einzelnen OK-Buttons alle Arten von Cookies zu akzeptieren. Ohne Einwilligung kann man die Website somit nicht nutzen. In solchen Fällen gilt

die Einwilligung nicht als freiwillig erteilt und ist daher unwirksam.



Häufig liest man auch Sätze wie „Durch die Nutzung der Website erklären Sie sich mit der Verwendung von Cookies einverstanden“. Derartige Formulierungen genügen den datenschutzrechtlichen

Anforderungen nicht, hier fehlt es an einer Erklärung oder sonstigen eindeutig bestätigenden Handlung.

Informierte Einwilligung

Eine Erklärung kann nur abgeben, wer hinreichend über den Einsatz von Cookies informiert wird. Ein Banner, der aus Platzgründen zunächst rudimentär darauf hinweist, für welche Zwecke Cookies genutzt werden, kann das Thema nur anreißen. Ein Link zur Datenschutzerklärung oder einer gesonderten Cookie-Policy, in der alle Pflichtinformationen sowie Ausführungen zu den verwendeten Cookies inklusive ihrer Funktionsdauer und möglicher Zugriffe durch Dritte enthalten sind, ist daher verpflichtend. Nutzer müssen darüber hinaus transparent auf den Einsatz von US-Dienstleistern und die damit verbundenen Risiken hingewiesen werden.

Nicht selten ist zu beobachten, dass zwar ein, den Kriterien einer wirksamen Einwilligung entsprechender Cookie-Banner vorhanden ist, beim Besuch der Website jedoch im Hintergrund bereits Cookies

Tipps für Verbraucher

Für viele Online- bzw. E-Commerce-Anbieter sind Cookies ein wichtiges Instrument, um Daten von (potenziellen) Kunden zu sammeln und so Aufschluss über deren spezifische Interessen zu erhalten. Mit Hilfe der kleinen Datenpakete können Website-Betreiber das Surfverhalten ihrer Nutzer theoretisch über Jahre verfolgen. Die gesammelten Informationen ergeben ein umfassendes Nutzerprofil, was sich für Werbezwecke gut vermarkten lässt.

Durch die strengen Anforderungen der DSGVO haben Internetnutzer ein Stück weit die Kontrolle über ihre Daten zurückerlangt. Rechtlich sauber umgesetzte Einwilligungslösungen (Consent Management Platform) bieten einen echten Mehrwert. Auch wenn die beim Website-Besuch aufpoppenden Banner als oft lästig empfunden werden, investieren sie ein paar Mausklicks, um weniger digitale Spuren im Netz zu hinterlassen.

Fallen Sie dabei nicht auf die psychologischen Tricks der Website-Betreiber herein. Meist sind „Zustimmen-Buttons“ farblich akzentuiert, vornehmlich grün, um die Nutzer dazu zu verleiten, ihr Einverständnis in die Cookie-Nutzung zu erteilen. Suchen Sie also vornehmlich nach unscheinbaren Schaltflächen, um den Datenfluss zu unterbinden. Nicht selten versteckt sich die Schaltfläche zum Ablehnen auch erst auf der zweiten Ebene des Banners.

Wem das individuelle Einstellen von Cookie-Berechtigungen über Cookie-Banner zu aufwendig ist, der kann auch im genutzten Browser entsprechende Regeln aufstellen. Unter den Datenschutzeinstellungen können Sie festlegen, welche Websites zum Setzen von Cookies berechtigt sind und insbesondere Drittanbieter-Cookies einschränken. Außerdem können Sie einstellen, dass die Cookies nach jeder Sitzung automatisch gelöscht werden.

in den Browser geladen werden, obwohl der Nutzer dem noch nicht zugestimmt hat. Dabei wird außer Acht gelassen, dass eine vorherige Einwilligung eingeholt werden muss und nicht eine nachträgliche Genehmigung. Ein rechtlich einwandfreier Einwilligungstext nützt wenig, wenn eine entsprechende technische Umsetzung nicht erfolgt.

Googles Marktmacht

Auch seitens der großen Internetunternehmen wird Druck gemacht. Wer etwa Googles Werbe- und Measurement-Produkte, Google Maps, YouTube oder reCAPTCHA auf der eigenen Website nutzt, muss der „Richtlinie zur Einwilligung der Nutzer in der EU“ (siehe [ct.de/w54s](https://www.google.com/policies/consent/)) zustimmen. Diese fordert von Website-Betreibern, dass sie von Endnutzern eine Einwilligung für den Einsatz von Cookies oder anderer Formen der lokalen Speicherung von Informationen einholen und dieses auch dokumentieren. Auch Facebook empfiehlt für das Facebook-Pixel – ein Analyse-

tool, mit dem man die Effektivität eigener Werbung messen kann – eine Opt-In-Lösung. Anstatt die angebotenen Dienste datenschutzfreundlicher zu gestalten, wird die Verantwortung gerade von Seiten der Internetgiganten offenbar lieber auf die einzelnen Website-Betreiber abgewälzt.

Ausblick

Wer denkt, mit der DSGVO hätte man nun eine beständige Rechtslage in Bezug auf Cookies, liegt daneben. Denn der nächste große Wurf der EU ist schon im Anmarsch: die ePrivacy-Verordnung. Diese sollte eigentlich zeitgleich mit der DSGVO den Bereich der elektronischen Kommunikation neu regeln. Ob und wann die Verordnung in Kraft treten wird, ist noch unklar. Zuvor wird auf nationaler Ebene das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft treten, welches ein Einwilligungserfordernis in das Speichern von Informationen in Endeinrichtungen des Nutzers enthalten wird.



Nicht essbar

? Was sind eigentlich Cookies?

! Bei Cookies handelt es sich um kleine Text-Pakete, die von einer Website an den Browser geschickt werden können und von diesem gespeichert und wieder zurückgeschickt werden. In Cookies können unterschiedliche Angaben gespeichert wer-

den, die von der Stelle, die den Cookie setzt, ausgelesen werden. Sie enthalten in der Regel eine charakteristische Zeichenfolge (ID), die eine eindeutige Identifizierung des Browsers beim erneuten Aufrufen der Website oder einem Seitenwechsel ermöglicht. Sie dienen in erster Linie dazu, Online-Angebote nutzerfreundlicher und effektiver zu gestalten, aber auch um Nutzern gezielt personalisierte Werbung anbieten zu können. Die in Cookies erhobenen Daten der Nutzer werden meist pseudonymisiert, wodurch eine Zuordnung zum Nutzer in Person nicht möglich ist. Es gibt jedoch auch Fälle, bei denen die Identifizierbarkeit gegeben ist, wie etwa bei einem Login-Cookie, dessen Session-ID notwendigerweise mit dem Account des Users verknüpft ist.

Verschiedene Sorten

? Ist Cookie gleich Cookie? Oder gibt es da Unterschiede?

! Es gibt verschiedene Arten von Cookies. Bei transienten Cookies, die auch als temporäre oder

Session-Cookies bezeichnet werden, handelt es sich um Cookies, die gelöscht werden, wenn man die entsprechende Website verlässt und den Browser schließt. In derartigen Cookies werden zum Beispiel Spracheinstellungen oder der Inhalt eines Warenkorbs gespeichert.

Persistente oder permanente Cookies bleiben hingegen auch nach dem Schließen des Browsers gespeichert. Sie enthalten beispielsweise den Login-Status oder eingegebene Suchbegriffe. Derartige Cookies werden auch für Reichweitenmessungen oder Marketingzwecke genutzt. Gelöscht werden sie in der Regel automatisiert nach einer vorgegebenen Dauer oder händisch in den Sicherheitseinstellungen des Browsers.

Darüber hinaus muss man insbesondere zwischen First-Party-Cookies, die von der besuchten Website selbst gesetzt werden, und Third-Party-

Cookies, die von anderen Anbietern gesetzt werden, unterscheiden.

Einwilligungsnachweis

? Wie weise ich nach, dass ein Nutzer eine Cookie-Einwilligung erteilt hat?

