Ausgabe 02/2018

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz

BvD-Herbstkonferenz
zum Datenschutz
24. - 26.10.2018
im STEIGENBERGER HOTEL
STUTTGART

Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

DS-GVO: 2018 – ein heißes Jahr in Sachen Datenschutz

DIE UMSETZUNG DER DS-GVO IN DEUTSCHLAND – ab S. 9

DIE ISO 27018 IM LICHTE DER DS-GVO – ab S. 32

DER SPUR DER DATEN FOLGEN – ab S. 64

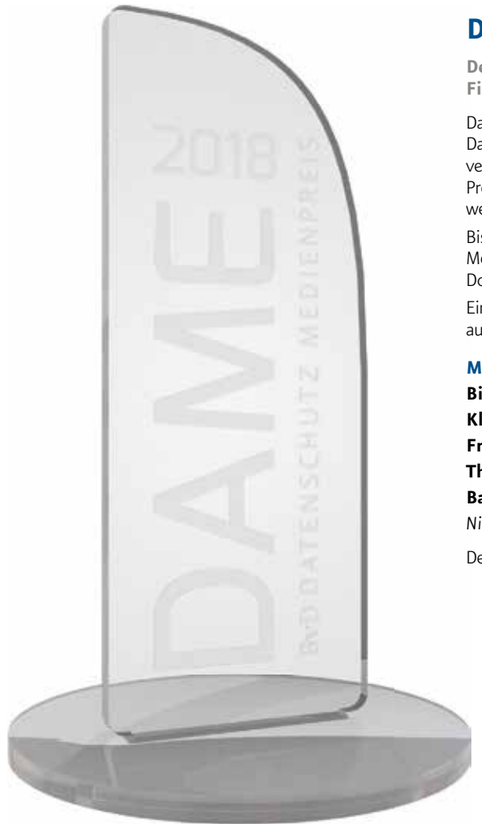
DATENSCHUTZSCHULUNG – AUF DIE INNOVATIVE ART – ab S. 72

BvD e.V.
DATENSCHUTZ GESTALTEN

Anzeige

DATENSCHUTZ MEDIENPREIS (DAME)

des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.



DATENSCHUTZ MEDIENPREIS (DAME) DES BVD

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. lobt einen Filmpreis für Datenschutz aus.

Damit alle in der komplexen digitalen Welt gleiche Chancen auf den Schutz persönlicher Daten haben, muss Datenschutz verständlich erklärt werden. Die Gesetze müssen bei den Bürgern ankommen, Regelungen verständlich und transparent sein. Deshalb lobt der BvD einen Datenschutz Medienpreis aus. Ziel des Preises ist es, das öffentliche Interesse für das Thema Datenschutz rund um zu fördern. Ausgezeichnet werden Beiträge, die Datenschutz verständlich darstellen und zugleich anschaulich erklären.

Bis zum 01. November können sich Filmschaffende, Produktionen, Video-Filmer, Jugendorganisationen, Medienschaffende, Kreative, Verbände und Initiativen mit langen oder kurzen Filmen, mit Spiel- oder Dokumentarfilmen, mit Video-Clips und Animations-Beiträgen um den Preis bewerben.

Eine Jury aus Datenschutzexperten, Medienvertretern und Filmschaffenden wird die eingesandten Beiträge auf fachliche Darstellung, Verständlichkeit, zielgruppengerechte Ansprache und Originalität bewerten.

Mitglieder der Jury sind:

Birgit Kimmel, *Päd. Leitung klicksafe.de*, Landeszentrale für Medien und Kommunikation (LMK)
Klaus Müller, *Vorstand des Verbraucherzentrale Bundesverbands (vzbv)*
Frederick Richter, *Vorstand Stiftung Datenschutz*
Thomas Spaeing, *Vorstandsvorsitzender des BvD*
Barbara Thiel, *Vorsitzende der Datenschutzkonferenz (DSK), Landesbeauftragte für den Datenschutz Niedersachsen*

Der Preis ist mit 3.000 Euro dotiert und wird im Rahmen der BvD-Verbandstage 2019 in Berlin übergeben.

Jetzt einreichen!
Einsendeschluss
1. November 2018

INITIATOREN

BvD e.V. DATENSCHUTZ GESTALTEN

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fördert und vertritt die beruflichen Interessen der Datenschutzbeauftragten in Behörden und Betrieben und setzt sich aktiv für einen rechtskonformen Datenschutz ein.

www.bvdnet.de

Datenschutz geht zur Schule BvD e.V. DATENSCHUTZ GESTALTEN

Die Initiative „Datenschutz geht zur Schule“ des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. sensibilisiert Schülerinnen und Schüler bundesweit von den 4. Klassen bis zur Berufsschule für den sicheren und bewussten Umgang mit dem Internet und den sozialen Medien.

www.dsgzs.de

KOOPERATIONSPARTNER

klicksafe.de

klicksafe.de - Die EU-Initiative für mehr Sicherheit im Netz.

In Deutschland ist die Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz gemeinsam mit der Landesanstalt für Medien (LfM) Nordrhein-Westfalen mit der Umsetzung beauftragt.

www.klicksafe.de

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Straße 31, 10787 Berlin, Telefon: +49 (0) 30 26 36 77 62, Telefax: +49 (0) 30 26 36 77 63
E-Mail: datenschutzmedienpreis@bvdnet.de, Website: www.bvdnet.de

ZWEI SCHRITTE VOR – EINEN ZURÜCK?

Die Verhandlungen zum DS-AnpUG 2 laufen, aber in welche Richtung?

Liebe Leserinnen und Leser,

Seit dem 25. Mai 2018 ist die DS-GVO wirksam. Zwei Jahre waren zuvor Zeit, um sich mit der Thematik zu befassen. Trotzdem will das Klagen über die Unzumutbarkeiten nicht abreißen. Genüsslich ausgeweidet von Teilen der Presse und den Aposteln der Datenfreiheit – nun im Gewand der Entbürokratisierer.

Die Datenschutzgrundverordnung enthält zweifelsohne einige praxisfremd und teils auch weltfremd anmutende Regelungen, die aber im Kontext gesehen durchaus zu verstehen sind. Nun haben wir es leider mit einer Vielzahl von mehr oder weniger selbsternannten Experten zu tun, die sich berufen fühlen das neue Datenschutzrecht auszulegen. Dabei kommt Spannendes und teilweise auch Erschreckendes zum Vorschein.

„Visitenkarten künftig nicht mehr zulässig“

Über dergleichen haben wir alle schon herzhaft gelacht, auch über die einstündige Belehrung des Anrufers zu den Informationspflichten. Und auch die leidige Diskussion zum Medienbruch gehört dazu – anstatt zu schauen, was für Verantwortliche und Betroffene am besten funktioniert – denn genau das will die DS-GVO - wird munter theoretisiert und mit Anforderungen überladen. Das hilft nicht, dass ist sogar der größte *Bärendienst*, den man dem Datenschutz und der DS-GVO derzeit erweisen kann. Keinesfalls soll Datenschutz kompliziert und unverständlich sein – man gewinnt aber derzeit den Eindruck, dass dies gezielt so dargestellt wird, damit man Munition sammelt, für die Demontage des Datenschutzes bei den nächsten Gesetzesvorhaben – und damit sind wir beim DS-AnpUG 2.

Seit Monaten lesen wir: „Datenschutzexperten händeringend gesucht – Unternehmen suchen dringend Unterstützung bei der Umsetzung der Anforderungen“ (siehe BITKOM-Studie). Selbstredend sucht man nicht den frisch geschulten Experten mit der 3-Tage Ausbildung, sondern die qualifizierten und erfahrenen Experten, die es im Augenblick nicht in ausreichender Zahl gibt. Bemerkenswert ist dabei, dass sogar von anderen EU-Staaten in Deutschland nach diesen Experten gesucht wird, denn in den anderen Staaten gibt es diese Experten noch viel weniger.

Datenschutzbeauftragte seit 1977 im BDSG verankert

In Deutschland hat der Gesetzgeber früh erkannt, dass es einen Experten in den Unternehmen braucht, der hilft, Gesetz und betriebliche Praxis zusammenzubringen. Mehr denn je ist dies heute der Fall. Der Unfug, der mit Halbwissen verbreitet wird, bereitet den Unternehmern schlaflose Nächte. Die Datenschutzbeauftragten sind es, die in der betrieblichen Praxis aufzeigen, wie die lebensnotwendigen Prozesse auch weiterhin funktionieren und auch, wie Visitenkarten eine Zukunft haben. Dieses Know-how hilft den Unternehmen pragmatisch vor Ort mit den Anforderungen umzugehen und weiter gute und vielleicht sogar bessere Geschäfte zu machen. Weltweit gesehen wird der EU-Datenschutz ja gerade ein Exportschlager. Leider treffen wir in der Praxis noch immer auf Vorstellungen aus der digitalen Frühzeit: *„Wenn bei uns weniger als zehn Personen personenbezogene Daten verarbeiten, dann bin ich doch beim Datenschutz raus!“* Diese Ansicht ist noch immer weit verbreitet und natürlich ist sie falsch. Tatsächlich sagt auch die Anzahl der Personen nicht ganz viel über das Risiko der Verarbeitung aus. Hier hilft der betriebliche Datenschutzbeauftragte. Diese Berufsgruppe leistet gerade Überragendes, um die Bürokratie in den Unternehmen im Rahmen zu halten. Machen wir ihnen diese Arbeit bitte leichter und helfen damit auch den Unternehmen.

Wie das geht? Mit klaren Standards beispielsweise zur Qualifikation und der Ausübung der Tätigkeit als Datenschutzbeauftragter, mit schnellen konkreten Auslegungen und Hilfestellungen, wie denen der Aufsichtsbehörden oder der Stiftung Datenschutz und natürlich des BvD.

Ich wünsche Ihnen eine anregende Lektüre.

T. Spaeing

Thomas Spaeing
BvD-Vorstandsvorsitzender

IMPRESSUM:
BvD-News
Das Fachmagazin des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Herausgeber:
Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Straße 31
10787 Berlin
Tel: 030 26 36 77 60
Fax: 030 26 36 77 63
E-Mail: bvd-gs@bvdnet.de
Internet: www.bvdnet.de
www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands
www.twitter.com/bvd_datenschutz
https://www.bvdnet.de/feed/

Redaktion:
Thomas Spaeing
(V.i.S.d.P., bvd-news@bvdnet.de)
Katrin Eggert, Regina Mühlich

Fotos:
123rf.com

Lektorat:
Frank Spaeing

Anzeigen:
Katrin Eggert
(bvd-gs@bvdnet.de)

Satz und Layout:
Trend Point Marketing GmbH,
Breitenbachstraße 24-29, 13509 Berlin
www.tpmarketing.de

Druck:
Trend Point Marketing GmbH,
Breitenbachstraße 24-29, 13509 Berlin
www.tpmarketing.de

ISSN: 2194-1025
Erscheinungsweise: 3 × jährlich, ca. 2.500 Exemplare
(Mediadaten anfordern unter bvd-gs@bvdnet.de)
Die Redaktion behält sich vor, Beiträge redaktionell zu überarbeiten und zu kürzen. Namentlich gekennzeichnete Beiträge müssen nicht die Meinung des BvD e.V. wiedergeben.

EDITORIAL

Zwei Schritte vor – einen zurück? – *Thomas Spaeing* 3

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Vier Wochen DS-GVO - Plädoyer für einen konstruktiven Dialog – *Peter Schaar* 5
Die Umsetzung der DS-GVO in Deutschland – *Thilo Weichert* 9
Die Europäische Datenschutz-Grundverordnung - eine Evolution, keine Revolution, die jedoch nicht ignoriert werden sollte – *Jutta Sonja Oberlin und Yasmine Deryckere* 13
Start-Ups und DS-GVO – Rechtliche Herausforderungen und Besonderheiten – *Kevin Marschall, LL.M. und Stephan Blazy, LL.M.* 16
DS-GVO seit Mai 2018 auch für Schweizer Unternehmer relevant – *Regina Mühlich* 22
Erlaubnistatbestand der Vertragsdurchführung – auch Dritte profitieren – *Dr. Carlo Piltz* 25
Transparenz als Strukturentscheidung – *Maria Wilhelm* 28
Die ISO 27018 im Lichte der DS-GVO – *Stefan Staub* 32
Technische und organisatorische Maßnahmen unter der DS-GVO: Herangehensweise und Auslegungen der Gesetzesterminologie in Bezug auf die Datensicherheit – *Jutta Sonja Oberlin und Gianni Crameri* 34

DATENSCHUTZPRAXIS

„Videobeweis“ auch im Straßenverkehr? – Rechtliche und praktische Konsequenzen der BGH-Entscheidung zum Einsatz von Dashcams – *Dr. Wolf-Tassilo Böhm und Isabelle Brams* 42
Bayerisches Verwaltungsgericht entscheidet über Einsatz von Facebook-Marketing-Tool – *Kristin Benedikt* 46
Reifegradmodell zur Darstellung der TOM – *Stephan Rehfeld* 50
Das neue KDG (Gesetz über den Kirchlichen Datenschutz) - Übersicht & Arbeitshilfen – *Steffen Pau* 54
SESSION TRACKING: So können Ihre User „MAN-IN-THE-MIDDLE-ATTACKEN“ stoppen – *Dennis Okpara, Al Lakhani, Calvin Hoenes, Dr. Daniel Schellenberg* 58

AUFSICHTSBEHÖRDE

Datenschutz macht selbstbewusst – *Kinder fordern besseren Datenschutz für ihre Generation* 62
Der Spur der Daten folgen – *„Projekt Freiheit 2.0“ in Stuttgart* 64

GESELLSCHAFT

Ohne Vertrauen geht es nicht – *Klaus Müller* 67
Datenschutzschulung – Auf die Innovative Art – *Dr. Niels Lepperhoff und Dipl. Ing. Harald Mais* 72

AUS DEM VERBAND

BvD Verbandstage 2018 - Ein Rückblick – *Datenschutzrechtliche Zeitenwende – Kopfzerbrechen inklusive* 76
Erfolgs-Motor DAME - Wie der BvD Filme- und Videomacher mit dem Datenschutz Medienpreis fördert 79
Vortagsreihe Daten-Dienstag – *Rückblick* 82

REZENSIONEN

„Datenschutz 2018“ – *Regina Mühlich, Boris Maskow, Sascha Kuhrau, Dr. Jan K. Köcher, Martin Agethen, LL.M., Katharina Schreiner, Peer Lambertz* 84
„Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung: Lösungen zur praktischen Umsetzung Textbeispiele, Musterformulare, Checklisten“ – *Grit Reimann* 85
„Sozialrechtshandbuch (SRH)“ – *Ruland / Becker / Axer (Hrsg.)* 86

TERMINE UND KONTAKTE

Termine der Regionalgruppen und Arbeitskreise des BvD 87
Überblick Seminare und Workshops 2018 88

SERVICE

Wichtige Kontakte im Überblick 89

VIER WOCHEN DS-GVO - PLÄDOYER FÜR EINEN KONSTRUKTIVEN DIALOG

Peter Schaar

Der Start des neuen Europäischen Datenschutzrechts verlief holprig, zumindest in Deutschland. Der Datenschutz schaffte es sogar auf die Titelseiten auflagenstarker Tageszeitungen, allerdings vorwiegend mit negativen Schlagzeilen. In kaum einem Lokalblatt fehlten Leidensmeldungen örtlicher Vereinsvorstände, Handwerker und Unternehmer über den mit der Umsetzung verbundenen Aufwand. Auch in Social Media hatten die Kritiker rein zahlenmäßig die Oberhand. Schließlich beschäftigte sich der Deutsche Bundestag genau drei Wochen nach dem Wirksamwerden der Datenschutzgrundverordnung mit der Materie – und auch hier gab es viel Kritik. Irgendetwas ist hier offenbar grundlegend schief gelaufen. Was sind die Ursachen dafür, dass sich jetzt viele überfordert fühlen? Und wie könnte eine Abhilfe aussehen?

Kommunikationsprobleme

Immer wieder hört man die Behauptung, die DS-GVO sei am 25. Mai 2018 „in Kraft getreten“. Tatsächlich ist das Regelwerk aber schon seit mehr als zwei Jahren in Kraft, seit Mai 2016. Die Falschaussage belegt, dass sich die wenigsten Entscheidungsträger in der Politik, der Wirtschaft und Gesellschaft rechtzeitig ernsthaft mit dem Datenschutz beschäftigt hatten. Viele Rechtsanwender haben die zweijährige Anpassungszeit bis zum Wirksamwerden der DS-GVO ungenutzt verstreichen lassen, wie Umfragen des Digitalverbandes Bitkom belegen. Die wenigsten Unternehmen hatten ihre Vorbereitungen auf das neue Datenschutzrecht fristgerecht abgeschlossen, manche hatten damit sogar erst unmittelbar vor dem 25. Mai begonnen. Noch erheblich gravierender war die Situation in Vereinen, Handwerksbetrieben, Selbstständigen und kleinen Betrieben: Vielfach nahmen Vorstände und andere Verantwortliche erst nach dem Wirksamwerden die Neuregelungen wahr. Umso größer war die Verunsicherung, ja Empörung bei Manchen, denen sehr spät klar wurde, dass sie sich nun ernsthaft mit der Materie auseinandersetzen müssen.

Die vielfach sehr späte Beschäftigung mit den neuen datenschutzrechtlichen Anforderungen ist großen Teils Ergebnis eines gravierenden Kommunikationsproblems: Die Bundesregierung hat dem Thema in ihrer Öffentlichkeitsarbeit kein besonderes Interesse gewidmet. So hat das für den Datenschutz zuständige Bundesinnenministerium erst im April 2018 ein Dokument zu einigen Grundfragen der neuen Datenschutzregeln auf seine Website gestellt, das aber ansonsten sehr allgemein bleibt. Zudem hat das Ministerium einige wenige Informationsveranstaltungen ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

für interessierte Verbände durchgeführt, aber auch diese erst zu einem sehr späten Zeitpunkt.

Auch die Öffentlichkeitsarbeit der unabhängigen Datenschutzbehörden über die Neuregelungen war kein Ruhmesblatt. Die immerhin 18 deutschen Behörden haben zwar einige gemeinsame Positions- und Kurzpapiere zu wichtigen Fragen veröffentlicht. Auf den Websites der Bundes- und Landesdatenschutzbeauftragten findet man darüber hinaus eine zunehmende Zahl von Leitfäden, Handreichungen und Anwendungshilfen. Sie haben allerdings den Nachteil, dass sie vielfach nicht abgestimmt sind und sich in einzelnen Punkten sogar widersprechen. Im Vergleich zu den Informationen, Tools und Medieninformationen der Datenschutzbehörden anderer Mitgliedsstaaten — etwa der britischen ICO oder der französischen CNIL — nimmt sich die Öffentlichkeitsarbeit der deutschen Datenschutzbehörden zum neuen Datenschutzrecht aber eher bescheiden aus.

Interpretationsspielräume

Die DS-GVO enthält eine Vielzahl von allgemeinen Rechtsbegriffen und auslegungsbedürftigen Regelungen. Zudem hatten die Regierungen der Mitgliedsstaaten gegenüber der Europäischen Kommission und dem Europäischen Parlament zahlreiche Öffnungsklauseln durchgesetzt, die durch nationales Recht gefüllt werden können oder sogar müssen. Damit wurde das wichtigste Ziel der Neuregelung in Frage gestellt, ein einheitliches Datenschutzrecht in der gesamten EU. Was zu befürchten war, ist inzwischen eingetreten: Die in nationalen Anpassungs- und Umsetzungsgesetze fallen sehr unterschiedlich aus. Dies hat zur Konsequenz, dass sich grenzüberschreitend tätige Unternehmen, anders als versprochen, weiterhin mit den Besonderheiten des nationalen Rechts auseinandersetzen müssen. Für große Unternehmen mit leistungsstarken Rechtsabteilungen ist das kein großes Problem, für kleinere Unternehmen und StartUps schon.

Bei näherem Hinsehen liefert das im Sommer 2017 beschlossene BDSG vor allem zusätzliche Spielräume für die staatliche Datenverarbeitung und schränkt Betroffenenrechte und Kontrollbefugnisse der Datenschutzbehörden ein. Dort, wo konkrete Regelungen erforderlich sind, bleibt das BDSG aber wenig konkret - etwa beim Datenschutz im Beschäftigungsverhältnis. Oder sie fehlen völlig - etwa beim gebotenen Ausgleich von Meinungsfreiheit und Datenschutz. Letzteren wollte die Bundesregierung allem Anschein nach völlig den Ländern überlassen, obwohl es hier durchaus Regelungsnotwendigkeiten im Bundesrecht gibt. Erst als daran Kritik aufkam, insbesondere im Hinblick auf den Umgang mit digitalen Fotografien, äußerte sich das Bundesinnenministerium dahingehend, dass das Kunsturhebergesetz weiterhin anwendbar sei. Zwar ist diese Klarstellung durchaus vertretbar, sie lässt allerdings weite Aspekte der Nutzung von Social Networks offen. Zudem wäre es durchaus möglich und sinnvoll gewesen, das betagte Gesetz — es stammt aus dem Jahr 1907 — im Sinne der Abwägung der widerstreitenden Grundrechte an die Vorgaben der Datenschutzgrundverordnung anzupassen.

Regelungslücken gibt es auch bei den in Deutschland besonders zahlreichen bereichsspezifischen Gesetzesbestimmungen zum Datenschutz. Eine Reihe davon wurde zwar im letzten Jahr novelliert — aber ohne die gebotene gründliche parlamentarische Beratung. Wie beim BDSG konzentrierte sich die Große Koalition auch hier vor allem darauf, bestehende Befugnisse zur behördlichen Datenverarbeitung abzusichern. Die Chance zu einer echten inhaltlichen Weiterentwicklung wurde verpasst.

Äußerst unklar ist die Rechtslage beim Datenschutz im Internet. So ist fraglich, inwieweit das Telemediengesetz (TMG) noch gilt, denn es ist umstritten, in welchem Verhältnis die Vorgaben der nach wie vor gültigen europäischen E-Privacy-Richtlinie und die Bestimmungen der DS-GVO stehen. Die Datenschutzbehörden des Bundes und der Länder vertreten die Position, dass die zentralen TMG-Regelungen zur Zulässigkeit der Verarbeitung nicht mehr angewendet werden dürfen. Vermutlich werden wir auf verbindliche Antworten bis zu einem Beschluss über die diskutierte E-Privacy-Verordnung warten müssen — wenn sie denn überhaupt kommt. Der Brüsseler Trilog darüber verläuft offenbar sehr zäh.

Auch bei der Datenschutzaufsicht bei Telekommunikationsunternehmen besteht große Unsicherheit. Da das Telekommunikationsgesetz (TKG) noch nicht novelliert wurde, stellt sich die Frage nach der Zuständigkeit für die Datenschutzaufsicht und deren Sanktionsbefugnissen. Die Aufgabenzuweisung für die Datenschutzkontrolle an die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) dürfte zwar Bestand haben. Anders sieht es jedoch in Bezug auf die Verfolgung von Ordnungswidrigkeiten und die Verhängung von Bußgeldern aus, die bisher der Bundesnetzagentur (BNA) oblagen. Angesichts der klaren Vorgaben der DS-GVO stehen diese Befugnisse seit dem 25. Mai 2018 allein der BfDI zu, denn nur sie ist eine unabhängige Datenschutzbehörde. Sollte die BNA gleichwohl Datenschutzverstöße mit Bußgeldern belegen, würde dies mit einem erheblichen rechtlichen Risiko verbunden sein.

Föderalismus

Die vom Grundgesetz vorgegebene föderale Struktur Deutschlands wirkt sich auch auf den Datenschutz aus. Dies muss nicht unbedingt schlecht sein, denn die Landesbehörden, denen neben der Datenschutzkontrolle der öffentlichen Stellen der Länder auch die Aufsicht über die Wirtschaft obliegt, sind näher an den Bürgerinnen und Bürgern und an den lokalen Datenverarbeitern, als es eine Bundeszentralbehörde sein könnte. Angesichts der durch die DS-GVO bewirkten signifikanten Ausweitung der Aufgaben, zusätzlicher Befugnisse und enger Bearbeitungsfristen sind aber die Nachteile des föderalistisch organisierten Datenschutzes nicht mehr zu übersehen.

Dass die Landesgesetze zum Datenschutz unterschiedliche Vorgaben beinhalten, ist nicht neu. Die DS-GVO hätte zum Anlass genommen werden können, diese Differenzen abzubauen oder zu beseitigen. Leider hatten sich die zuständigen Landesministerien aber nicht einmal auf einen Musterentwurf verständigen können. Zudem ist der Gesetzgebungsprozess in den Ländern sehr erst recht spät in Gang gekommen, so dass bis zum 25. Mai 2018 ein Teil der Landesdatenschutzgesetze nicht novelliert war. Das ist ein Problem, denn die alten, als Vollregelungen ausgelegten Gesetze sind nach dem Wirksamwerden der DS-GVO zum Teil nicht mehr anzuwenden.

Bei den bereichsspezifischen Bestimmungen der Länder sieht es kaum besser aus. Zwar wurden durch den 21. Rundfunkänderungsstaatsvertrag einige medienrechtliche Regelungen upgedatet, jedoch erfolgte das in einer Weise, die den Vorgaben der DS-GVO kaum gerecht zu werden vermochte.

Der von der DS-GVO erteilte Gesetzgebungsauftrag, für einen Ausgleich zwischen Datenschutz und Informations- und Meinungsfreiheit zu sorgen, wurde von den Ländern einseitig dahingehend interpretiert, den redaktionell-journalistischen Bereich weiterhin pauschal von den wichtigsten Vorgaben des Datenschutzrechts auszunehmen. In vielen anderen Bereichen haben sich die Länder nicht einmal auf gemeinsame Vorgaben einigen können, etwa im Presserecht. Damit bleibt das Patchwork unterschiedlicher Datenschutzbestimmungen auch hier erhalten.

So stellt sich die Frage, ob das wichtigste zugunsten unterschiedlicher Datenschutzbestimmungen angeführte Argument überhaupt greift: Ein Wettbewerb der Länder um den besten Datenschutz („kompetitiver Föderalismus"). Schon in den letzten zwei Dekaden musste man solche datenschutzrechtlichen Innovationen mit der Lupe suchen. Angesichts der durch die DS-GVO eingeschränkten Regelungskompetenzen der Länder werden die Spielräume für eine kreative Weiterentwicklung des Datenschutzes jedenfalls noch geringer.

Die DS-GVO versieht die Datenschutzbehörden mit stärkeren Durchsetzungs- und Sanktionsbefugnissen. Um eine einheitliche Aufsichtspraxis zur gewährleisten, enthält das neue Recht zudem detaillierte Vorgaben zur gegenseitigen Kooperation und zur Kohärenz ihrer Entscheidungen. Eine zentrale Stellung nimmt dabei der Europäische Datenschutzausschuss (EDSA) ein, der von den nationalen Datenschutzbehörden beschickt wird. Es liegt auf der Hand, dass es großer Anstrengungen bedarf, um die Positionen der Vertreter der Aufsichtsbehörden der 28 Mitgliedsländer unter einen Hut zu bringen. In Deutschland mit seinen 18 unabhängigen Datenschutzbehörden — Bundesbeauftragte, Landesbeauftragte und LDA Bayern — (hinzu kommen die Datenschutzbeauftragten der Kirchen und der Landesrundfunkanstalten) besteht zusätzlich die Notwendigkeit zur Vereinheitlichung auf nationaler Ebene.

Die BfDI vertritt Deutschland im EDSA und ist „zentrale Anlaufstelle" für grenzüberschreitende Datenschutz-Angelegenheiten. Ihre Stellvertreter/-in ist vom Bundesrat aus dem Kreis der Leiter-/innen der Landesdatenschutzbehörden zu wählen. Leider hat der BR jedoch den bzw. die Ländervertreterin nicht gewählt, so dass die BfDI Deutschland ▸

bis auf weiteres allein im EDSA vertritt, aber in Fragen, die in Länderzuständigkeit liegen, an das Votum der Landesdatenschutzbehörden gebunden ist.