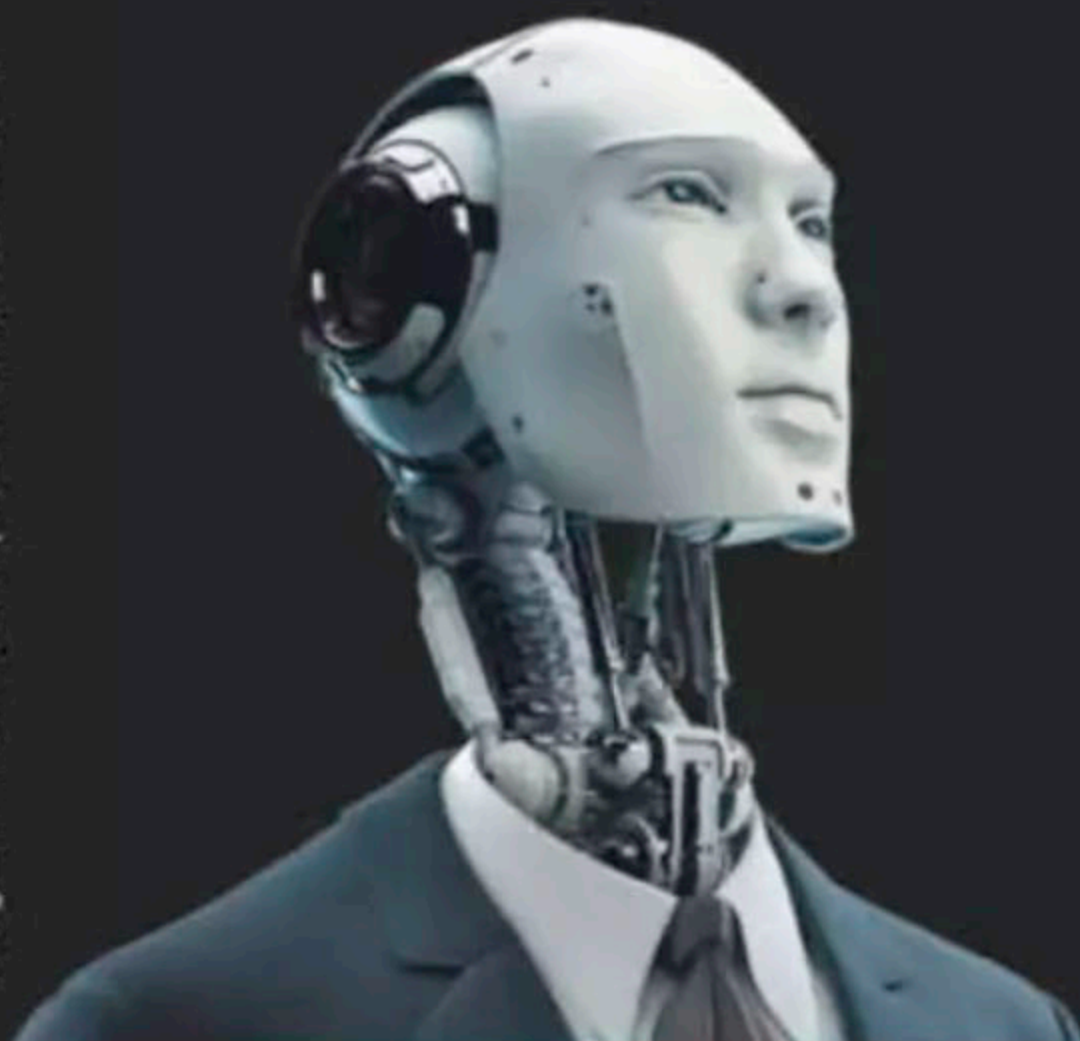
! Im Rahmen der Rechenschaftspflicht sind Web-sitebetreiber verpflichtet auch nachweisen zu können, dass ein Nutzer eine Einwilligung ins Speichern von Cookies erteilt hat. Die auf dem Markt verfügbaren Cookie-Tools nutzen hierfür in der Regel ein ID-System. Dabei wird oft ein Cookie auf dem Endgerät gespeichert. Für das Setzen derartiger Cookies muss keine Einwilligung eingeholt werden, sie fallen in die Kategorie „unbedingt erforderlich“. (keh) **ct**



**DSK-
Positionspapier,
EU-Richtlinie:**

ct.de/w54s

*Ausgabe 11/2013: Computer machen die Arbeit.



Alle reden heute
über die Zukunft
der Arbeit –
wir seit 2013.*

**Technology
Review**
Das Magazin für Innovation

**Testen Sie 3 Ausgaben Technology
Review mit 35 % Rabatt.**

Jetzt bestellen: trvorteil.de/testen

✉ leserservice@heise.de

☎ +49 541/80 009 120

+ Ihr
Geschenk:



Smartwatch



**Lesen, was wirklich zählt in Energie,
Digitalisierung, Mobilität, Biotech.**



DSGVO für Fotografen

Ob auf Webseiten oder in Firmenzeitschriften und Flyern: Fotos sind ein gern genutztes Gestaltungselement. Lesen Sie, welche Bilder Sie unter welchen Voraussetzungen machen und veröffentlichen dürfen und welche Anforderungen die DSGVO sonst noch an Fotografen stellt.

Von Nicolas Maekeler

Menschen zu fotografieren, heißt gleichzeitig auch personenbezogene Daten zu verarbeiten. Betätigt der Fotograf den Auslöser seiner Kamera und eine Person erscheint vor der Linse, benötigt er eine datenschutzrechtliche Legitimation. Das gilt in der Regel sogar dann, wenn die fotografierte Person nicht eindeutig zu erkennen ist. Denn bei moderner digitaler Fotografie kann davon ausgegangen werden, dass anhand zusätzlich gespeicherter Daten eine Person identifiziert werden kann. Datum, Uhrzeit und GPS-Daten einer Aufnahme

lassen neben dem eigentlichen Bildnis Rückschlüsse zu, wann sich die betroffene Person wo befunden hat. Damit stehen auch Fotografen vor der Aufgabe, die Erfordernisse der DSGVO im Alltag praktikabel umzusetzen.

KUG vs. DSGVO

Wenig hilfreich ist hierbei die unbefriedigende Rechtslage. Seit dem Wirksam werden der DSGVO hat nämlich das Kunsturhebergesetz (KUG), welches

seit 1907 das Veröffentlichen von Bildnissen regelt, an Bedeutung verloren. Es wird von der DSGVO weitestgehend verdrängt, weil diese den Bereich des Datenschutzes abschließend regelt.

Lediglich Fotojournalisten, die unter das sogenannte Medienprivileg fallen, können sich noch auf die alten Regelungen des KUG verlassen. Dies bestätigt ein Beschluss des Oberlandesgerichts (OLG) Köln (OLG Köln, Beschl. v. 18.06.2018 – Az.: 15 W 27/18), wonach das KUG für journalistische Zwecke weiterhin gültig ist. Im Bereich der gewerblichen, beziehungsweise kommerziellen Personenfotografie besteht weiterhin Rechtsunsicherheit.

Fotografieren nur mit Erlaubnis

Datenschutzrechtlich betrachtet ist es nämlich grundsätzlich verboten, Aufnahmen von Personen anzufertigen und zu veröffentlichen. Möglich ist es laut DSGVO dennoch, wenn eine Erlaubnis vorliegt. Man spricht insoweit von einem Verbot mit Erlaubnisvorbehalt für die Verarbeitung personenbezogener Daten. Demnach ist eine Datenverarbeitung zulässig, wenn entweder eine Einwilligung des Betroffenen oder eine anderweitig gesetzlich geregelte Erlaubnis vorliegt.

Lächeln reicht nicht

In der Prä-DSGVO-Ära wurde ein Lächeln in die Kamera unter gewissen Umständen als konkludentes Einverständnis, also als stillschweigende Willenserklärung gewertet. Jetzt muss eine datenschutzrechtliche Einwilligung freiwillig, bestimmt, in informierter Weise und unmissverständlich eingeholt werden. Dafür sind dem Betroffenen gegenüber zunächst alle notwendigen Informationspflichten zu erfüllen. Im Zweifelsfall muss man nachweisen können, dass eine Einwilligung tatsächlich erteilt wurde. Der

Fotograf sollte daher alles schriftlich dokumentieren. Ein unterschriebenes Einwilligungsformular nebst Datenschutzerklärung ist nötig.

Vorsicht vor Einwilligung



Allerdings sollte man nur auf die Einwilligung zurückgreifen, wenn man sich auf keine andere Rechtsgrundlage berufen kann. Denn diese kann frei widerrufen werden. Schlimmstenfalls müssten dann bereits veröffentlichte Fotos umständlich gelöscht oder geschwärzt werden. Insofern ist die Einwilligung ein eher unsicheres Instrument für Fotografen. Nach dem KUG war der Widerruf von Einwilligungen in Fotoaufnahmen, abgesehen von strengen Ausnahmen, fast unmöglich. Es mussten schon wichtige Gründe hierfür vorliegen, was der Rechtssicherheit zugutekam. Der Widerruf einer Einwilligung nach DSGVO kann hingegen ohne die Angabe von Gründen erfolgen.

Berechtigte Interessen

Zur Einwilligung gibt es im Bereich der Fotografie Alternativen. Laut Art. 6 Abs. 1 lit. f DSGVO ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen, Grundrechte und -freiheiten der betroffenen Person dem nicht entgegenstehen. Dabei kommen rechtliche, wirtschaftliche, aber auch ideelle Interessen des Verantwortlichen in Betracht, wie zum Beispiel bei der Eventfotografie (siehe Seite 174).

Die Ausübung der Tätigkeit als Fotograf fällt unter die grundrechtlich geschützte Kunstfreiheit. Auch die Freiheit der Meinungsäußerung und die Informationsfreiheit begründen ein entsprechendes Interesse. In vielen Fällen



stehen dem auch keine schutzwürdigen Interessen der fotografierten Personen entgegen, etwa bei Fotografien im öffentlichen Raum, da hier nur die Sozial-sphäre des Abgelichteten betroffen ist. Der Fotografierte hat zwar aus Gründen, die sich aus seiner besonderen Situation ergeben, das Recht, gegen die Verarbeitung seiner personenbezogenen Daten Widerspruch einzulegen. Aufgrund der Interessenabwägung muss dies aber nicht zwangsläufig Erfolg haben. Im Gegensatz zur Einwilligung ist dies also ein echter Vorteil der Rechtsgrundlage der berechtigten Interessen.

Fotografieren im Auftrag

Wird ein Fotograf beauftragt, Aufnahmen zu machen, darf er die Daten des Auftraggebers für die Erfüllung des Vertrages verarbeiten, das heißt, ihn ablichten, wie zum Beispiel bei Bewerbungsfotos. Auch für das Brautpaar, das einen Hochzeitsfotografen engagiert hat, gilt diese Rechtsgrundlage. Problematisch wird es bei den Hochzeitsgästen, da sie selbst dem Fotografen nicht den Auftrag und somit die Erlaubnis erteilt haben. Hier kann aber von der Wahrung berechtigter Interessen gesprochen werden. Laut Erwägungsgrund 47 der DSGVO liegt ein „berechtigtes Interesse“ vor, „wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, etwa wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht“. Es lässt sich gut vertreten, dass man beim Besucher einer Hochzeit, eines Konzerts oder einer Sportveranstaltung vom Vorhandensein einer solchen angemessenen Beziehung zwischen Veranstalter und Besucher ausgehen kann.

Haushaltsprivileg für private Fotos

Für Hobbyfotografen, die Bilder im privaten Bereich schießen, gilt weiterhin das KUG. Die DSGVO regelt nicht die Verarbeitung personenbezogener Daten im persönlichen oder familiären Bereich. Dieses Haushaltsprivileg gilt auch für die Nutzung sozialer Netzwerke und anderer Online-Tätigkeiten. Nach Ansicht der Datenschutzbehörden muss man aber sehr genau differenzieren: Macht man Personenfotos einem unbeschränkten Personenkreis zu-

gänglich, gilt dies nicht mehr als ausschließlich persönliche oder familiäre Nutzung. Wenn man hingegen innerhalb geschlossener Nutzergruppen oder in passwortgeschützten Bereichen einer Web-

site private Fotos ins Netz stellt, muss man das Datenschutzrecht nicht berücksichtigen. Als Faustformel gilt: Je mehr Menschen involviert sind, desto eher fehlt es an einer persönlichen Verbundenheit und die Anwendung des Haushaltsprivilegs scheidet aus.

Auch professionelle Analog-Fotografen können zum Teil aufatmen. Solange sie ihre Bilder nicht digitalisieren oder die Abzüge bzw. Negative nicht nach bestimmten

Kriterien, wie etwa nach Aufnahmezeitpunkt, systematisch ordnen oder verschlagworten, findet die DSGVO auch hier keine Anwendung. Konkret: Die ungeordnete Sammlung loser Polaroids in einem Karton unterliegt nicht der DSGVO, dieselben Bilder in einem nach Jahren sortierten Fotoalbum eingeklebt, aber sehr wohl.

Die gesamte Auseinandersetzung mit der Thematik zeigt: Die Rechtslage ist in Bezug auf Personenfotografie kompliziert. Hier sollte der deutsche Gesetzgeber dringend nachbessern. Bis es so weit ist, lassen sich auch mit der DSGVO einigermaßen praktikable Lösungen für Fotografen finden. Weitere konkrete Tipps hierzu lesen Sie auf den folgenden Seiten.

(keh) **ct**



Für Maker!

Zubehör und Lesestoff

shop.heise.de/gadgets



Waveshare Game HAT für Raspberry Pi

Ein Muss für jeden Retro Gamer! Verwandeln Sie Ihren Raspberry Pi in kürzester Zeit in eine Handheld-Konsole. Mit Onboard-Speakern, 60 Frames/s, Auflösung von 480x320 und kompatibel mit allen gängigen Rasperrys.

shop.heise.de/game-hat

41,90 € >

BEST-SELLER



ODROID-GO

Mit diesem Bauplatz emulieren Sie nicht nur Spiele-Klassiker, sondern programmieren auch in der Arduino-Entwicklungsumgebung.

shop.heise.de/odroid

49,90 € >



NVIDIA Jetson nano

Das Kraftpaket bietet mit 4 A57-Kernen und einem Grafikprozessor mit 128 Kernen ideale Voraussetzungen für die Programmierung neuronaler Netze, die ähnlich wie Gehirnzellen arbeiten. **Inklusive Netzteil!**

shop.heise.de/jetson

134,90 € >

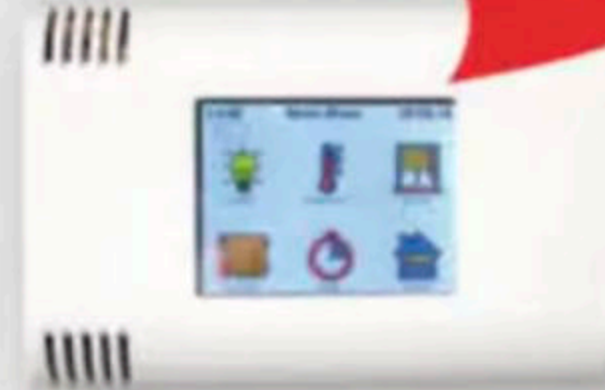


Raspberry Pi-Kameras

Aufsteckbare Kameras, optimiert für verschiedene Raspberry Pi-Modelle mit 5 Megapixel und verschiedenen Aufsätzen wie z. B. Weitwinkel für scharfe Bilder und Videoaufnahmen.

shop.heise.de/raspi-kameras

ab 18,50 € >



NEUER PREIS!

ArduiTouch-Set

Setzen Sie den ESP8266 oder ESP32 jetzt ganz einfach im Bereich der Hausautomation, Metering, Überwachung, Steuerung und anderen typischen IoT-Applikationen ein! Dieses Gehäuseset beinhaltet ein formschönes Wandgehäuse mit integrierter Leiterplatte.

shop.heise.de/arduitouch

~~60,90 €~~

36,90 € >



NEU

„No Signal“ Smartphone-Hülle

Passend für Smartphones aller Größen bis 23cm Länge blockt diese zusammenrollbare Hülle alle Signale von GPS, WLAN, 3G, LTE, 5G und Bluetooth, sowie jegliche Handy-Strahlung.

shop.heise.de/no-signal-sleeve

29,90 € >



NEUER PREIS!

Komplettset Argon ONE Case mit Raspberry Pi 4

Das Argon One Case ist eines der ergonomischsten und ästhetischsten Gehäuse aus Aluminiumlegierung für den Raspberry Pi. Es lässt den Pi nicht nur cool aussehen, sondern kühlt auch perfekt und ist leicht zu montieren. Praktisch: alle Kabel werden auf der Rückseite gebündelt ausgeführt – kein Kabelsalat!

shop.heise.de/argon-set

~~117,60 €~~

99,90 € >



Stockschirm protec'ted

Innen ist Außen und umgekehrt. Dieser etwas andere Regenschirm sorgt für interessierte Blicke auch bei grauem und nassem Wetter. Als Highlight kommt noch das stilvolle und dezente Design in Schwarz und Blau mit der mehr als passenden Aufschrift "Always protec'ted" daher.

shop.heise.de/ct-schirm

22,90 € >

> Bestellen Sie ganz einfach online unter **shop.heise.de** oder per E-Mail: **service@shop.heise.de**

> Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise shop

shop.heise.de >



Rechtssicher fotografieren

Von Nicolas Maekeler

Online-Dienstleister

? Ich nutze einen Online-Dienstleister, um meinen Kunden per Download Bilder bereitzustellen. Muss ich mit ihm das Thema Datenschutz vertraglich regeln?

! Sobald Personenfotos oder die Namen der Kunden an den Dienstleister übermittelt werden, muss man die DSGVO beachten. Der Fotograf hat dafür Sorge zu tragen, dass bei der Verarbeitung der personenbezogenen Daten seiner Kunden oder Fotomodelle die DSGVO-Vorschriften eingehalten werden.

Grundsätzlich ist eine Übermittlung personenbezogener Daten nur erlaubt, wenn eine Einwilligung des Betroffenen oder eine gesetzliche Erlaubnis vorliegt. Werden Dritte mit der Datenverarbeitung beauftragt, müsste der Fotograf von allen Kunden das Einverständnis dafür einholen.