Das neue BDSG hat die Regelungen der DS-GVO für die Zusammenarbeit der Aufsichtsbehörden im EDSA für sinngemäß für die Kooperation der deutschen Datenschutzbehörden untereinander für anwendbar erklärt, allerdings nur, soweit es um Angelegenheiten geht, die im EDSA verhandelt werden. Dies bedeutet, dass die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) erheblich aufgewertet wurde und Entscheidungen zur Datenschutzaufsicht per Mehrheitsbeschluss treffen kann. Ob dies generell zu einer Vereinheitlichung der Datenschutzaufsicht in Deutschland führt, bleibt abzuwarten. Absehbar ist aber schon jetzt, dass das zweistufige Verfahren der Meinungsbildung - auf nationaler und auf europäischer Ebene - erheblichen Aufwand erzeugt und die Möglichkeiten Deutschlands, auf die Entscheidungen des EDSA einzuwirken, erheblich einschränkt.

Was jetzt zu tun ist

Angesichts der verbreiteten Verunsicherung brauchen wir zunächst eine **Kommunikationsoffensive** der Bundesregierung und der Datenschutzbehörden. Es ist Sache insbesondere des Bundesinnenministeriums, den Kenntnisstand in der Bevölkerung über die Bedeutung, die Prinzipien und konkreten Regelungen zum Datenschutz zu verbessern. Besonders gefragt sind die Datenschutzbehörden: Sie müssen unmissverständliche Antworten auf die zentralen Auslegungsfragen geben. Auch wenn sich wirkliche Rechtssicherheit erst mittelfristig einstellen wird, wenn sich eine gefestigte Rechtsprechung herausgebildet hat, brauchen die Bürgerinnen und Bürger, Vereine und Unternehmen und auch die öffentlichen Stellen klare Aussagen der Datenschutzbehörden darüber, wie sie die Rechtsvorschriften verstehen und woran sie sich in ihrer Aufsichtspraxis orientieren werden. Die 19 von der Datenschutzkonferenz bisher veröffentlichten „Kurzpapiere" sind zwar ein guter Ausgangspunkt, ausreichend sind sie bei weitem nicht. Notwendig sind abgestimmte, zielgruppenorientierte Anwendungshinweise, Musterformulare und elektronische Tools. Statt das Rad immer wieder neu zu erfinden, sehe ich die dringende Notwendigkeit zu gemeinsamen Positionierungen. Wenn nötig, sollte die DSK auch hier mit Mehrheit entscheiden.

Die **Gesetzgebung** muss auf Bundes- und Landesebene zügig vorangebracht werden. Dies gilt sowohl für die Landesdatenschutzgesetze als auch für die spezialgesetzlichen Datenschutzbestimmungen. Angesichts der verbreiteten Verunsicherung - etwa bei der Benennungspflicht von Datenschutzbeauftragten bei nicht-öffentlichen Stellen - sollte hier eine Präzisierung erfolgen, ebenso hinsichtlich der Bestimmungen zum Ausgleich von Meinungsfreiheit und Datenschutz und beim Datenschutz im Internet und in Sozialen Netzwerken. Notwendig sind auch Gesetzeskorrekturen im Wettbewerbsrecht, die sicherstellen, dass Missbräuche von Abmahnmöglichkeiten unterbunden werden.

Schließlich müssen die **Datenschutzbehörden besser ausgestattet** werden. Die Ausstattung der Datenschutzbehörden mit Personal und Sachmitteln ist in manchen Bundesländern so schlecht, dass sie die vielen ihnen zugewiesenen Aufgaben nicht ansatzweise erfüllen können. Dies hat zur Konsequenz, dass ihre Aufsichtstätigkeit nicht effektiv wahrnehmen können und auch nicht über die notwendigen Beratungskapazitäten für Bürger, Vereine, Unternehmen und Kommunen verfügen.

Es bleibt zu hoffen, dass alle Beteiligten möglichst bald in einen **konstruktiven Dialog** kommen und die notwendigen Schritte unternehmen, damit das neue Europäische Datenschutzrecht seine zentrale Aufgabe erfüllt: Die datenschutzrechtliche Flankierung der Digitalisierung, die ohne entsprechende Leitplanken sehr schnell zu einer Sackgasse werden könnte. Datenschutz und informationelle Selbstbestimmung sind zentrale Grundrechte des Informationszeitalters - das dürfen wir bei aller Kritik an dieser oder jener Regelung nicht aus dem Auge verlieren!

Über den Autor

Peter Schaar

Bundesbeauftragter für den Datenschutz a.D.
Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID), Berlin

▶ www.eaid-berlin.de

DIE UMSETZUNG DER DS-GVO IN DEUTSCHLAND

Thilo Weichert

Die Umsetzung der Europäischen Datenschutz-Grundverordnung (DS-GVO) ist – zumindest für Datenschützer – spannend wie ein Krimi: Die Einführung dieses grundsätzlichen Gesetzeswerks mit Auswirkungen auf unseren Alltag und unsere Wirtschaft ist in der Rechtsgeschichte der EU einzigartig. Gesetze werden nicht einfach beschlossen und dann exekutiert, schon gar nicht, wenn es um Grundrechtsschutz geht. Überraschungen – positive wie negative – gab und gibt es zu Hauf. Das Wechselspiel zwischen Europa, Deutschland und den Bundesländern, zwischen Politik und Rechtsprechung, zwischen Datenschutzaufsicht, Wirtschaft und Verwaltung sowie Betroffenen, produziert überraschende Ergebnisse. Wenige Tage nach dem Wirksamwerden der DS-GVO kann gesagt werden, dass die DS-GVO ein Erfolgsmodell ist und das Zeug zu mehr hat.

Vor der DS-GVO

Der DS-GVO geht eine Erfolgsgeschichte des Datenschutzes in Deutschland voraus, der für die DS-GVO in starkem Maß bestimmend war. Die Initiativen hierfür gingen nie von der Bundespolitik aus, sondern von der Wissenschaft, der Rechtsprechung und den Bundesländern. 1970 erließ Hessen das weltweit erste Datenschutzgesetz und war unter dem Einfluss von Spiros Simitis wegweisend und inspirierend. Das 1971 veröffentlichte Gutachten „Grundfragen des Datenschutzes" von Wilhelm Steinmüller und anderen legte die wissenschaftliche Grundlage für die weitere Gesetzgebung. Das Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 und später dessen Urteil zur Online-Durchsuchung 2008 haben den Datenschutz verfassungsrechtlich auf eine solide moderne Grundlage gestellt.

In den 90er Jahren wurde die Notwendigkeit einer europäischen Harmonisierung des Datenschutzes angesichts der Informatisierung des EU-Binnenmarktes immer drängender. Datenschützer in Deutschland – ich eingeschlossen – befürchteten ein Verhökern des Grundrechtsschutzes auf dem freien Markt. Dazu kam es nicht. Die Rechtsform der Richtlinie ermöglichte Harmonisierung wie auch nationale experimentelle Sonderwege, etwa in Deutschland mit dem betrieblichen Datenschutzbeauftragten. Es wurden rechtliche Standards festgeschrieben, die international Anerkennung fanden. Die Flexibilität der Richtlinie ermöglichte es zugleich, nationalen Besonderheiten gerecht zu werden. Zu flexibel waren aber die Ausweichmöglichkeiten etwa von US-Internet-Unternehmen, die sich insbesondere Irland als datenschutzfreie Oase auswählten. Zu unflexibel erwies sich die Richtlinie bzgl. ihrer Anpassungsfähigkeit an die rasante technische Entwicklung.

Nach der EG-Richtlinie 1995 war es Schleswig-Holstein, das unter dem Einfluss von Helmut Bäumler im Jahr 2000 innovative und moderne Elemente ins Datenschutzrecht einführte: Das dortige Landesdatenschutzgesetz enthielt einen umfassenden Verarbeitungsbegriff, eine Regelung zu Datenvermeidung und Datensparsamkeit, sah Gütesiegel- und Auditverfahren und ein strukturiertes Verfahren bei der Einführung neuer Informationstechnik (IT) mit Dokumentation, Test und Freigabe vor, regelte den technischen Datenschutz technikneutral über Schutzziele, benannte explizit spezielle Sicherungsmaßnahmen wie z. B. die Verschlüsselung, normierte gemeinsame Verfahren, mobile Systeme und die Internetveröffentlichung, privilegierte die pseudonyme Datenverarbeitung und ergänzte das Aufsichtsregime um Service-, Beratungs- und Zertifizierungsfunktionen. In der Praxis kamen Forschungs- ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

aktivitäten der Aufsichtsbehörde hinzu. Vieles von dem, was 2000 in Schleswig-Holstein Gesetz und Praxis wurde, war damals weltweit einzigartig und findet sich heute in der DS-GVO wieder. Keines dieser Instrumente wurde von der Bundespolitik bei der Ausarbeitung der DS-GVO offensiv gefördert, einiges wurde – zumeist nur symbolisch – aufgegriffen (z. B. Datensparsamkeit, Audit, Definition der Pseudonymisierung).

Die Verabschiedung der DS-GVO

Mit der Diskussion über die DS-GVO 2012 verlagerte sich der Fokus nach Brüssel bzw. nach Europa. Die zuständige Kommissarin Viviane Reding und der Berichterstatter im EU-Parlament Jan-Philipp Albrecht sorgten dafür, dass Sabotageversuche von Gegnern digitaler Grundrechte und von Wirtschaftslobbyisten abgewehrt und eine fortschrittliche Gesetzgebung vorangetrieben wurden. Die deutsche Politik profilierte sich mit Angriffen auf die Pläne und mit Verzögerungsaktionen. Es sollte eine Richtlinie sein, nicht eine direkt anwendbare Verordnung. Der Bundesrat demonstrierte per Subsidiaritätsrüge sein provinzielles Datenschutzverständnis. Das Bundesinnenministerium machte sich zum Sprachrohr von Wirtschaftsinteressen und favorisierte privatwirtschaftliche Selbstregulierung und die Beseitigung des Gesetzesvorbehalts im nichtöffentlichen Bereich. Noch wenige Tage vor dem Abschluss des Trilogs zwischen Kommission, Parlament und Rat der EU Ende 2015 propagierte die Spitze der Bundesregierung mit Angela Merkel (CDU), Siegmar Gabriel (SPD) und Alexander Dobrindt (CSU) – in erklärter Opposition zur DS-GVO – die Aufweichung des Zweckbindungsgrundsatzes und „Datenreichtum", um das „Öl des 21. Jahrhunderts", also personenbezogene Daten, für die Wirtschaft leichter nutzbar zu machen. Besonders perfide war die – im Ergebnis erfolglose – Argumentation der Bundesregierung gegen die DS-GVO, mit dieser gingen die Errungenschaften des angeblich so fortschrittlichen deutschen Datenschutzes verloren.

Die europäischen Institutionen einigten sich nicht nur auf ein Präzisierung der Datensparsamkeit und der Zweckbindung, sondern auf weitere zeitgemäße Instrumente des digitalen Grundrechtsschutzes in einer globalisierten Informationsgesellschaft: harmonisierte verbindliche Regelungen, Marktortprinzip, One-Stop-Shop für Unternehmen und Betroffene, verbesserte Betroffenentransparenz, „Privacy by Default" und „Privacy by Design", generelle Anwendbarkeit der Datenschutz-Folgenabschätzung, rechtssicherere Drittlands-Datentransfers, verbesserte Beschwerde- und Rechtsschutzmöglichkeiten, wirksame Sanktionen.

Kontroll- und Sanktionskompetenz

Die deutsche Politik versuchte nun, über eine extensive Interpretation der Öffnungsklauseln das zurückzuholen, was sie gegenüber dem europäischen Gesetzgeber nicht verhindern konnte: eine effektive Datenschutzkontrolle und -sanktionierung. Bei der zeitgleich mit der DS-GVO verabschiedeten Datenschutzrichtlinie für Polizei und Justiz wurde, statt wirksame Abhilfeinstrumente vorzusehen, auf die zahnlose Beanstandung fokusiert. Nicht nur gegenüber Post- und Telekommunikationsunternehmen, sondern auch im gesamten öffentlichen Bereich wurden die Sanktionsmöglichkeiten auf symbolische Rechtsakte reduziert, indem nicht nur Bußgelder, sondern auch die zwangsweise Durchsetzung von rechtskräftigen Anordnungen ausgeschlossen wurde. Das Vorbild dafür gab der Bund mit seinem BDSG; die Landesgesetzgeber schlossen sich gerne nicht nur dieser Fehlinterpretation des europäischen Rechts an.

Jeder Sanktion muss Kontrolle vorausgehen. Die aktuellen Strategien, sich der aufsichtlichen Kontrolle zu entziehen, erinnern erschreckend an vergleichbare Versuche in der Frühzeit des Datenschutzes. So bleibt die Geheimdienstkontrolle eingeschränkt wie bisher. Landesbeauftragte beanstandeten immer wieder zu Recht massenhafte Rechtsverstöße von Finanzämtern z. B. in Form von Auskunftsverweigerungen, die durch Erlasse des Bundesfinanzministeriums gedeckt waren. 2017 wurden diese Verstöße durch eine Änderung der Abgabenordnung formal legitimiert; zugleich entledigte man sich der Kontrolle durch die Landesdatenschützer und übertrug die Aufgabe der zahnlos agierenden Bundesbeauftragten. Der Staatsanwaltschaft wurde, entgegen der Rechtsstellung in Deutschland, justizielle Unabhängigkeit zugesprochen. In Niedersachsen wurde gar das gesamte strafrechtliche Ermittlungsverfahren, auch wenn es von der Polizei geführt wird, von der Datenschutzkontrolle ausgenommen.