Um die Vorgehensweise zu erleichtern, hilft die sogenannte Auftragsverarbeitung (siehe Seite 56). Der beauftragte Dienstleister wird nicht mehr als Dritter angesehen, weil er den Weisungen des Auftraggebers unterliegt, der als „Herr der Daten“ die alleinige Verfügungsgewalt behält.

Grundlage für die Auftragsverarbeitung bildet ein Vertrag, dessen inhaltliche Mindestanforderungen sich aus Art. 28 Abs. 3 DSGVO ergeben. Entsprechende Vertragsmuster sind im Internet zu finden (siehe [ct.de/wee4](https://www.ct.de/wee4)). Etliche Dienstleister haben aber auch eigene Vertragsvorlagen.

Verfallsdatum

? Dürfen Personenfotos uneingeschränkt aufbewahrt werden oder zwingt mich das neue europäische Datenschutzrecht, sie irgendwann zu löschen?

! Es gilt der Grundsatz der Datenminimierung. Demnach müssen personenbezogene Daten auf den Zweck der Verarbeitung beschränkt sein. Entfällt dieser, zum Beispiel nachdem der Auftrag erfüllt und die Fotos ausgehändigt oder verkauft wurden, sind sie grundsätzlich zu löschen. Mit den Auftraggebern kann jedoch vertraglich vereinbart werden, dass die Bilder zum Zwecke der Nachbestellung für eine bestimmte Zeit aufbewahrt werden dürfen.

Darüber hinaus kann ein berechtigtes Interesse (siehe Seite 164) bestehen, welches die Anfertigung und Speicherung von Fotos erlaubt. So kann sich etwa der professionelle Street-Fotograf zur Ausübung seiner Tätigkeit auf die Kunstfreiheit berufen. Auch bei journalistisch-redaktioneller Nutzung von Fotos gelten im Rahmen des sogenannten Medienprivilegs Ausnahmen von der Löschpflicht.

Unter Juristen wird zum Teil die Ansicht vertreten, dass Personenfotos, entsprechend der urheberrechtlichen Schutzfristen, grundsätzlich bis zu siebenzig Jahre nach dem Tod des Fotografen gespeichert bleiben dürfen. Denn gemäß Art. 17 Abs. 3 DSGVO besteht kein Löschungsanspruch, wenn personenbezogene Daten zur Geltendmachung, Ausübung

oder Verteidigung von Rechtsansprüchen erforderlich sind. Um nachweisen zu können, dass man der Urheber eines bestimmten Fotos ist, muss man zur Beweisführung vor Gericht idealerweise das Original im RAW-Format vorlegen können. Um dies gewährleisten zu können, soll folglich kein Lösungsanspruch seitens der abgebildeten Personen bestehen.

Dem ist allerdings entgegenzuhalten, dass die Berechtigung zur weiteren Speicherung nur besteht, wenn urheberrechtliche Auseinandersetzungen tatsächlich anstehen oder mit hinreichender Wahrscheinlichkeit zu erwarten sind. Die bloß theoretische Möglichkeit einer Auseinandersetzung reicht hingegen nicht aus.

Kein Mensch zu sehen

? Ich habe mich auf Sach- und Architekturfotografie spezialisiert. Kann mir die DSGVO egal sein?

! Auch wenn auf einem Foto keine Menschen abgebildet sind, kann es sich um eine Verarbeitung personenbezogener Daten im Sinne des Datenschutzrechts handeln. Sobald irgendeine Information Rückschlüsse auf eine Person zulässt, sollte man jedes Bild aus der datenschutzrechtlichen Perspektive betrachten. Beispielsweise beim Fotografieren eines Autos: Das Kfz-Kennzeichen gehört gemäß § 45 Straßenverkehrsgesetz (StVG) zu solchen Daten, die einen Bezug zu einer bestimmten oder bestimmbarer Person ermöglichen. Hier genügt allein die Möglichkeit einer Auskunft aus dem zentralen Fahrzeugregister, welche den Halter des Fahrzeugs identifizierbar macht.

Auch beim Fotografieren auf Privatgrundstücken oder in Häusern können personenbezogene Daten anfallen. Soweit Standortdaten als GPS-Koordinaten in den Metadaten gespeichert sind, kann über den zum Standort gehörenden Grundbucheintrag der Eigentümer ermittelt werden und die Fotos sind ihm zuordenbar. Bei sogenannten Property-Release-Verträgen, in denen der Besitzer einer Veröffentlichung



eines von seinem Eigentum erstellten Bildes zustimmt, sollte auch an den Datenschutz gedacht werden. Insbesondere müssen die sich aus Art. 13 DSGVO ergebenden Informationspflichten erfüllt werden.

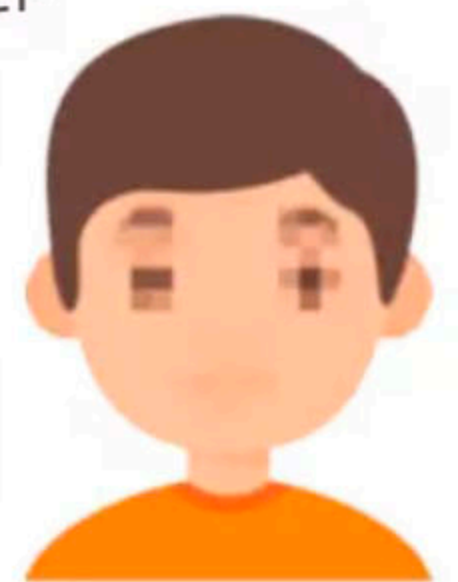
Modelverträge

? Stimmt es, dass eine Einwilligung in die Veröffentlichung von Fotos jederzeit widerrufen werden kann? Dann sind Model-Release-Verträge ja nicht das Papier wert, auf dem sie geschrieben sind!

! Eine datenschutzrechtliche Einwilligungserklärung kann tatsächlich jederzeit frei und ohne Angabe von Gründen widerrufen werden. Für Fotografen ist das ein echtes Problem. Rechtmäßig erstellte Bilder dürften dann nicht mehr genutzt werden. Daher empfiehlt es sich, möglichst nicht auf Einwilligungen zu setzen (siehe Seite 164).

Bei einem Model-Release-Vertrag, der neben den konkreten Verwendungszwecken auch eine Klausel enthalten sollte, die die unwiderrufliche Übertragung von Verwertungsrechten regelt, ist die datenschutzrechtliche Legitimation für die Veröffentlichung der Fotos nach Art. 6 Abs. 1 lit. b) DSGVO der Vertrag an sich. In diesem Fall besteht keine Widerrufsmöglichkeit.

Eine zusätzliche Einwilligung frei nach dem Motto „doppelt hält besser“ sollte tunlichst nicht eingeholt werden. Das Problem: Da ein wirksamer Einwilligungstext auf die Widerrufsmöglichkeit hinweisen muss, würde dies mit dem Model-Release-Vertrag inhaltlich unvereinbar sein. Das führt im Zweifel zu unnötigen Rechtsstreitigkeiten. Dennoch müssen dem Model gegenüber alle notwendigen datenschutzrechtlichen Informationspflichten erfüllt werden. Entsprechende Musterverträge sollten daher um eine Datenschutzerklärung ergänzt werden.



Unkenntlich machen

? Ich möchte ein Foto veröffentlichen. Leider habe ich von einer Person, die dort mit abgebildet ist, keine Einwilligung. Reicht es, das Bild zu verpixeln?

! Fehlt eine erforderliche Einwilligung oder wurde diese vom Betroffenen widerrufen, muss der Fotograf die Bilder, auf denen Personen abgebildet sind, löschen. So sieht es die DSGVO vor. Es genügt in der Regel nicht, das Gesicht der jeweiligen Person zu verpixeln oder ihr den typischen schwarzen Balken zu verpassen. Denn oft beseitigt die Verpixelung eines Gesichts den Personenbezug nicht. Die ver-

meintlich unkenntlich gemachte Person bleibt häufig für Familienangehörige und Bekannte erkennbar. So urteilte das Landgericht Hamburg (Urteil vom 20.10.2006, Az.: 324 O 922/05), dass trotz großflächiger Verpixelung der Gesichtspartie das allgemeine Persönlichkeitsrecht einer in der Bildzeitung abgebildeten Frau verletzt wurde. Aufgrund individueller Merkmale wie Kopfform, Ohren, Frisur, Körperhaltung und Kleidung war die Frau von Bekannten identifiziert worden. Außerdem verraten die Metadaten eines Bildes in der Regel den Aufnahmezeitpunkt oder sogar den Aufnahmeort, was zusätzlich die Möglichkeit einer Identifizierung erleichtert. Mithilfe entsprechender Software gelingt es zudem mittlerweile, aus verpixelten Bildern doch noch eine brauchbare Darstellung zu berechnen.