Einen besonderen Coup landete die Anwaltschaft, die sich unter Verweis auf eine Öffnungsklausel mit dem § 29 Abs. 3 BDSG unter Berufung auf ihr Mandantengeheimnis der Datenschutzkontrolle entziehen kann. Dieser Kontrollausschluss erfasst sämtliche Berufsgeheimnisträger, z. B. auch die Ärzteschaft mit ihrem Patientengeheimnis. In Baden-Württemberg wurden auch die öffentlichrechtlichen Notare von der unabhängigen Datenschutzkontrolle befreit. Dass es sich bei der Verarbeitung von Berufsgeheimnissen sowie bei strafrechtlichen Ermittlungen um persönlichkeitsrechtlich besonders intensive Eingriffe handelt und insofern das BVerfG eine besonders intensive Prüfung einforderte und Art. 8 Abs. 3 GRCh kontrollfreie Räume ausschließt, ließ die jeweiligen Gesetzgeber kalt.

Effektiver Datenschutz wird auch durch die systematische Überforderung von Aufsichtsbehörden verhindert. Das bisherige Personal und die bereit gestellten Ressourcen genügten schon bisher nicht zur wirksamen Aufgabenerfüllung. Die erlangten Zuwächse wegen der DS-GVO in den Haushalten stehen zumeist in keinem Verhältnis zu den zusätzlichen Aufgaben. Besonders profiliert sich hier die Politik Hamburgs, deren Aufsichtsbehörde in Deutschland für Google, Facebook und viele weitere große Unternehmen zuständig ist. Sie soll ihre Aufgabe künftig mit insgesamt 25 Stellen stemmen, was ein unmögliches Ansinnen darstellt. Dem gegenüber wurde eine lammfromme Bundesbeauftragte vergleichsweise üppig ausgestattet. Der Verdacht drängt sich auf, dass so Zahnlosigkeit mit Ressourcenzuwachs belohnt wurde.

Es besteht die begründete Gefahr, dass sich nicht nur die Bundesländer, sondern auch andere EU-Mitgliedsländer die Bundesgesetzgebung zum schlechten Vorbild nehmen. Animiert von Antidatenschutzpropaganda verschlechterte kurz vor dem 25.05.2018 die ÖVP/FPÖ-Mehrheit in Österreich ein schon verabschiedetes Datenschutzgesetz, mit dem Ziel, Sanktionsmöglichkeiten weiter zu reduzieren.

Die leidige Föderalismusdebatte

Harmonisierungsdruck war ein Motor der DS-GVO-Gesetzgebung. Hierfür gibt es nun administrativ in den Art. 60 ff. DS-GVO Kooperations- und Kohärenzregeln. Viele Bundespolitiker, insbesondere bei der CDU, versuchen nun, im Einklang mit Wirtschaftsforderungen die föderale Kontrolle zu zentralisieren. Schon in den Jahren 2011/2012 wurde die Aufsicht wesentlicher Sozialbereiche (Arbeitslosenverwaltung, Krankenkassen) von den Ländern auf den Bund übertragen. Die nächste Kompetenzbeschneidung der Länderaufsicht erfolgte 2017 für die Finanzverwaltung. Die Vertretung Deutschlands im Europäischen Datenschutzausschuss (EDSA) wurde der sachlich weitgehend unzuständigen Bundesbeauftragten (BfDI) übertragen. Und die Stellvertretung im EDSA wird gemäß § 17 Abs. 2 BDSG – unter Missachtung der Unabhängigkeit der Aufsicht – politisch vom Bundesrat besetzt.

Bei den ersten Divergenzen zwischen der BfDI und der Landesaufsicht nach dem 25.05.2018 in Bezug auf die Erstellung von Blacklists bzw. Whitelists zur Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DS-GVO wurde sofort wieder die Forderung nach nur einer Datenschutzaufsicht in Deutschland erhoben. Wer in diesen Chor einstimmt, übersieht, dass der Föderalismus den Datenschutz bisher mehr voranbrachte, als dass er ihn behinderte.

Von den kurz vor oder nach dem 25.05.2018 verabschiedeten Landesdatenschutzgesetzen gehen aber keine Fortschritte aus. Der Versuch einer Koordinierung der Landesgesetzgebung wurde frühzeitig abgebrochen. Heraus kamen bzw. kommen Gesetze, deren Einheitlichkeit dort am größten ist, wo grundrechts- und europarechtswidrige Normen des BDSG kopiert werden. Es bleibt weiterhin die Chance für die Länder, beim digitalen Grundrechtsschutz innovativ voranzuschreiten. Soweit Landesgesetzgeber wegen der terminlichen Zwangslage eine Evaluation des neuen Datenschutzrechts nach zwei Jahren zusagten, sollten sie dabei den Blick nicht nur nach hinten, sondern vor allem nach vorne richten.

Eine weit verbreitete Praxis bestand in der Vergangenheit darin, die Leitung der Aufsichtsbehörden mit Personen zu beauftragten, deren mangelnde fachliche Kompetenz durch die Perspektive politischer Gefügigkeit „kompensiert" wurde. Dem hat Art. 53 Abs. 2 DS-GVO ein wenig dadurch vorgebeugt, dass Qualifikation, Erfahrung und Sachkunde gefordert werden. Weiterhin fordert Art. 53 Abs. 1 DS-GVO die Benennung in einem „transparenten Verfahren". Bisher wurden die „Mitglieder" zumeist in Hinterzimmern ausgekungelt. Hieran soll sich aber gesetzlich nichts ändern: Ausschreibungen und ein öffentliches Auswahlverfahren sind nirgendwo in Deutschland vorgesehen, wohl aber, dass die Wahl „ohne Aussprache" erfolgt. ▸

Die gefühlte Praxis

Zeitlich kurz vor der direkten Anwendbarkeit der DS-GVO erlebten wir ein erstaunliches Phänomen: Rechtsanwälte, Unternehmensberater und professionelle Datenschützer mussten Überstunden schieben. Zwar waren die Regeln lange bekannt, mit ihrer Umsetzung befassten sich viele erst wenige Wochen vor dem Tag, ab dem – vermeintlich – Abmahnungen oder Bußgelder drohten. Der Panik vor dem 25.05.2018 und letztlich vor dem Datenschutz allgemein wurde befeuert durch Geschäftemacher, die mit den starken Sanktions- und Abmahnmöglichkeiten dafür warben, die Aufgabe des Datenschutzes auf sich outzusourcen und damit oft für überteuertes Geld in wenig kompetente Hände zu übertragen.

Die absolut überzogene und mit Falschinformationen gespickte Angstmache hatte einen positiven Effekt: Sie trug dazu bei, dass sich viele Unternehmen erstmals überhaupt mit Datenschutz beschäftigten. Wer sich bisher an das Recht gehalten hat, muss auch in Zukunft wenig befürchten: Aufsichtsbehörden sind nicht nur aus Kapazitätsgründen dem Verhältnismäßigkeitsgrundsatz verpflichtet. Als zusätzliche von Abmahnvereinen feststellbare Pflichtverletzung kommt bei Internetpräsenz allenfalls die Informationspflicht nach Art. 12 ff. DS-GVO in Betracht, die einzuhalten kein Hexenwerk ist. Die Abmahnpraxis der Verbraucherverbände zielte nicht auf kleine Webseitenbetreiber, sondern auf die ganz Großen; hieran wird sich mit der DS-GVO nichts ändern.

Ausblick

Der aktuell dem Datenschutz entgegen gebrachte Respekt sollte erhalten bleiben. Insofern sind Aufsichtsbehörden und Verbraucherorganisationen, aber auch Betriebsräte, Nichtregierungsorganisationen und die Betroffenen gefordert. Offizielle politische Rückenstärkung ist nur begrenzt zu erwarten, wohl aber öffentliche und mediale Unterstützung.

Viele Potenziale der DS-GVO warten noch auf ihre Aktivierung. Dies gilt für die Datenschutzzertifizierung, die 18 Jahre, nachdem sie in Schleswig-Holstein eingeführt wurde, noch nicht abgehoben hat. Ohne eine unabhängige, transparente und fachlich seriöse Zertifizierung werden künftig viele Datenschutzpflichten nicht verlässlich umgesetzt werden können.

Verhaltensregeln aus regulierter Selbstregulierung spielten in der deutschen Datenschutzpraxis bisher nur eine untergeordnete Rolle. Dies sollte sich kurzfristig ändern. Hierüber können Entlastungen für kleine und mittlere Unternehmen (KMU) bewirkt und die Generalklauseln des Art. 6 DS-GVO branchenspezifisch präzisiert werden.

Die Weiterentwicklung des Rechts der Digitalisierung kann und darf mit der DS-GVO nicht stehen bleiben. Europa muss die Datenschutzregeln für die EU-Institutionen und in der E-Privacy-Verordnung für den Bereich der Telekommunikation überarbeiten. Die EU kann aber nur im Rahmen ihrer weiterhin beschränkten normativen Befugnisse tätig werden. Ihre Innovationskraft ist zudem durch den sehr weitgehenden Einigungszwang begrenzt. Hier sind eher nationale Initiativen nötig, die bei Bewährung von Brüssel übernommen werden können und sollten. Dies gilt z. B. für den Beschäftigtendatenschutz. Die föderale Struktur Deutschlands sollte als Chance wahrgenommen werden. Es ist unrealistisch, dass eine neue Föderalismusreform unter den Vorzeichen der Digitalisierung in Angriff genommen werden wird. Insofern sollten sich Bund und Länder auf das Instrument von Staatsverträgen besinnen, das sich im Medienbereich bewährt hat. Über Bund-Länder-Staatsverträge zu Digitalisierungsthemen, etwa für eine Forschungsinfrastruktur, können einheitliche Standards festgelegt werden, die regional wie national diskutiert werden müssen und dadurch letztlich ein hohes Akzeptanzpotenzial haben.

Über den Autor

Thilo Weichert
Mitglied des Netzwerk Datenschutzexpertise; war 2004 bis 2015 Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

▶ www.netzwerk-datenschutzexpertise.de

NETZWERK DATENSCHUTZEXPERTISE

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

DIE EUROPÄISCHE DATENSCHUTZ-GRUNDVERORDNUNG - EINE EVOLUTION, KEINE REVOLUTION, DIE JEDOCH NICHT IGNORIERT WERDEN SOLLTE

Jutta Sonja Oberlin und Yasmine Deryckere

1. Einleitung

Im April 2016 hat die Europäische Union (im Folgenden „EU") einer umfassenden Reform des Regelwerks zum Datenschutz in Europa zugestimmt. Dieses neue Datenschutzinstrument für Europa, die Europäische Datenschutz-Grundverordnung („DS-GVO"), ist am 25. Mai 2018 anwendbar geworden und stellt das Datenschutzrecht auf ein neues Fundament.

Obwohl die DS-GVO auf der früheren Richtlinie 95/46/EG aufbaut, ist sie mit ihren 99 Artikeln und 173 Erwägungsgründen zu den bestehenden Grundsätzen wesentlich umfangreicher und führt eine Reihe neuer Anforderungen für die Unternehmen ein, um den aktuellen digitalen Gegebenheiten gerecht zu werden und darüber hinaus die Rechte von Individuen zu stärken. Diese regulatorische Evolution wird sich aufgrund des exterritorialen Anwendungsbereiches auch auf Unternehmen ausserhalb der EU auswirken, soweit diese Daten von in der EU ansässigen Personen bearbeiten oder Datensubjekte überwachen.

Zusätzlich zu der bisher verfügbaren Literatur, begannen mehrere Datenschutzbehörden, einschließlich der Artikel-29-Datenschutzgruppe[1], Interpretationen und Empfehlungen zur Anwendung der DS-GVO zu erarbeiten und damit, neben dem eigentlichen Gesetzestext, den Mindeststandard für Unternehmen zu setzen, um den Datenschutz so hoch wie möglich in der unternehmerischen Managementagenda[2] zu positionieren.

Die DS-GVO bedeutet für Unternehmen nicht nur einen organisatorischen und finanziellen Mehraufwand, sondern es werden auch die Vorteile des digitalen Zeitalters aufgezeigt. Trotz Vorteilen droht das Gesetz dennoch mit einer strikten Durchsetzung der DS-GVO, falls Unternehmen sich nicht an diese halten.

Die Verordnung zielt darauf ab, die Entwicklung von sich verändernden Geschäftsprozessen zu einem datenschutzfreundlichen Ansatz zu begleiten und ermöglicht es Unternehmen sich auf Datenspeicherung, Datensicherheit und Transparenz von Datenverarbeitungsaktivitäten zu konzentrieren. Anstatt die DS-GVO in Frage zu stellen, müssen Unternehmen diese Chancen nutzen und das gesetzliche Rahmenwerk als vertrauensbildende Massnahme für ihre Kunden verstehen, nicht aber als Showstopper der unternehmerischen Tätigkeit.

Stärkere gesetzliche Rahmenbedingungen

Mit der Anwendbarkeit der Regulation stellen sich Unternehmen nun die Frage, warum sie die DS-GVO ernst nehmen sollten. Auch wenn die Ermittlungen zur Einhaltung der DS-GVO zwischen sechs und acht Monaten dauern werden und einige Datenschutzbehörden nach dem 25. Mai 2018 eine Nachfrist einräumen könnten, ist der Ansatz „Laissez-faire, lassez-passer" eher naiv.[3]

Wie in den Erwägungsgründen ausgeführt, besteht das übergeordnete Ziel der DS-GVO darin, einen starken, kohärenten und harmonisierten Datenschutzrahmen innerhalb der Europäischen Union zu schaffen, der ein hohes Schutzniveau für personenbezogene Daten gewährleistet, welches durch starke Vollzugsmaßnahmen unterstützt wird.[4] Letztere werden durch ▶

[1] Die Artikel-29-Datenschutzgruppe stellt ein unabhängiges Beratungsgremium dar, bestehend aus den Leitern aller nationalen Datenschutzbehörden, einschließlich eines Vertreters der Europäischen Kommission sowie des Europäischen Datenschutzbeauftragten.

[2] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[3] https://www.cnil.fr/fr/rgpd-comment-la-cnil-vous-accompagne-dans-cette-periode-transitoire, 11 April 2018.

[4] Erwägungsgrund 7 DS-GVO.

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Art. 58 DS-GVO normiert. In diesem Artikel werden alle Ermittlungs-, Korrektur- und Beratungsbefugnisse der Datenschutzbehörden geregelt. Zu diesem Zweck haben einige EU-Mitgliedstaaten bereits begonnen, ihre Datenschutzbehörden zu reformieren; so zum Beispiel Belgien mit dem Gesetz zur Einrichtung der Datenschutzbehörde in 2017.[5]

Für einige Behörden stellen die Vollstreckungsbefugnisse eine Neuheit im Datenschutzrecht dar. Diese weiteren Befugnisse der Behörden lassen aber auch Zweifel erwachsen, ob diese überhaupt im Stande sind die grundlegend neuen Aufgaben erfüllen können. In der DS-GVO heißt es ergänzend, dass jede Entscheidung, mit der die Datenschutzbehörden Korrekturbefugnisse ausüben, Gegenstand einer Beschwerde vor den nationalen Gerichten sein kann.[6] Daher können sich Unternehmen nicht hinter der Tatsache verstecken, dass eine nationale Behörde über ungenügende Ressourcen bzw. Verfahrensmaßnahmen verfügt. Dies zeigt exemplarisch das kürzlich ergangene Urteil des belgischen Gerichtshofs, mit dem Facebook eine Geldbuße in Höhe von 100 Millionen € auferlegt wurde.[7]

Für grenzüberschreitende Fälle, in denen mehrere Datenschutzbehörden beteiligt sind und widersprüchliche Auffassungen oder gar Streitigkeiten zwischen den Datenschutzbehörden bestehen, ist der Europäische Datenschutzausschuss (im Folgenden „EDPB“), der die Artikel-29-Datenschutzgruppe ersetzt, befugt verbindliche Entscheidungen zur Durchsetzung einer einheitlichen Anwendung der DS-GVO zu treffen.[8] Um eine zeitnahe Beilegung von Streitigkeiten zu gewährleisten, wird ein harmonisiertes IT-System[9] eingerichtet (wie anlässlich des „Computer Privacy and Data Protection (CPDP)“-Kongresses 2018 kommuniziert),.[10]

Abgesehen von seinen verbindlichen Entscheidungsprozessen wird der EDPB in der Lage sein, Stellungnahmen abzugeben und Leitlinien zu erstellen.[11] Dies folgt dem Vorgehen der früheren Artikel-29-Datenschutzgruppe, die eine Schlüsselrolle bei der Vorbereitung der Anwendung der DS-GVO durch die Veröffentlichung von Leitlinien gespielt hat. Diese Leitlinien sind zwar unverbindlich, sie sind jedoch öffentlich zugänglich, da ihre Mitglieder am besten geeignet sind, zusätzliche Rechtssicherheit in Bezug auf die Auslegung der DS-GVO zu schaffen.

Ein weiterer wichtiger Hinweis ist der Gestaltungsraum, den die DS-GVO den EU-Mitgliedstaaten zur Verfügung stellt, um beispielsweise strengere Bestimmungen für Gesundheits- und Beschäftigungsdaten zu erlassen.[12] Bisher haben nur Deutschland und Österreich nationale Gesetze verabschiedet, während andere Mitgliedstaaten ihre lokalen Gesetze noch anpassen müssen. Es wird jedoch erwartet, dass diese Länder bis Ende Mai folgen werden.[13]

Stärkere Durchsetzungsmöglichkeiten

Ein Schlüsselelement der DS-GVO besteht darin, deren Durchsetzungsmaßnahmen zu stärken. Die Datenschutzbehörden und Gerichte der EU-Mitgliedstaaten sind nun befugt, erhebliche Durchsetzungsmaßnahmen zur Untersuchung des Verdachts des nicht-Datenschutz-konformen Verhaltens, einschließlich der Durchsuchung von Geschäftsräumen, durchzuführen und private Räumlichkeiten mit einem Haftbefehl (sogenannte Dawn Raids) durchsuchen zu lassen. Verstösse können hierbei mit bis zu 4% des weltweiten Umsatzes des vorangegangenen Geschäftsjahres geahndet werden.

Die mit der Unkenntnis der Datenschutzbestimmungen verbundenen Risiken sind nach heutigem Ermessen ernst zu nehmen. Neben möglichen Konsequenzen wie erheblichen Bußgeldern, ist auch ein höheres Reputationsrisiko zu verzeichnen. Langwierige Untersuchungen und anschliessende Rechtstreitigkeiten, einschließlich Sammelklagen, können die Reputation eines Unternehmens für einen längeren Zeitraum schädigen.

Eine stärkere Durchsetzung der Regulation, sowie aber auch die damit einghergehenden Bemühungen der Unternehmen compliant zu sein, erhöht die Vertrauenswürdigkeit und Glaubwürdigkeit von Verbrauchern und Mitarbeitern[14] und kann so eine Kundenabwanderung abwenden.

Conclusio

Angesichts der oben genannten schwerwiegenden Folgen der Nichteinhaltung empfehlen wir Unternehmen eine Datenschutzstrategie festzulegen, um kurz-, mittel- und langfristig die Einhaltung der DS-GVO sicherzustellen, und eine Datenschutz-Governance-Struktur zu schaffen sowie wenn erforderlich einen Datenschutzbeauftragten zu definieren (wer wird konsultiert und ist verantwortlich, rechenschaftspflichtig (bedingt!)) - alles auf einem risikobasierten Ansatz. Darüber hinaus sollten Unternehmen alle Prozesse identifizieren, welche die Verarbeitung personenbezogener Daten (auch «alte» Datenbestände!) betreffen, und regelmäßig überprüfen, ob die Verträge des Unternehmens mit Lieferanten und Subunternehmern der DS-GVO oder anderen relevanten Datenschutzbestimmungen entsprechen. Für alle Unternehmen ist es äußerst wichtig, ein Verständnis dafür zu entwickeln, welches Verhalten unter der DS-GVO zulässig ist und welches nicht; insbesondere dann, wenn die unternehmerischen Kerntätigkeiten darin bestehen, sensible Daten oder personenbezogene Daten in großem Umfang zu verarbeiten.

Ein praktischer Weg zur Förderung des Verständnisses von Arbeitnehmern bzgl. der DS-GVO und deren damit zusammenhängenden Pflichten besteht darin, Datenschutzschulungen und Sensibilisierungsworkshops durchzuführen und die Umsetzung von Datenschutzrichtlinien und -verfahren (Verstöße gegen persönliche Daten, Rechte von betroffenen Personen, Risikoklassifizierung, Datenschutzfolgenabschätzungen), die speziell auf dieses Unternehmen zugeschnitten sind, zu kontrollieren. Dies minimiert nicht nur das Risiko, von vornherein nicht konform zu sein, sondern dient dies auch als Beweis- und Nachweisfunktion, wenn ein Unternehmen später auf mögliches nicht-konformes Verhalten hin untersucht wird. Beweise für konforme Verarbeitung von Daten, Risikomethoden, Datenschutzrichtlinien und -verfahren können bei einem Verstoss von den behördlichen Investigationstätigkeiten als positiv berücksichtigt werden und zu einer Milderung der Geldbuße führen.

Ab dem 25. Mai 2018 ist die DS-GVO für alle Länder in ihrem territorialen Geltungsbereich anwendbar. Es ist eher naiv, ihre Umsetzung zu ignorieren, und der Ansatz sollte immer auf dem folgenden Compliance-Leitspruch abzielen:

> *Lieber an der Präventive arbeiten als an der Verfolgung, Sanktionierung und Schadensbehebung.*

Über die Autorinnen

Jutta Sonja Oberlin
CIPM, CO (Universität Augsburg), zertifizierte Datenschutzbeauftragte, Master of Compliance, studierte Rechtswissenschaften an der Universität Zürich (UZH) ist Managerin im Cyber Security Team bei der Deloitte AG in Zürich. Auch doziert sie zum Thema EU Datenschutz und BDSG an der Universität Augsburg. Ihre Expertise umfasst die Beratung von datenschutzrechtlichen Sachverhalten und Problematiken unter diversen Regulationen wie die DS-GVO und weiteren internationalen Bestimmungen.

Yasmine Deryckere
CIPP/E, LLM, ist Senior Consultant im Cyber Security Team bei der Deloitte AG in Zürich. Sie studierte Rechtswissenschaften in Belgien und berät cross industry Kunden bezüglich Datenschutz mit besonderem Augenmerk auf die Entwicklungen im europäischen Datenschutzrecht. Ihre Expertise erstreckt sich über die Interpretation der regulatorischen Vorgaben bis hin zur Prozessdefinition der technischen Umsetzungen der DS-GVO.

▶ www2.deloitte.com

Deloitte.

[5] Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, BS 10 januari 2018.

[6] Artikel 78 (3) DS-GVO.

[7] Belgian Data Protection Authority vs. Facebook, https://www.privacycommission.be/sites/privacycommission/files/documents/Facebook_vonnis_16022018_0.pdf.

[8] Artikel 68-76 DS-GVO.

[9] https://edps.europa.eu/data-protection/our-work/edps-worldwide_de

[10] CPDP Conference 2018: « The future of data protection enforcement: what to expect and how to prepare" https://www.youtube.com/watch?v=bp-CYThJsjxE&t=41955.

[11] Communication from the Commission to the European Parliament and the Council: "Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018", COM(2018) 43 final, 24 January 2018, https://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi13cSl6uvZAhWBA8AKHZsgBMYQFggs5MAE&url=https%3A%2F%2Fec.europa.eu%2Fcommission%2Fsites%2Fbeta-political%2Ffiles%2Fdata-protection-communication-com.2018.43.3_en.pdf&usg=AOvVaw0eqQzyqQYzZgSVpERH7nFn.

[12] Articles 9 (health data) and 88 (employee data) GDPR.

[13] Communication from the Commission to the European Parliament and the Council: "Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018", COM(2018) 43 final, 24 January 2018, https://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi13cSl6uvZAhWBA8AKHZsgBMYQFggs5MAE&url=https%3A%2F%2Fec.europa.eu%2Fcommission%2Fsites%2Fbeta-political%2Ffiles%2Fdata-protection-communication-com.2018.43.3_en.pdf&usg=AOvVaw0eqQzyqQYzZgSVpERH7nFn. Austria:http://www.ris.bka.gv.at/Dokumente/BglbAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf, Germany: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl1752097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl1752097.pdf%27%5D__1513091793362.

[14] Siehe den Fall Lidl, in dem die deutsche Datenschutzbehörde das Unternehmen wegen der illegalen Aufbewahrung der Gesundheitsdaten der Mitarbeiter bestraft hat.

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

START-UPS UND DS-GVO – RECHTLICHE HERAUSFORDERUNGEN UND BESONDERHEITEN

Kevin Marschall, LL.M. und Stephan Blazy, LL.M.

Die Datenschutz-Grundverordnung (DS-GVO) ist heiß diskutiert, auch bei Start-Ups. Für sie stellt sich die Frage nach dem Umgang mit der Verordnung. Dass Start-Ups generell unter die Verordnung fallen ist unkritisch. Besonders Dokumentations- und Rechenschaftspflichten, Datensicherheit, Datenschutz-Folgenabschätzung und die Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB) sind von Brisanz.

Bürokratie als Erleichterung – Notwendigkeit für Start-Ups?

Das Ziel von Dokumentationspflichten ist die Herstellung von Transparenz bei der Datenverarbeitung. Hierdurch kann die Einhaltung der Vorgaben unterstützt und diese auch gegenüber der Aufsichtsbehörde demonstriert werden. Die zentrale Vorschrift ist Art. 30 DS-GVO, wonach grundsätzlich jeder Verantwortliche ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen hat, die seiner Zuständigkeit unterliegen.

Müssen Start-Ups überhaupt dokumentieren?

Von Bedeutung ist, ob Start-Ups überhaupt dokumentieren müssen, da Art. 30 Abs. 5 DS-GVO Ausnahmen vorsieht. Diese waren ausweislich des Wortlauts ursprünglich zur Entlastung von KMU gedacht. Diese müssen nicht dokumentieren, wenn sie weniger als 250 Mitarbeiter beschäftigen. Dies dürfte auf nahezu alle Start-Ups zutreffen. Hiervon gibt es jedoch gravierende Rückausnahmen, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, wenn sie nicht nur gelegentlich erfolgt oder die Datenverarbeitung sich auf besonders schützenswerte Daten wie Gesundheitsdaten oder auf strafrechtliche Verurteilungen und Straftaten bezieht. Entscheidend ist das Geschäftsmodell und die Datenverarbeitungen sowie deren Art und Umfang. So muss ein Start-Up, das eine App im Bereich der Telemedizin anbietet, besondere Arten von Daten der Patienten verarbeiten und ist dann auch Adressat der Pflicht. Ebenso muss dokumentiert werden, wenn die Datenverarbeitung nicht nur gelegentlich erfolgt. Sofern ein Start-Ups regelmäßig Kunden- oder Mitarbeiterdaten verarbeitet, erfolgt die Verarbeitung schon regelmäßig und nicht nur gelegentlich.

Die Dokumentationspflichten sind von allen Start-Ups zu erfüllen. Diese mögen zwar besonders aus Sicht junger Unternehmen lästig erscheinen. Die Dokumentation interner Prozesse ist aber u.a. als Wettbewerbsvorteil zu begreifen. Auch schon innerhalb eines Investor-Pitchs kann ein solides Datenschutz-Konzept Investoren überzeugen, da jedes Unternehmen mit Einhaltung rechtlicher Vorgaben steht und fällt.

Was ist besonders wichtig bei der Dokumentation?

Die Inhalte der Dokumentationspflicht sind in Art. 30 Abs. 1 lit. a bis g DS-GVO festgelegt.