Mitarbeiterfotos

? Ich möchte Fotos von Mitarbeitern veröffentlichen. Darf ich das ohne Weiteres?

! Laut § 26 BDSG dürfen personenbezogene Daten für betriebliche Zwecke nur verarbeitet werden, wenn dies für die Entscheidung über die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. In den meisten Fällen wird man daher eine Einwilligung der Mitarbeiter benötigen, wenn sie in der Mitarbeiterzeitschrift, auf der Unternehmenswebseite oder in Werbebroschüren abgebildet werden sollen. Nach einer Anpassung des BDSG muss diese Einwilligung allerdings nicht mehr zwingend schriftlich eingeholt werden. Es genügt, wenn der Mitarbeiter seine Zustimmung in elektronische Form, beispielsweise per E-Mail, erteilt. Einen Mustertext für eine Einwilligung finden Sie im Kasten auf Seite 171.

Achtung: Nicht zu empfehlen ist es, eine derartige Einwilligung direkt im Arbeitsvertrag unterzubringen. Eine solche Klausel dürfte aufgrund unangemessener Benachteiligung unwirksam sein, zudem fehlt es an der erforderlichen Freiwilligkeit der Einwilligung, da sie unter Zwang zustande kommt – ohne Einwilligung kein Job.

Wer als Fotomodell arbeitet, muss selbstverständlich akzeptieren, dass Fotos der eigenen Person erstellt und verwendet werden. Auch der Pressesprecher eines Unternehmens darf davon ausgehen, dass Fotos von ihm gemacht werden, wenn er eine Pressekonferenz hält. Das gehört schließlich zu seinem Job. Besonders achtsam muss man bei jüngeren

Arbeitnehmern sein. Soll der aktuelle Azubi-Jahrgang auf der Facebook-Fanpage des Unternehmens präsentiert werden, benötigt man bei allen unter 16 Jahren das Einverständnis beider Eltern.

Problematisch ist auch die Rechtslage bei Firmenfeiern, denn hier stößt das Instrument der Einwilligung an seine Grenzen. Nicht getan ist es mit dem Hinweis in der Einladungskarte: „Wenn Sie an der Firmenfeier teilnehmen, erklären Sie sich mit dem Anfertigen und Veröffentlichen von Fotos einverstanden.“ Soweit im Vorfeld umfassend die datenschutzrechtlichen Informationspflichten erfüllt werden, auf das Widerspruchsrecht hingewiesen wird und strenge Maßstäbe bei der Veröffentlichung von Fotos angelegt werden, kann sich das Unternehmen jedoch auf die Rechtsgrundlage der berechtigten Interessen berufen.

Mögliche Sanktionen

? Welche Konsequenzen drohen, wenn ich als Fotograf gegen datenschutzrechtliche Vorschriften verstoße?

! Jede Person hat das Recht, sich bei einer Datenschutzaufsichtsbehörde über den Fotografen zu beschweren, wenn sie das Gefühl hat, dass beim Anfertigen, Speichern oder Nutzen eines Fotos gegen Vorschriften der DSGVO verstoßen wurde. Kommt die Behörde zu dem Ergebnis, dass die Datenverarbeitung illegal war, dann drohen Bußgelder, die gemäß Artikel 83 DSGVO „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein sollen. Wie hoch eine mögliche Geldstrafe dann ausfällt, hängt unter anderem von der Art und Schwere des Verstoßes ab und ob man „Wiederholungstäter“ ist. Bevor ein Bußgeld verhängt wird, kann die Behörde auch zunächst eine Verwarnung aussprechen.

Eine fotografierte Person kann aber auch direkt den Fotografen, dessen Dienstleister oder Auftraggeber auf Schadensersatz verklagen. Insbesondere wenn ein immaterieller Schaden entstanden ist, etwa weil durch die Veröffentlichung eines kompromittierenden Fotos der Ruf einer Person geschädigt wurde, kann der Betroffene eine Art „Schmerzensgeld“ zur Wiedergutmachung verlangen. Dabei haften alle an der Datenverarbeitung Beteiligten gesamtschuldnerisch, man kann sich also den solventesten Verantwortlichen herauspicken und gegen diesen vorgehen.

Unter Umständen kann man sich sogar strafbar machen. Wer Fotos einer Person ohne deren Einwil-

ligung über eine Bilddatenbank vermarktet, verstößt gegen § 42 BDSG. Demnach wird mit einer Freiheitsstrafe von bis zu drei Jahren oder einer Geldstrafe unter anderem bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Anzahl von Personen ohne Berechtigung zugänglich macht und hierbei gewerblich handelt.

Man sollte auch nicht vergessen, dass das Datenschutzrecht nur ein Teil des gesamten Fotorechts darstellt. Es sind im Zusammenhang mit Bildrechtverletzungen noch eine Vielzahl weiterer zivilrechtlicher oder auch strafrechtlicher Konsequenzen denkbar, wie etwa Unterlassungs- und Schadensersatzansprüche des Betroffenen und sogar Haftstrafen durch die Herstellung von Bildern, die höchstpersönliche Lebensbereiche verletzen.

Biometrische Daten

? Wann gelten Gesichtsfotos als biometrische Daten?

! Bei einem Gesichtsbild kann es sich unter Umständen auch um ein biometrisches Datum nach Art. 4 Nr. 1 DSGVO handeln. Wird ein solches Bild mit einem speziellen technischen Verfahren gewonnen, welches die Verarbeitung biometrischer Charakteris-

tika des Gesichts ermöglicht, mit dem Ergebnis, dass sich das Gesichtsbild dann im Rahmen eines automatisierten Verfahrens einer Person eindeutig zuordnen lässt,

ist es als biometrisches Datum anzusehen. Hierunter fallen etwa die Bilder im Personalausweis, da sich diese für einen automatisierten Abgleich mit der Person eignen. Auch das Entsperren eines iPhones mittels Face ID beruht auf biometrischen Gesichtsdaten.

Die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ist gemäß Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Der zentrale Erlaubnistatbestand für die Nutzung derartiger Fotos und Verfahren ist für Unternehmen daher die Einwilligung des Betroffenen. Sollen biometrische Verfahren zum Beispiel für die Zugangskontrolle eingesetzt werden, sollte das jeweilige Unternehmen zunächst sorgfältig die datenschutzrechtlichen Voraussetzungen klären. Im Regelfall wird es erforderlich sein, eine Datenschutz-Folgenabschätzung (siehe Seite 128) durchzuführen.

Hilfreich zu diesem Thema ist das „Positionspapier zur biometrischen Analyse“ der Datenschutzaufsichtsbehörden, welches einige Fallbeispiele enthält.



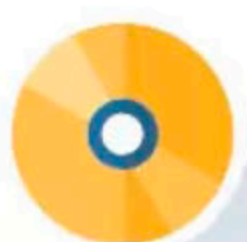
Einwilligungserklärung zur Veröffentlichung von Fotos

Die Firma [...] beabsichtigt, zur Darstellung des Unternehmens im Rahmen der Öffentlichkeitsarbeit und zur Vermarktung der von ihr angebotenen Produkte und Dienstleistungen, Fotos von Mitarbeitern im Internet und auf gedruckten Werbematerialien zu veröffentlichen.

Ich willige ein, dass von meiner Person zu diesen Zwecken digitale Fotoaufnahmen (Bildnisse) angefertigt, gespeichert und ohne räumliche und zeitliche Beschränkung zur Veröffentlichung insbesondere

- im Internet, insbesondere auf den von der Firma [...] betriebenen Onlinepräsenzen und Social-Media-Kanälen (z.B. Facebook, Twitter, Instagram);
 - in gedruckten und digitalen Werbematerialien für eigene Waren und Dienstleistungen;
 - in Stellenanzeigen und PR-Materialien des Unternehmens;
 - sowie im Intranet
- veröffentlicht werden dürfen.

Soweit sich aus den Bildnissen Hinweise auf meine ethnische Herkunft, Religion oder Gesundheit (z.B. Hautfarbe, Kopfbedeckung, Brille), bezieht sich meine Einwilligung auch auf diese Angaben...



**Positionspapier
zur biometrischen
Analyse und
Vertragsmuster
Auftragsver-
arbeitung:**

[ct.de/wee4](https://www.ct.de/wee4)



Kinder fotografieren

? Dürfen Kinder ohne Weiteres fotografiert werden?

! Soweit ein unter 16-jähriges Kind fotografiert werden soll, benötigt man grundsätzlich die vorherige Zustimmung beider Elternteile. Die nachträgliche Genehmigung ist nicht ausreichend. Erscheint bei einem Kinder-Fotoshooting nur ein Sorgeberechtigter, sollte sich der Fotograf schriftlich bestätigen lassen, dass der erschienene Elternteil entweder mit Zustimmung des Partners handelt oder allein sorgeberechtigt ist. Personenbezogene Daten von Kindern werden durch die DSGVO in besonderer Weise geschützt. Erst ab einer Altersgrenze von 16 Jahren dürfen Minderjährige selbst in die Verarbeitung Ihrer Daten einwilligen.