- Name und Kontaktdaten des Start-Ups sowie ggf. die des Datenschutzbeauftragten
- Zwecke der Verarbeitung

  → Die Zwecke müssen für alle Datenverarbeitungsprozesse gesondert festgelegt und dokumentiert werden; ein One-Size-Fits-All-Konzept („Generalzweck") ist unzureichend. Mögliche Zwecke sind beispielsweise „Vertrieb von Produkten", „Durchführung der Zahlungsverarbeitung" oder „Marketing zur Kundengewinnung"
- Beschreibung der Daten- und Betroffenenkategorien (Kategorisierungserfordernis)

  → Dies schließt Daten von Kunden, Webseitenbesuchern, Dienstleistern und Beschäftigten mit ein. Diese Kategorien sollten mit den betreffenden Datenarten verknüpft werden. Hierdurch wird auch bei Ergänzungen sichtbar, welche Daten für welche Kategorien verarbeitet werden.
- Kategorien von Empfängern der Daten

  → Hier muss gefragt werden, ob und an welche Empfänger (z.B. Dienstleister, Steuerberater etc.) übermittelt werden soll; es reicht aus, wenn diese Übermittlung nur beabsichtigt ist. Zu „Empfängern" zählen nicht die rein internen Empfänger der Daten.
- Übermittlungen der Daten in Drittländer

  → Sofern die Daten in Drittländer (außerhalb der EU) übermittelt werden sollen, was häufig bei der Nutzung von Cloud-Storage-Diensten so ist, sind auch diese und die Rechtsgrundlagen der Übermittlung zu dokumentieren.
- Fristen für die Löschung verschiedener Datenkategorien

  → Diese Angabe ist nur mitaufzunehmen, wenn es dem Start-Up überhaupt möglich ist, eine solche Löschfrist zu bestimmen. So kann schon keine Frist zur Löschung bestimmt werden, wenn der Zeitpunkt der Erreichung des Verarbeitungszwecks, wie etwa bei einem laufenden Vertragsverhältnis, unbestimmt ist.
- Allgemeine Beschreibung der Sicherheitsmaßnahmen zum Schutz der Daten

  → Hier kann im Vorfeld eine Art „Mind-Map" über die jeweiligen Prozesse detailliert ausgearbeitet und mit den betreffenden Maßnahmen versehen werden. Diese Übersicht sollte gepflegt werden und „mitwachsen".

Start-Ups im Auftragsverarbeitungs-Bereich

Auch Auftragsverarbeiter müssen diese Pflichten modifiziert mit Bezug zum Auftragsverhältnis erfüllen. So ist es verbreitet, dass Start-Ups externe Ressourcen, wie Cloud-Computing, nutzen. Andererseits können auch Start-Ups selbst als Auftragsverarbeiter, z.B. im Rahmen eines Instant-Messaging-Service, fungieren. Sie müssen dann den Verantwortlichen auch in zahlreichen Fällen – etwa bei der Evaluation von etwaigen Schutzverletzungen/Datenpannen – ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

unterstützen. Eine Vermischung beider Rollen ist ebenfalls möglich.

Datensicherheit als Grundgerüst jedes Unternehmens

Plant ein Start-Up personenbezogene Daten zu verarbeiten, muss es die Sicherheit der Daten, Systeme und Prozesse gewährleisten können. Für diesen „Dreiklang" geben Art. 5 und 32 DS-GVO den Rahmen vor. Die hiernach zu ergreifenden technischen und organisatorischen Maßnahmen haben sich an dem jeweiligen Zweck der Verarbeitung, dem Stand der Technik sowie dem Risiko der Datenverarbeitung für die Betroffen zu orientieren. Sie müssen ferner geeignet sein, um einer missbräuchlichen Verarbeitung, dem unbeabsichtigten Verlust, der Schädigung oder Zerstörung personenbezogener Daten vorzubeugen.

Maßnahmen und zu berücksichtigende Aspekte

Wie solche Maßnahmen ausgestaltet sein können, verdeutlicht der Beispielkatalog in Art 32 Abs. 1 DS-GVO. So sind ein effektives Risikomanagement für die Sicherheit der Verarbeitung ebenso entscheidend wie Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste. Auch die Pseudonymisierung und Verschlüsselung personenbezogener Daten sowie die Fähigkeit der Datenwiederherstellung müssen die ergriffenen Maßnahmen abdecken. Derartige Sicherheitsvorkehrungen sind unabhängig von Betriebsgröße, aber abhängig vom Risiko, zu ergreifen. Für junge, speziell datengetriebene Unternehmen ist allerdings der damit verbundene Kostenfaktor mitunter eine Belastung. Auch wenn gemäß Art. 32 DS-GVO die Implementierungskosten mit in die Waagschale einzubringen sind, darf nicht übersehen werden, dass Folgekosten der Implementierung unberücksichtigt bleiben. Bei der Finanzplanung sollten daher auch die Wartungskosten berücksichtigt werden. Dies kann im Extremfall auch zu einer risikosenkenden Veränderung der Datenverarbeitungsprozesse führen, da die zu implementierenden Maßnahmen mit Absenkung des Risikos abnehmen.

[1] S. auch Marschall, DuD 2015, 183 ff.

Innerbetriebliche Schutzbedarfsfeststellung

Um zu beurteilen welche Schutzmaßnahmen genau zu ergreifen sind, muss das Start-up zunächst den Schutzbedarf der Daten ermitteln. Hierfür sind zwei unterschiedliche Bewertungsfaktoren maßgeblich. Der erste Faktor bemisst sich an der Sensitivität der personenbezogenen Daten. Art. 9 und 10 DS-GVO legen etwa besondere Kategorien von Daten fest. Der zweite Faktor konturiert sich an dem Gefährdungspotenzial, das den Betroffenen aus dem jeweiligen Verarbeitungskontext erwächst. Die Maßnahmen orientieren sich daher maßgeblich an dem Risiko, das durch die Verarbeitung entsteht.

Datenpannen – Was ist zu tun?

Eine weitere Herausforderung für Start-Ups ist die Meldepflicht bei Schutzverletzungen. Schutzverletzungen sind nach Art. 4 Nr. 12 DS-GVO Vernichtung, Verlust, Veränderung, unbefugte Offenlegung und Zugang der personenbezogenen Daten. Eine Verletzung darf nicht bagatellisiert werden, sondern das Start-Up muss grundsätzlich nach Art. 33 und 34 DS-GVO die Aufsichtsbehörde und bei einem hohen Risiko auch die Betroffenen informieren, deren Daten von der Verletzung betroffen sind. Hervorzuheben ist hierbei, dass die Hürde für die Annahme einer Schutzverletzung und die Meldung an die Aufsichtsbehörde niedrig ist. Durch die Schutzverletzung muss „lediglich" ein Risiko (!) für die Rechte und Freiheiten der Betroffenen bestehen; nur bloße Unannehmlichkeiten, wie etwa die erneute Zurverfügungstellung der Adressdaten nach einem Serverabsturz (ohne vorhandenes Back-Up) – ohne Dritteinwirkung – dürfte hiervon ausgenommen sein.[1] Demnach wäre etwa auch ein nicht gesichertes Speichermedium mit personenbezogenen Daten, das unauffindbar bleibt, als meldepflichtige Schutzverletzung zu deklarieren. Gerade auch ein unbefugter Zugang oder die Offenlegung zu bzw. von Daten gegenüber Unberechtigten ist – etwa ohne zureichende Zugriffskonzepte – eine häufige Form der Schutzverletzung. Diese kann durch räumliche Open-Office-Konzepte in sog. Start-Laps/Inkubatoren noch begünstigt werden, da sich hier mehrere Start-Ups dieselben Räumen und Infrastrukturen teilen.

Zeit als wesentlicher Faktor

Da Start-Ups selten eine IT-Abteilung mit einem IT-Sicherheitsbeauftragten haben, ist ein risikoadäquater Schutz der Verarbeitung von Relevanz. Nur durch ein schnelles Handeln nach Feststellung der Schutzverletzung kann die 72h-Grenze, innerhalb derer eine (Erst-)Meldung an die Behörde erfolgen muss, eingehalten werden. Hieran zeigt sich deutlich, wie wichtig ein angemessenes Sicherheitskonzept für Start-Ups ist. Auch schon durch weniger aufwändige Schutzvorkehrungen (z.B. Verschlüsselung von Daten) können sie sich schützen.

Abschätzung der Folgen? Risiken erkennen und handeln!

Liegt in der jeweiligen Verarbeitung – z.B. beim Einsatz von personenzugehörigen Geo-Tracking-Systemen – ein hohes Risiko für die Betroffenen so ist unabhängig von der Unternehmensgröße auch eine Datenschutzfolgenabschätzung durchzuführen.

Besonderes Risiko durch neue Technologien und Geschäftsfelder

Für junge und innovative Unternehmen ist von Relevanz, dass in Art. 35 Abs. 1 DS-GVO explizit Datenverarbeitungsformen durch „neue Technologien" ein hohes Risiko zugemessen wird. Hierbei dürften sich alle Start-Ups auf dem Gebieten der technologischen Vernetzung wie dem IoT-, Autonomik- oder Big-Data-Bereich und Co. angesprochen fühlen. Im Einzelfall ist jedoch immer auf das konkrete Risiko für den Betroffenen abzustellen, welches ihm durch den Einsatz der jeweiligen Technologien widerfährt. Das Risiko konturiert sich nicht ausschließlich an der Menge oder Art der Daten, sondern besonders an dem Informationsgehalt über das Individuum, der sich aus ihrer Verarbeitung und dem Kontext ergibt. Es geht also darum, Risiken für die Betroffenen bereits während der Business- und Technikkonzeption zu erkennen und durch die Erkenntnisse der Folgenabschätzung einzudämmen. Liegt das Betätigungsfeld z.B. im Profiling, Scoring, Tracking, der (großflächigen) Überwachung öffentlicher Plätze oder in der Verarbeitung besonderer Kategorien von Daten so ist stets eine Datenschutz-Folgenabschätzung durchzuführen. Einen Überblick über die Pflicht zur Durchführung einer Folgenabschätzung bieten auch die kürzlich veröffentlichen Blacklists der Aufsichtsbehörden.[2]

Einfluss von Datenschutzgrundsätzen

Besteht eine Pflicht zum Handeln, stellt sich anschließend die Frage wie man genau zu Werke gehen soll. Als junger Unternehmer kann es nicht schaden über die wichtigsten Mindestprüfelemente im Bilde zu sein. Zentral sind hier die Grundsätze der Verarbeitung personenbezogener Daten gem. Art. 5 Abs. 1 DS-GVO wie etwa Rechtmäßigkeit der Verarbeitung oder die Speicherbegrenzung. Möchte das Unternehmen beispielsweise eine App entwickeln, so muss die Datenverarbeitung im Lichte dieser Grundsätze analysiert werden und die Grundsätze bei der Produktgestaltung beachtet werden (Privacy by Design und by Default). Wie das Risiko der Datenverarbeitung für den App-Nutzer erwächst, muss in der Folge bewertet werden können. Dem sind die ergriffenen Sicherheits- und Eindämmungsmaßnahmen gegenüberzustellen. Mit ihnen muss sich das Risiko beherrschen lassen. Allgemeingehaltene Checklisten helfen hierbei kaum, da die Verarbeitungsvorgänge und Risiken je nach internen Prozessen stark variieren.

Kommen die Gründer letztlich zu dem Schluss, dass sie die hohen Risiken nicht eindämmen können ist zudem gemäß Art. 36 DS-GVO die Aufsichtsbehörde zu konsultieren. Diese wird dann Empfehlungen aussprechen. Zur Prüfung, ob eine erneute Folgenabschätzung durchzuführen ist, etwa wenn sich substanzielle Abweichungen im Hinblick auf die Risiken für die Betroffenen ergeben, bietet sich eine synoptische Gegenüberstellung der Schnittmengen und Risiken beider Verfahren an. Haben sich die „Rahmenbedingungen" und das Risiko nicht erhöht, kann eine erneute Abschätzung unterbleiben.

Datenschutzbeauftragter – Pflicht oder Kür?

Nach der Verordnung kommt es bei der Bestellpflicht auf die von den Datenverarbeitungen ausgehenden Risiken für die Betroffenen an.[3] Hierbei muss die Kerntätigkeit der Start-Ups gerade aufgrund ihres Wesens, Umfangs ▶

[2] S. etwa für Hamburg https://datenschutz-hamburg.de/assets/pdf/Liste%20Art%2035-4%20DS-GVO%20HmbBfDI-%C3%B6ffentlicher%20Bereich_v1.0.pdf; für Schleswig-Holstein s. https://datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf; für den Bund s. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_Verarbeitungsvorgaenge.pdf?__blob=publicationFile&rv=2.

[3] S. Marschall/Müller, ZD 2016, 415 ff.

und ihrer Zwecke auf eine regelmäßige oder systematische Beobachtung von Betroffenen ausgerichtet sein. So wären beispielsweise solche Start-Ups zur Bestellung verpflichtet, die – insbesondere bei neuen Technologien – Profilbildungen, Bewertungen oder Katalogisierungen der Betroffenen vornehmen, wie etwa bei Start-Ups, die das Verhalten von Nutzern elektronischer Dienste, wie Apps, aufzeichnen, auswerten und zu kommerziell nutzbaren Ergebnissen aufbereiten. Dies gilt insbesondere dann, wenn im Rahmen der Kerntätigkeit besondere Datenarten verarbeitet werden, was im Bereich Wearable-Computing-Systems der Fall sein kann. Besteht hiernach keine Bestellpflicht für Start-Ups, so müssen diese aber auch das nationale Recht beachten. Nach § 38 BDSG-neu „gelten" die bisher bestandenen Regelungen weitgehend fort. Hiernach ist auch bei mind. 10 Personen die ständig mit der Datenverarbeitung betraut sind ein bDSB zu bestellen; ebenso, wenn eine Datenschutz-Folgenabschätzung durchzuführen ist. Start-Ups müssen im Falle einer personellen Erweiterung oder einer Ausdehnung bestehender Datenverarbeitungen aufs Neue doppelt prüfen, ob eine Bestellung verpflichtend ist.

Eine „Eigenbestellung" zum bDSB als Geschäftsführer ist aufgrund von Interessenskonflikten nicht möglich. Jedoch kann es eine Alternative sein, sich die Dienstleistung extern einzukaufen.