Fotografierverbot an Schulen

? Dürfen Schulen das Fotografieren bei Einschulungsfeiern oder anderen Schulveranstaltungen verbieten?

! Immer wieder werden bei Einschulungsfeiern Fotografierverbote verhängt und dies mit Datenschutzbedenken begründet. Dies führt regelmäßig zur Verärgerung von Eltern und Verwandten, die nur ein paar Erinnerungsfotos schießen wollten. Ein generelles Foto- und Filmverbot bei Schulveranstaltungen lässt sich mit der DSGVO nicht begründen. Denn grundsätzlich darf zu privaten und persönlichen Zwecken fast überall fotografiert werden. Erst bei der Veröffentlichung sind Grenzen zu beachten. Trotzdem können Schulen das Anfertigen von Aufnahmen verbieten. Dies hat jedoch nichts mit Datenschutz zu tun, sondern es wird lediglich vom Hausrecht

Gebrauch gemacht. Wenn Schulleiter der DSGVO die Schuld in die Schuhe schieben, ist dies irreführend und rechtlich falsch.

Will eine Schule selbst Fotos von Veranstaltungen veröffentlichen, muss in der Regel eine Einwilligung der Betroffenen eingeholt werden.

Mannschaftsfotos

? Muss ein Verein für die Veröffentlichung von Mannschaftsfotos die Einwilligung der Mitglieder einholen?

! Vereine dürfen Mannschaftsfotos auch ohne vorherige Einwilligung der Mitglieder veröffentlichen, da ein berechtigtes Interesse besteht, über das Vereinsgeschehen zu informieren. Die Rechtsgrundlage ergibt sich aus Art. 6 Abs. 1 lit. f) DSGVO. Wichtig ist allerdings, dass die Mitglieder über mögliche Fotoveröffentlichungen unterrichtet werden, etwa über ein Informationsblatt für Neumitglieder oder in der Vereinszeitung. Hierbei ist auch ausdrücklich auf das Widerspruchsrecht hinzuweisen. Anders ist die Situation bei Mannschaftsfotos von Minderjährigen, hier ist stets die Einwilligung der Erziehungsberechtigten erforderlich.

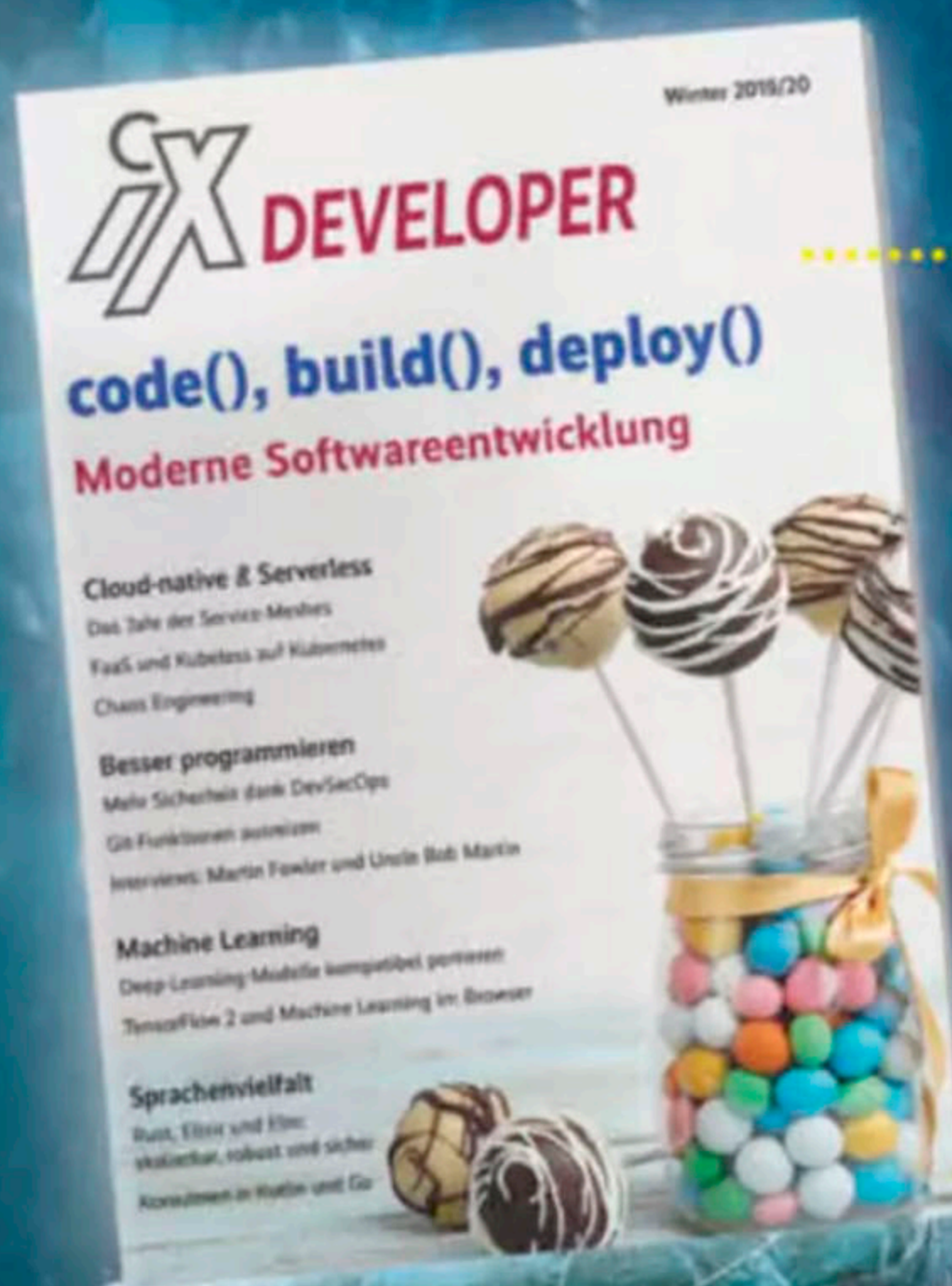
Zeitliche Reichweite

? Wie lange gilt die Einwilligung der Eltern in die Veröffentlichung von Fotos ihrer Kinder?

! Eltern können grundsätzlich in die Veröffentlichung von Fotos ihrer Kinder einwilligen. Doch diese Einwilligung, die ohnehin jederzeit widerrufen werden kann, ist nicht von unbestimmter Dauer. Denn Kinder werden älter und können irgendwann selbst eine Entscheidung hinsichtlich der Veröffentlichung von Fotos treffen. Diese Entscheidungsmöglichkeit muss auch Personen zugebilligt werden, die als minderjährige Kinder mit Zustimmung der gesetzlichen Vertreter abgebildet wurden, aber nun die Volljährigkeit erreicht haben. Einen entsprechenden Fall hatte das Landgericht Frankfurt zu entscheiden (LG Frankfurt, Urteil vom 29.08.2019, Az.2-03-O 454/18). Die Tochter eines Politikers wehrte sich gegen die erneute Veröffentlichung eines Fotos, welches vor 19 Jahren im Rahmen einer Homestory abgedruckt wurde. Das Gericht urteilte, dass die damals vom Vater erteilte Einwilligung unerheblich ist. (keh)

Mit allen Wassern gewaschen:

Auch digital erhältlich



iX Developer Moderne Softwareentwicklung

Verschaffen Sie sich Orientierung im Dschungel der Softwareentwicklung: Machine und Deep Learning, mehr Sicherheit dank DevSecOps, Git-Funktionen ausreizen, Chaos Engineering, Rust, Elixir und Elm - dieses Sonderheft bietet mit einem breiten Themenmix und umfangreichen Praxisartikeln Überblick und vielfältige Anregungen.

Auch komplett digital erhältlich

shop.heise.de/ix-software20

12,90 € >

iX Kompakt Container 2020

Das neue Sonderheft liefert fundiertes Basiswissen unter anderem zu diversen *aaS-Architekturen, Containern und Mikrovirtualisierung. Außerdem jede Menge Tipps und Entscheidungshilfen, um aus der Vielzahl von Tools und Anbietern die passende Container-Software für sich zu finden.

Auch komplett digital erhältlich!

[shop-heise.de/ix-container20](https://shop.heise.de/ix-container20)

14,90 € >



iX Developer Moderne Softwarearchitektur

Fortwährend werden neben den traditionellen immer mehr neue Anforderungen an Softwarearchitekten gestellt. In diesem iX-Sonderheft war es das Ziel der Redaktion, eine breite Themenmischung über neue Technologien und Trends abzubilden wie Domain-driven Design, Cloud-native, Shift Left u.v.m. Profitieren Sie von den Erfahrungen und Ratschlägen der Experten!