Checkliste

Bestandsaufnahme und Dokumentation folgender Inhalte:

- ○ Welche Verarbeitungsprozesse werden zu welchen Zwecken vorgenommen?
- ○ Welche Datenarten und welche Kategorien von Betroffenen werden im Rahmen des Geschäftsmodells grundsätzlich und prognostisch verarbeitet?
- ○ Wo liegt die Kerntätigkeit des Start-Ups? Branchenbestimmungen?
- ○ Sind das Geschäftsmodell und die Kerntätigkeit mit einem besonderen Risiko für die Betroffenen verbunden?
- ○ Welche Sicherheitsmaßnahmen müssen mindestens zur Begegnung dieser Risiken implementiert werden?
- Bezugnahme zu Schutzverletzungen als Orientierungspunkt hilfreich
- Wie hoch sind die Implementierungskosten der Maßnahmen?
- Beurteilung des Verhältnisses von Risiko und Maßnahmen – werden diese angemessen abgedeckt oder muss ich notfalls die Art und den Umfang der Datenverarbeitung anpassen/reduzieren?

Wie erhalte ich Kenntnis von Schutzverletzungen?

- ○ Wer wird in die Bewertung des Vorfalls eingebunden?
- ○ Ist Hilfe von Extern, auch von der Aufsichtsbehörde, erforderlich?
- ○ Existiert ein Kommunikations- und Handlungskonzept im Umgang mit Schutzverletzungen?

Fazit: Große Herausforderungen, aber machbar!

Die Verordnung stellt gerade Start-Ups vor große Herausforderungen. Ob sich seitens der Politik – wie derzeit diskutiert[4] – noch Erleichterungen für kleine Unternehmen ergeben, ist fraglich. Ein bDSB hilft nachhaltig, die Vorgaben angemessen umzusetzen. Insbesondere auch eine frühzeitige Zusammenarbeit mit der zuständigen Aufsichtsbehörde kann jungen Unternehmen ebenfalls helfen, sich im Bereich des (neuen) Datenschutzrechts einzufinden.

[4] https://www.golem.de/news/DS-GVO-ganz-grosse-koalition-fordert-aenderungen-beim-datenschutz-1806-134941.html.

Über die Autoren

Kevin Marschall, LL.M.

Stephan Blazy, LL.M.

sind Geschäftsführer und Gründer der GDPC GbR einer auf Datenschutz und Informationssicherheit spezialisierten Unternehmensberatung mit Sitz in Kassel. Sie beraten Unternehmen und Behörden insbesondere bei der Umsetzung der DS-GVO und fungieren auch als externe DSB.

▶ www.gdpc.de

GDPC GLOBAL DATA PROTECTION CONSULTING

Anzeige

Seminare und Lehrgänge.

Für eine gesetzeskonforme und professionelle Umsetzung von Datenschutz und Compliance.

Haben Sie auf die neue EU-DSGVO umgestellt?

Sichern Sie sich jetzt umfangreiches und aktuelles Know-how für Ihre persönliche berufliche Entwicklung.

TÜV Rheinland bietet ein breit gefächertes Portfolio an Bildungs- und Beratungsdienstleistungen auf höchstem fachlichen Niveau. Mehr als 7.500 Angebote, über 2.500 Referenten. Deutschlandweit.

Zum Thema Datenschutz bieten wir zahlreiche Seminare und modulare Lehrgänge mit der Möglichkeit, ein Zertifikat unter Einbeziehung der neuen EU-DSGVO der unabhängigen Personenzertifizierungsstelle PersCert von TÜV Rheinland zu erwerben. Auch im Bereich Compliance finden Sie bei uns eine Vielzahl praxisorientierter Qualifizierungsangebote.

Datenschutz

Alle Seminare und Lehrgänge beziehen sich selbstverständlich auf die EU-DSGVO und das neue BDSG.

- Datenschutzfachkraft.
- Datenschutzbeauftragter (TÜV).
- Datenschutzauditor (TÜV).
- Externer Datenschutzbeauftragter (TÜV).
- EU-Datenschutz-Grundverordung.
- Datenschutzbeauftragter. Update auf die EU-DSGVO.
- EU-DSGVO und Informationssicherheit. Vom ISMS zum DSMS.
- Auftragsverarbeitung nach EU-DSGVO und neuem BDSG.
- Datenschutz Update – Fortbildung für Datenschützer.
- Übersicht der Verarbeitungstätigkeiten & Datenschutz-Folgenabschätzung.
- Videoüberwachung nach DSGVO und neuem BDSG.

Weitere Details, Seminare und Anmeldung unter:
www.tuv.com/datenschutz

Compliance

- Compliance-Officer (TÜV).
- Compliance-Beauftragter: Anforderungen, Aufgaben, Risiken.
- Compliance-Organisation – erste Schritte beim Aufbau.
- Compliance-Risikoanalyse.
- Interne Untersuchungen bei Compliance-Verstößen.
- Geldwäschebeauftragter (TÜV).

Weitere Details, Seminare und Anmeldung unter:
www.tuv.com/seminare-compliance

Weitere Informationen erhalten Sie auch bei:
TÜV Rheinland Akademie GmbH
Am Grauen Stein · 51105 Köln
Sandra Fahling · Tel. 0221 806-3561
sandra.fahling@de.tuv.com

www.akademie.tuv.com

TÜVRheinland®
Genau. Richtig.

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

DS-GVO SEIT MAI 2018 AUCH FÜR SCHWEIZER UNTERNEHMER RELEVANT

Regina Mühlich

Revision des Schweizer Datenschutzgesetzes geplant

Zahlreiche Schweizer Unternehmen sind immer dann betroffen, wenn sich EU-weit etwas tut. Seit 25. Mai 2018 ist die neue Datenschutz-Grundverordnung (DS-GVO) für alle Mitgliedsstaaten der Europäischen Union gültig. Die DS-GVO regelt den einheitlichen Schutz für den Umgang mit personenbezogenen Daten in der EU. Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, müssen sich ausgehend vom Anwendungsbereich an die Regelungen der DS-GVO halten. Dies gilt für Unternehmen mit Sitz außerhalb der EU und somit auch für solche in der Schweiz – sobald sie Daten von EU-Bürgern verarbeiten oder als Auftragsverarbeiter in Vertragsbeziehungen zu EU-Unternehmen stehen.

Ausschlaggebend: Das Marktortprinzip

Gemäß Art. 3 Abs. 2 DS-GVO (Räumlicher Anwendungsbereich) findet die Verordnung Anwendung, sobald ein nicht in der Union niedergelassener Verantwortlicher oder Auftragsverarbeiter personenbezogene Daten von betroffenen Personen, die sich in der Union befinden, verarbeitet. Man spricht hier vom so genannten „Marktortprinzip". Davon betroffen sind somit unter anderem Betreiber von Online-Portalen, Versandhändler, Exporteure sowie jegliche Dienstleister, die Leistungen in der Europäischen Union anbieten und dabei personenbezogene Daten verarbeiten.

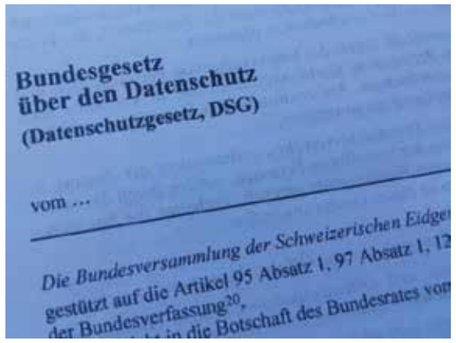
Kommt 2018: Schweizer Revision des Datenschutzgesetzes

Die Schweiz gilt als sicheres Drittland im Sinne der Datenschutzrichtlinie 95/46/EG. Nach EU-Kriterien bietet die Schweiz ein angemessenes Schutzniveau für die Übermittlung personenbezogener Daten von der EU in die Schweiz. Um auch zukünftig nach Art. 45 DS-GVO (Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses) über ein angemessenes Schutzniveau für die Übermittlung personenbezogener Daten nach EU-Kriterien zu verfügen, hat die Schweiz bereits Ende 2016 eine Revision des eigenen Datenschutzgesetzes (DSG) beschlossen. Einige Parallelen zwischen der DS-GVO und dem DSG, wie etwa im Bereich des so genannten Verzeichnisses der Bearbeitungstätigkeiten oder der Datenschutz-Folgenabschätzung, sind vorhanden. Ziel der geplanten Neuerungen ist es, das Schweizer Datenschutzniveau dem der EU anzugleichen. Diese könnte aber noch eine Weile dauern.

Die Staatspolitische Kommission des Nationalrates entschied im Januar 2018, dass die Totalrevision in zwei Teilschritten aufzuteilen sei: die notwendige Umsetzung der Schengen-Verträge und im Anschluss die Totalrevision des Datenschutzgesetzes. Die Kommission könne so der großen Komplexität der Thematik gerecht werden.

Dokumentationspflicht (Art. 19) laut Schweizer DSG heute

Bereits heute ist der Verantwortliche und der Auftragsbearbeiter laut Art. 19 DSG verpflichtet, seine Datenbearbeitungsvorgänge an das Register zu melden. Welche Angaben zukünftig dokumentiert werden müssen, sieht das DSG in seiner jetzigen Form im Gegensatz zur DS-GVO der Europäischen Union nicht vor: Die Dokumentation muss jedoch so ausgestaltet sein, dass der Verantwortliche und der Auftragsbearbeiter ihren Informations- und Meldepflichten nachkommen können. Die bis dahin übliche Meldung an das Register soll zukünftig entfallen (Ausnahme: Bundesorgane). Die Dokumentationspflicht gilt länderübergreifend als zentrales Element zur Verwirklichung einer transparenten Datenbearbeitung. So muss zum Beispiel dem Auskunftsersuchen einer betroffenen Person gem. Art. 20 VE-DSG jederzeit nachgekommen werden können. Ein Verstoß gegen die Dokumentationspflicht wird sanktioniert (Art. 51 Bst. F VE-DSG Verletzung der Sorgfaltspflichten).



Neu 2018: Verzeichnis der Bearbeitungstätigkeiten (Art. 11 im DSG Entwurf)

Damit personenbezogene Daten durch den Verantwortlichen und den Auftragsbearbeiter wirkungsvoll geschützt werden können, muss ermittelt werden, in welchen Fällen personenbezogene Daten – beispielsweise von Mitarbeitern, Bewerbern, Kunden, Lieferanten, etc. – erhoben, bearbeitet und genutzt werden. Im ersten Schritt ist dafür eine Listung aller Systeme, Tools und Verfahren, in welchen und bei denen personenbezogene Daten automatisiert und/oder nicht-automatisiert bearbeitet und gespeichert werden, zu erstellen. Die Verantwortlichen und Auftragsbearbeiter werden darüber hinaus verpflichtet, ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen.

Das Verzeichnis des Verantwortlichen muss gemäß Satz 2 mindestens nachstehende Angaben enthalten:

- Die Identität des Verantwortlichen,
- den Bearbeitungszweck,
- eine Beschreibung der Kategorien betroffener Personen und die Kategorien bearbeiteter Personendaten.
- Die Kategorien der Empfängerinnen und Empfänger,
- wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer.
- Wenn möglich eine allgemeine Beschreibung der Maßnahmen zur Gewährleistung der Datensicherheit nach Art. 7 und
- falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Art. 13.

Übersicht der Bearbeitungstätigkeiten schafft Klarheit

Wie das Verzeichnis der Bearbeitungstätigkeiten im Detail gestaltet und durchgeführt werden soll, dazu liefert der vorliegende Gesetzesentwurf keine konkreten Vorgaben. Im Rahmen der Dokumentationspflichten sind jedoch entsprechende Informationen vorzuhalten, um zum Beispiel im Fall des Auskunftsersuchens der betroffenen Person den Informationenpflichten nachkommen zu können. Des Weiteren ist der Verantwortliche verpflichtet, die betroffene Person zu informieren, wenn die Bearbeitung einem Auftragsbearbeiter übertragen wird. In diesem Zug muss der Verantwortliche der betroffenen Person ebenso die Daten oder Kategorien von Daten mitteilen, die bearbeitet werden. Darüber hinaus stiftet eine Übersicht der Bearbeitungstätigkeiten im Hinblick auf die Einhaltung des Datenschutzes vielfachen Nutzen. So werden Datenflüsse im Unternehmen ermittelt und definiert. Die Übersicht dient darüber hinaus als Grundlage für die Erfüllung der Betroffenenrechte (Art. 20), für die Erstellung des Lösch- und Aufbewahrungskonzepts (Art. 17) oder ebenso als Informationsgeber für die Meldung von Verletzungen des Datenschutzes (Art. 17). Außerdem verlangt das Marktortprinzip aus der DS-GVO zwingend nach einer Erstellung des Verzeichnisses der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO (Accountability) für einen nicht in der Union niedergelassenen Verantwortlichen.

Wenn ein Auftrag aus der EU einen Schweizer Auftragsverarbeiter trifft…

Im Rahmen einer Auftragsverarbeitung mit einem EU-Auftraggeber (Controller) hat der Schweizer Auftragnehmer (Prozessor) ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO zu führen. In dieser Übersicht sind alle durchgeführten Tätigkeiten der Verarbeitungen im Auftrag eines Verantwortlichen (Controller) zu dokumentieren. Der Auftragnehmer hat zusätzlich auch im notwendigen Umfang bei der Erstellung des Verarbeitungsverzeichnisses mitzuwirken und den Auftraggeber dabei zu unterstützen. Spätestens auf Anfrage beziehungsweise im Rahmen von Kontrollen durch den Auftraggeber ist diese Dokumentation vorzulegen.

Wahrscheinlich gibt es vor der Verabschiedung des neuen Schweizer Datenschutzgesetzes noch die eine oder andere Anpassung. Für Schweizer Unternehmen mit Geschäftsbeziehungen in die EU empfiehlt es sich – unabhängig von der zentralen Bedeutung innerhalb der beiden Gesetze – mit der geforderten Dokumentation zu beginnen. Ein Unternehmen, das sich an die Datenschutz-Grundverordnung hält, kann auch in der Schweiz beruhigt sein. Die DS-GVO sollte ausreichend sein, um auch die persönliche Integrität eines Schweizer Bürgers zu schützen.