Auch komplett digital erhältlich!

shop.heise.de/ix-dev-msa20

14,90 € >

NEU

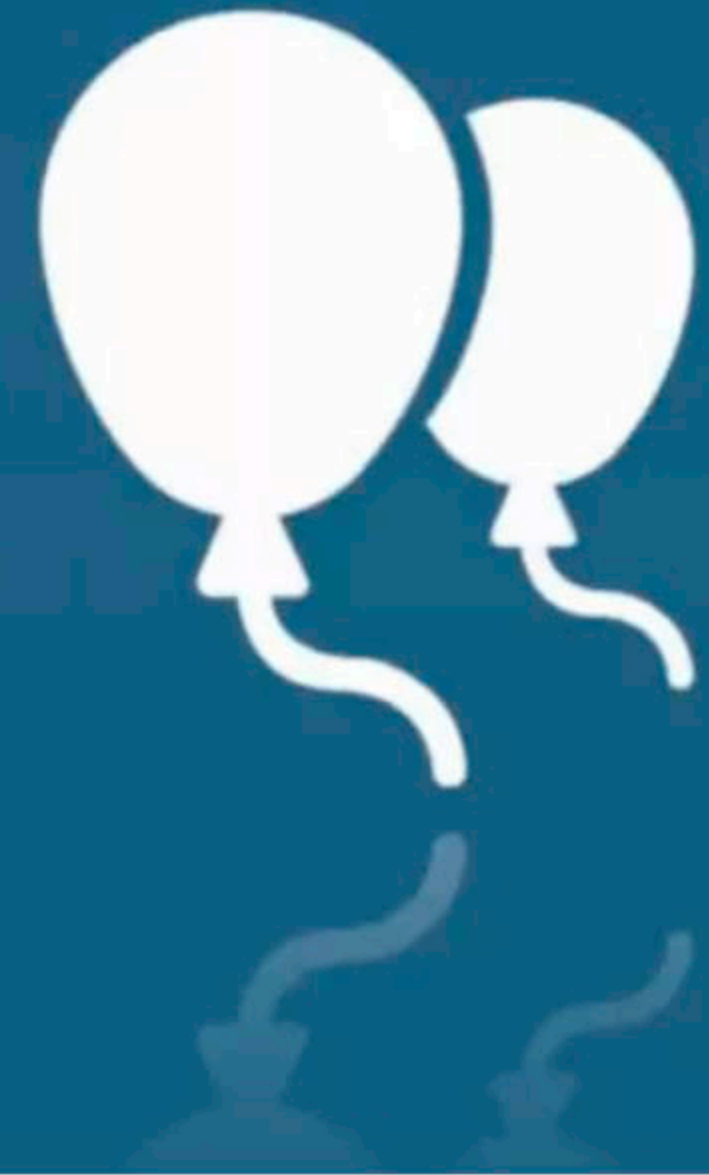
Weitere Sonderhefte zu vielen spannenden Themen finden Sie hier: shop.heise.de/specials-aktuell

> Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

 **heise shop**

shop.heise.de/specials-aktuell >

Event-Fotografie



Rechtsunsicherheit besteht insbesondere dann, wenn von den abgebildeten Personen keine Einwilligung eingeholt werden kann, wie bei großen Menschenansammlungen im Rahmen öffentlicher Events. Doch selbst für diese Fälle gibt es Lösungen.

Von Nicolas Maekeler

Ein datenschutzrechtlich besonders unsicheres Terrain ist das Fotografieren auf Sportevents, Konzerten, Kongressen und sonstigen Veranstaltungen. Immer dann, wenn der Fotograf eine Person nicht auf Grundlage eines Model-Release-Vertrages oder einer sonstigen Beauftragung, die als Rechtsgrundlage für die Datenverarbeitung dient, ablichtet, wird es kompliziert.

Geschlossene Gesellschaft

Der einfache Fall sind kleine, nicht öffentliche Veranstaltungen, zu denen Teilnehmer namentlich eingeladen sind oder die einen Ticketerwerb erfordern. Bei Tagungen, Konferenzen oder dergleichen hat man es in der Regel mit einem überschaubaren Teilnehmerkreis zu tun. Hier wäre es prinzipiell möglich, eine Einwilligung zur Fotonutzung von den Besuchern einzuholen.

Öffentliche Veranstaltungen

Grundsätzlich ist jeder Fotograf dazu verpflichtet, sämtlichen fotografierten Personen eine Datenschutzerklärung zukommen zu lassen. Bei einer unüberschaubaren Anzahl von Menschen ist das allerdings schwer durchführbar.

Hier kann sich der Fotograf auf ein berechtigtes Interesse (siehe Seite 164) berufen. Schließlich sind die abgebildeten Menschen nur in ihrer Sozialsphäre betroffen. Sie haben sich freiwillig zu einer öffentlichen Veranstaltung, wie zum Beispiel Sportveranstaltungen, Demonstrationen oder Konzerten, begeben. Sie müssen damit rechnen, dass dort fotografiert wird und diese Bilder ihren Weg ins Internet oder in weitere Medien finden. Etwas an-

deres gilt nur dann, wenn Personen besonders unvorteilhaft abgebildet werden, etwa weil sie sichtbar betrunken sind. In solchen Fällen muss der Fotograf im Rahmen einer Interessenabwägung zurückstecken.

Presse- und Öffentlichkeitsarbeit

Es ist durchaus legitim, wenn der Fotograf beziehungsweise der Veranstalter sich darauf beruft, Aufnahmen von Besuchern im Rahmen der Presse- und Öffentlichkeitsarbeit zu nutzen, um etwa den Bekanntheitsgrad der Veranstaltung zu erhöhen.

Hierfür genügt es, die Teilnehmer darauf hinzuweisen, dass Fotos erstellt und wie diese verwendet werden. Idealerweise geschieht das bereits, wenn sie das Ticket kaufen oder sich anmelden. Am Tag der Veranstaltung sind zusätzlich entsprechende Hinweisschilder sichtbar auszuhängen (siehe Beispiel auf Seite 175). Wichtig ist es, die Art der Datenverarbeitung korrekt darzustellen. Um die restlichen Informationspflichten zu erfüllen, genügt es, auf die allgemeine Datenschutzerklärung zu verweisen.

Die Teilnahme an der Veranstaltung darf dabei von der Einwilligung zur Fotonutzung nicht abhängig gemacht werden – dies würde dem Kriterium der Freiwilligkeit nicht entsprechen. Das Stichwort lautet hier „Kopplungsverbot“.

Massen-Events

Auch beim Fotografieren auf Groß-Veranstaltungen, zum Beispiel bei einer Demonstration, wird eine Rechtsgrundlage aus der DSGVO benötigt. Das große Problem bei einer unüberschaubaren Anzahl von

Menschen ist die Informationspflicht. Um dieser nachzukommen, müsste der Fotograf zusätzliche personenbezogene Daten von fotografierten Personen erheben. Er hat allerdings weder das Interesse noch die Möglichkeit, die abgebildeten Personen zu identifizieren, was auch dem Grundsatz der Datenminimierung widersprechen würde. Der Fotograf braucht daher nicht zu informieren. Zudem regelt

Art. 14 Abs. 5 lit. b DSGVO, dass keine Informationspflicht besteht, wenn es unmöglich ist, die Informationen zu erteilen oder wenn dies einen unverhältnismäßigen Aufwand erfordert. So schätzt es auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein, der in einem Vermerk ausführlich die gesamte Problematik rechtlich würdigt (siehe [ct.de/wm1m](https://www.ct.de/wm1m)). (keh) **ct**

Datenschutzinformationen

Während der heutigen Veranstaltung werden Fotos gemacht. Wenn Sie nicht abgebildet werden möchten, lassen Sie es den jeweiligen Fotografen bitte wissen. Wir können allerdings nicht verhindern, dass Sie auf Aufnahmen größerer Menschenansammlungen abgebildet werden.

Verantwortliche Stelle:

[Name und Kontaktdaten des Verantwortlichen]

Zweck der Verarbeitung, Rechtsgrundlage und Speicherdauer:

Die Aufnahmen werden im Rahmen unserer Presse- und Öffentlichkeitsarbeit zur Darstellung und Dokumentation unserer Aktivitäten auf unserer Website und unseren Social-Media-Kanälen (Facebook, Twitter, Instagram etc.) veröffentlicht. Hierin liegt auch unser berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO. Nicht veröffentlichte Fotos werden zwei Jahre lang elektronisch gespeichert und danach gelöscht.

Empfänger:

Die Aufnahmen geben wir im Rahmen unserer Pressearbeit ggf. auch an Medienvertreter/innen weiter. Auf Wunsch stellen wir das Bildmaterial auch Personen und Organisationen zur Verfügung, die an unserer Veranstaltung beteiligt sind.

Widerspruchsrecht:

Sie haben das Recht, gegen die genannte Verarbeitung Widerspruch zu erheben. Nutzen Sie hierfür bitte die oben genannten Kontaktdaten. Soweit die rechtlichen Voraussetzungen vorliegen, werden wir zukünftig durch geeignete Maßnahmen die weitere Verarbeitung der entsprechenden Aufnahmen unterlassen. Löschungen auf Websites oder in Social-Media-Kanälen erfolgen im Rahmen der technischen Möglichkeiten.

Weitere Informationen zum Thema Datenschutz, insbesondere über Ihre Rechte als betroffene Person, erhalten Sie in unserer Datenschutzerklärung, die an der Kasse eingesehen oder im Internet unter [Link zur Datenschutzerklärung] abgerufen werden kann.



Infopflicht bei
Massen-Events:

[ct.de/wm1m](https://www.ct.de/wm1m)

Die DVD zum Heft

Die folgenden Vorträge, Webinare, Podcasts, Musterformulare und weitere Zusatzinformationen finden Sie auf der beiliegenden DVD oder online unter ct.de/wnzzr.

Vorträge und Webinar

Webinar „Privacy Shield gestoppt“

Das iX-Webinar beschäftigt sich mit den Auswirkungen des Wegfalls des Privacy Shield insbesondere auf die IT. Was ist passiert und was müssen Unternehmen tun, um rechtlichen Ärger zu vermeiden?

Referenten: Joerg Heidrich / Dr. Oliver Diedrich

„Datenschutz im Homeoffice“

Vortrag über die Anforderungen der DSGVO an die technischen und organisatorischen Maßnahmen sowie sonstige rechtliche Anforderungen im Homeoffice.

Referenten: Dr. Michael Koch / Joerg Heidrich

„Anatomie eines Datenschutz-GAU“

Vortrag von der Heise Security Konferenz 2020 über die technischen Anforderungen der DSGVO und den Umgang mit Datenpannen. Diese Vorgaben werden anhand eines praktischen Beispiels dargestellt. Was ist bei Data Breaches zu tun, welche Risiken drohen?

Referent: Joerg Heidrich

Podcast

Auslegungssache: c't-Datenschutz-Podcast

- Ausblick auf die kommende Gesetzgebung
- Big Brother Arbeitgeber



- Blick über den Tellerrand nach Österreich
- Chimäre Einwilligung
- Cloud oder nicht Cloud?
- Datenpannen: Irgendwann erwischt es jeden
- Datenschutzfolgenabschätzung bei der Corona-App
- Der betriebliche Datenschutzbeauftragte
- Gespräch mit dem Bundesdatenschutzbeauftragten
- Gespräch mit der Datenschutzbeauftragten Niedersachsen
- Videoüberwachung
- Next Stop Privacy Harbour?
- Zeitbombe Schadensersatz II

Formulare und Muster

Beispieldateien aus der c't-Redaktion

- Beispiel: Ähnlichkeitswerbung
- Beispiel: Folterfragebogen
- Beispiel: Newsletter
- Checkliste: Cookie-Banner & Content-Tools
- Muster: Datenschutzinformation
- Muster: Einwilligungserklärung
- Muster: Verarbeitungsverzeichnis - Betrieb einer Webseite
- Muster: Verarbeitungsverzeichnis - Verantwortlicher Mitarbeiter

Kurzpapiere der Datenschutzkonferenz

Die Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) geben eine Orientierung, wie die DSGVO im praktischen Vollzug angewendet werden sollte.

1. Verzeichnis von Verarbeitungstätigkeiten
2. Aufsichtsbefugnisse/Sanktionen
3. Verarbeitung personenbezogener Daten für Werbung
4. *Das Kurzpapier zur Datenübermittlung in Drittländer war zum Redaktionsschluss noch nicht aktualisiert.*
5. Datenschutz-Folgenabschätzung
6. Auskunftsrecht der betroffenen Person
7. Marktortprinzip – Regelungen für außereuropäische Unternehmen
8. Maßnahmenplan DSGVO für Unternehmen
9. Zertifizierung

10. Informationspflichten bei Dritt- und Direkterhebung
11. Recht auf Löschung / „Recht auf Vergessenwerden“
12. Datenschutzbeauftragte
13. Auftragsverarbeitung
14. Beschäftigtendatenschutz
15. Videoüberwachung
16. Gemeinsam für die Verarbeitung Verantwortliche
17. Besondere Kategorien personenbezogener Daten
18. Risiko für die Rechte und Freiheiten natürlicher Personen
19. Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen
20. Einwilligung nach der DSGVO

Weitere Informationen der Datenschutzkonferenz

- Konzept der DSK zur Bußgeldzumessung in Verfahren gegen Unternehmen
- Orientierungshilfe Videokonferenzsysteme

Online-Zugriff auf
die DVD-Inhalte

[ct.de/wnzt](https://www.ct.de/wnzt)

RABATTAKTION

heise Security Prevent – IT-Risiken im Griff

Der technische Datenschutz spielt in jedem Unternehmen eine immer wichtigere Rolle. Dieses halbtägige Webinar gibt einen Überblick zu aktuellen Sicherheitsrisiken und erklärt, wie Sie Ihr Unternehmen effizient und datenschutzkonform schützen. Die Referenten kommen alle aus dem direkten Umfeld der heise-Security-Redaktion:

- Jürgen Schmidt, Leiter von heise Security, analysiert aktuelle Gefahren und wie man sich davor schützt.
- Joerg Heidrich, Justitiar des Heise-Verlags, informiert, wie Sie Ihr Unternehmen für die ständig steigenden Anforderungen an den Datenschutz fit machen.
- Der freiberufliche Security-Berater Dr. Christoph Wegener gibt praktische Handreichungen für die Vorbereitung auf IT-Security-Vorfälle.
- In das abschließende Fachgespräch Cybercrime bringt zusätzlich Frank Puschin seine Erfahrung aus der Zentralen Ansprechstelle Cybercrime des LKA Niedersachsen ein.

Die Aufzeichnung des Online-Webinars „heise Security Prevent: IT-Risiken im Griff“ erhalten Leser von c't DSGVO 2021 mit 50 Euro Rabatt zum Vorzugspreis von 199 Euro. Hierzu geben Sie bei der Bestellung unter shop.heise.de/DSGVO-Prevent diesen Code **DSGVO21-PREVENT** ein. Der Code ist gültig bis zum 31.12.2021.

c't Windows –

Das Praxishandbuch 2020

NEU

Auch als
Heft + PDF
erhältlich mit
29 % Rabatt



c't WINDOWS Das Praxishandbuch 2020

Effizienter nutzen

Neue Funktionen entdecken
Windows im Homeoffice
Dateien schneller finden
Tipps zum Startmenü

Schlauer einrichten

Microsoft-Konto vermeiden
Maßgeschneidert installieren
Gratis umsteigen auf Windows 10
So finden Sie die richtige Lizenz

Tiefer einsteigen

Windows-Rechte verstehen
Registry-Änderungen nachvollziehen
Windows virtualisieren wie die Profis

Windows absichern

Trojanersicheres Backup · Privacy-Checkliste
SSDs, Festplatten und USB-Sticks verschlüsseln
Passwörter sicher und trotzdem bequem verwahren



c't Windows 2020

Das Praxishandbuch 2020 der c't-Experten gibt Ihnen einen perfekten Rundumblick über Ihr Windows-System. Auf über 200 Seiten gibt es Tipps darüber wie Sie eine ganze Reihe kaum bekannter, praktischer Funktionen für sich nutzen können. Aber auch zahlreiche Infos, die im Homeoffice hilfreich sind, oder wie Sie Ihr System besser schützen können und vieles mehr.

shop.heise.de/ct-windows20

Einzelheft
für nur

14,90 € >

 **heise shop**

shop.heise.de/ct-windows20 >

> Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

ONLINE-WORKSHOPS

3. MÄRZ 2021

- // **Schneller als der eigene Schatten –
Entwicklung einer schnellen Reaktionsfähigkeit im Notfall**
Lukas Reike-Kunze
- // **Stolpersteine in der Wolke –
Sicherer Einsatz von Microsoft Office 365**
Kevin Kirchner
- // **„Ist das sicher oder in JavaScript?“ – Webanwendungen in den Augen eines Angreifers**
Christian Biehler

4. MÄRZ 2021

- // **Active Directory in Gefahr. Was Fehlkonfigurationen bewirken und wie man
Angriffe entdeckt und verhindert**
Frank Ullly
- // **Ohne Bullshit-Bingo: Windows-Sicherheit mit Bordmitteln**
Christian Biehler
- // **Panik und Schockstarre vermeiden: Richtig reagieren bei IT-Sicherheitsvorfällen**
Marco Lorenz