Über die Autorin

Regina Mühlich
Geschäftsführerin der
AdOrga Solutions GmbH

Datenschutzbeauftragte, Datenschutz-Auditorin, Qualitätsmanagementbeauftragte, ISO 27001 Vorstandsmitglied BvD e. V.
Autorin u. a. „Datenschutz 2018“ Forum Verlag Herkert GmbH

▶ www.AdOrgaSolutions.de

Anzeige

Wichtiges Datenschutzwissen für Ihre Kollegen

Mitarbeiterinformation zum Datenschutz

BvD-Rabatt 30%

TKMmed!a

Kommen Sie Ihrer Verpflichtung zum Datenschutz nach und schulen Sie Ihre Mitarbeiter mit der kompakten Infobroschüre. Jetzt auch in englischer Sprache!

Profitieren Sie von unseren BVD-Staffelpreisen:

→ Einzelpreis für BVD-Mitglieder	6,98 €/Stk.
→ 10-50 Stk. für BVD-Mitglieder	4,87 €/Stk.
→ 51-100 Stk. für BVD-Mitglieder	4,13 €/Stk.
→ 101-500 Stk. für BVD-Mitglieder	2,17 €/Stk.

INDIVIDUALISIEREN

Sie Ihre Infobroschüre mit Ihrem eigenen Firmenlogo und den Kontaktdaten des Datenschutzbeauftragten! Bestellen Sie Ihre individualisierte Broschüre einfach per Mail: mib@datenschutz-aktuell.de

Jetzt **HIER** bestellen – exklusiv mit BVD-Rabatt:
www.datenschutz-aktuell.de/mib-bvd/

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

ERLAUBNISTATBESTAND DER VERTRAGSDURCHFÜHRUNG – AUCH DRITTE PROFITIEREN.

Dr. Carlo Piltz

Einleitung

Der Erlaubnistatbestand der Vertragsdurchführung (Art. 6 Abs. 1 lit. b) DS-GVO) ist, neben der Interessenabwägung, für Unternehmen oft das Mittel der Wahl, wenn es um die Legitimation der Verarbeitung personenbezogener Daten geht. Jedoch wurde in der Literatur bisher kaum eine praxisrelevante Alternative des Erlaubnistatbestandes nach Art. 6 Abs. 1 lit. b) DS-GVO näher diskutiert. Per se würde man davon ausgehen, dass diese Norm sich stets nur auf das direkte Vertragsverhältnis zwischen dem Betroffenen und dem Verantwortlichen bezieht. Dabei erlaubt die Vorschrift auch außerhalb dieses Sachverhalts liegende Verarbeitungen durch Dritte. Es geht um eine Verarbeitung, die zwar zur Durchführung eines Vertrags erforderlich ist, jedoch von einem Verantwortlichen unternommen wird, der gerade nicht Vertragspartner des Betroffenen ist. In dem nachfolgenden Beitrag soll diese Alternative des Erlaubnistatbestandes der Vertragsdurchführung näher beleuchtet werden.

Erlaubnistatbestand des Art. 6 Abs. 1 lit. b) DS-GVO

Nach Art. 6 Abs. 1 lit. b) DS-GVO ist die Verarbeitung rechtmäßig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Zwar erwähnt die DS-GVO nur die „Erfüllung“ des Vertrages. Jedoch wird allgemein davon ausgegangen, dass hiervon nicht etwa nur der konkrete Leistungsaustausch, sondern auch vertragliche Änderungen oder auch die Abwicklung des Vertrages umfasst sind.[1] Nach dem eindeutigen Wortlaut der Norm muss der Betroffene Vertragspartei sein. Jedoch ergibt sich aus dem Gesetz nicht die Anforderung, dass der ▶

[1] Schulz, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 6 Rn. 27; Buchner/Petri, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 6 Rn. 33.

Betroffene die einzige Vertragspartei sein muss. Umfasst sind daher potentiell auch mehrseitige Verträge.

Vertragspartner des Betroffenen

Art. 6 Abs. 1 lit. b) DS-GVO schweigt komplett dazu, wer Vertragspartner des Betroffenen sein muss. So verlangt das Gesetz nicht, dass nur der Verantwortliche und der Betroffene Parteien des Vertrages sein müssen. Das Vertragsverhältnis muss nicht zwischen dem Verantwortlichen (der Daten verarbeitet) und dem Betroffenen bestehen.[2] Es muss sicherlich einen Vertragspartner des Betroffenen geben. Der Vertragspartner des Betroffenen und der die Daten verarbeitende Verantwortliche müssen aber nicht personenidentisch sein.[3]

Auch ErwG 44 DS-GVO stellt keine anderen Anforderungen an die Eigenschaft von Verantwortlichen als Vertragspartner des Betroffenen. Nach ErwG 44 DS-GVO sollte die Verarbeitung von Daten als rechtmäßig gelten, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist. Es werden keine weiteren Ausführungen zu den beteiligten Verantwortlichen und deren vertragliche Stellung gegenüber dem Betroffenen gemacht. Daher spricht auch die recht allgemeine Vorgabe des ErwG 44 DS-GVO dafür, dass auch solche Verantwortliche personenbezogene Daten auf der Grundlage von Art. 6 Abs. 1 lit. b) DS-GVO verarbeiten dürfen, die nicht Vertragspartner des Betroffenen sind.

Dafür, dass auch sonstige Dritte den Erlaubnistatbestand des Art. 6 Abs. 1 lit. b) DS-GVO für sich nutzbar machen können, spricht auch, dass der Gesetzgeber der DS-GVO an anderer Stelle sehr wohl ausdrücklich vorsieht, dass der Verantwortliche und der Betroffene einen Vertrag abgeschlossen haben müssen. Nach Art. 22 Abs. 2 lit. a) DSVGO ist Art. 22 Abs. 1 DS-GVO und damit das Verbot der automatisierten Entscheidung mit erheblichen Konsequenzen für den Betroffenen dann nicht anwendbar, wenn die Entscheidung „für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist". Hier verlangt der Gesetzgeber ausdrücklich, dass der datenverarbeitende Verantwortliche Vertragspartner der betroffenen Person ist. Diese Voraussetzung wird in Art. 6 Abs. 1 lit. b) DS-GVO nicht aufgestellt und, mit Blick auf Art. 22 Abs. 2 DS-GVO, ist davon auszugehen, dass dies bewusst geschah.

Erforderlichkeit

Natürlich muss die jeweilige Datenverarbeitung für die Erfüllung des Vertrages erforderlich sein. Dies ist dann der Fall, wenn sie zur Erfüllung von Pflichten oder zur Wahrnehmung von Rechten aus einem mit dem Betroffenen geschlossenen Vertrag vorgenommen und hierfür benötigt wird.[4] Es muss ein unmittelbarer Zusammenhang mit dem konkreten Zweck des Vertragsverhältnisses bestehen.[5] Erforderlichkeit bedeutet aber nicht „absolut zwingende Notwendigkeit", wonach nur solche Verarbeitungen zulässig wären, ohne die die Durchführung des Vertragsverhältnisses nicht möglich wäre.[6] Auch hier ist jedoch zu beachten, dass das Merkmal der „Erforderlichkeit" nicht an den Status als Vertragspartner eines bestimmten Verantwortlichen anknüpft. Der Betroffene muss auf jeden Fall Vertragspartner sein. Auf der anderen Vertragsseite können aber durchaus mehrere, getrennt voneinander agierende Verantwortliche ein Interesse daran haben, eine Verarbeitung durchzuführen, um den Vertrag des Betroffenen erfüllen zu können, obwohl sie nicht selbst Vertragspartner sind. So kann etwa der eingeschaltete Spediteur Adressdaten des Betroffenen (als Käufer) erhalten und diese Daten verarbeiten, um dem Betroffenen das von ihm bestellte Produkt nach Hause zu liefern.[7]

Was konkret für die Durchführung des Vertrages erforderlich ist, ergibt sich stets aus dem Inhalt des jeweiligen Vertrages. Umfasst ist in jedem Fall die Erfüllung sowohl von Primär- als auch Sekundärpflichten.[8] Die Verarbeitung ist jedenfalls immer dann erforderlich, wenn der Vertrag ohne sie nicht so erfüllt werden könnte, wie die Parteien sich geeinigt haben.

Für die hier beschriebenen Konstellationen ist zu beachten, dass der dritte Verantwortliche die Erforderlichkeit seiner Verarbeitung an dem Zweck eines Vertrages auszurichten hat, dessen Vertragspartei er gerade nicht ist, sondern sein eigener Vertragspartner (z.B. sein Auftraggeber). Art. 6 Abs. 1 lit. b) DS-GVO kann also als Erlaubnistatbestand entlang vertraglicher Ketten dienen. Freilich nur, soweit als verbindendes Kettenglied stets die Erforderlichkeit der Durchführung des Vertrages mit dem Betroffenen dient.

Zusätzliche Anforderung an die Einschaltung Dritter?

Zum Teil wird verlangt, dass, soweit der Verantwortliche nicht selbst an dem Vertrag beteiligt ist, der Vertragspartner ihn zumindest in die Vertragsanbahnung oder -durchführung eingeschaltet haben muss („Funktionsübertragung"), damit die Verarbeitung gerechtfertigt ist.[9] Aus dem Gesetz ergibt sich diese Anforderung nicht. In der Praxis wird sie aber wohl stets erfüllt sein, wenn eine Verarbeitung des Dritten auf Art. 6 Abs. 1 lit. b) DS-GVO gestützt werden soll. Denn die Einschaltung des Dritten, etwa des oben erwähnten Spediteurs, wird im Rahmen der Vertragsdurchführung erfolgen.

Zusätzliche, also über die in Art. 6 Abs. 1 lit. b) DS-GVO definierten, Anforderungen sind nicht zu erfüllen. Auch der dritte Verantwortliche, der nicht Vertragspartei ist, muss als Verantwortlicher die Voraussetzungen des Erlaubnistatbestandes erfüllen.

Praxisbeispiele

In der Praxis wird eine Verarbeitung auf der Grundlage des Art. 6 Abs. 1 lit. b) DS-GVO überall dort in Betracht kommen, wo der Dritte gerade nicht als Auftragsverarbeiter agiert.[10] Wenn also kein Auftrag zur Verarbeitung personenbezogener Daten vorliegt, sondern eine Weitergabe von Daten für die Durchführung einer bestimmten Tätigkeit einen notwendigen Annex, aber gerade nicht Hauptgegenstand eines Auftrages darstellt. Wann eine Auftragsverarbeitung vorliegt, wird in der Praxis freilich stets von den konkreten Umständen (etwa auch der Weisungsgebundenheit) abhängen. So kann man im Rahmen der Weitergabe von personenbezogenen Daten für Reparaturen (Erfüllung von Gewährleistungsansprüchen aus dem Vertrag), die Bearbeitung von Reklamation, die bereits erwähnte Lieferung durch Speditionen oder auch Weitergabe von Daten an einen Rechtsanwalt zur Geltendmachung von Vertragsansprüchen die Datenverarbeitung durch diese Dritte auf der Grundlage von Art. 6 Abs. 1 lit. b) DS-GVO begründen. Ebenfalls umfasst kann die Weitergabe von Daten im Konzern an Tochter- oder Schwestergesellschaften sein, so z. B. bei dem Betrieb eines konzernweiten CRM-Systems, in dem alle vertragsrelevanten Daten von Kunden vorgehalten und für die Vertragsdurchführung genutzt werden. Dem Grunde nach lassen sich hier all jene Fälle erfassen, in denen der Vertragspartner des Betroffenen, im Rahmen seiner vertraglichen Pflichten, Dienste Dritter in Anspruch nimmt.

Schluss

Es zeigt sich, dass die Einschaltung anderer Parteien in der Praxis nicht nur ein Fall der Auftragsverarbeitung sein muss, sondern vielfach eine Weitergabe von Daten an einen eigenständig verantwortlichen Dritten darstellt, der sich für die Legitimation seiner Datenverarbeitungen auf den Vertrag des Betroffenen mit einem anderen Verantwortlichen stützen kann. Die gesetzlichen Anforderungen sind hierbei nicht höher, als jene, die für den direkten Vertragspartner zu beachten sind. Bisher führt diese Variante des Erlaubnistatbestandes der Vertragsdurchführung aber eher noch ein Schattendasein.

Über den Autor

Dr. Carlo Piltz
Rechtsanwalt, Reusch Rechtsanwaltsgesellschaft mbH, Berlin
Teamleader Cyber Security & Datenschutz
Zertifizierter Datenschutzbeauftragter (TÜV®)
Certified Information Privacy Professional/Europe (CIPP/E)

▶ www.reuschlaw.de

reuschlaw
Legal Consultants

[2] Wolff, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 550.
[3] Albers/Veit, in: BeckOK Datenschutzrecht, Stand: 1.5.2018, Art. 6 Rn. 30.
[4] Schulz, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 6 Rn. 36.
[5] Schulz, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 6 Rn. 36; Albers/Veit, in: BeckOK Datenschutzrecht, Stand: 1.5.2018, Art. 6 Rn. 32.
[6] Schulz, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 6 Rn. 36; Buchner/Petri, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 6 Rn. 45.
[7] Beispiel nach Wolff, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 550.
[8] Reimer, in: Sydow, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 6 Rn. 20; Wolff, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 560.
[9] Reimer, in: Sydow, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 6 Rn. 18.
[10] Denn nach h. M. gilt auch unter der DS-GVO die bekannte „Privilegierung" des Einsatzes von Auftragsverarbeitern und die Weitergabe von Daten an diese erfordert keinen Erlaubnistatbestand, vgl. hierzu Gola, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 4 Rn. 57 f. mwN.

TRANSPARENZ ALS STRUKTUR-ENTSCHEIDUNG

Maria Wilhelm

Die praktische Umsetzung der Datenpannenmeldung und Informationspflichten der Datenschutz-Grundverordnung (DS-GVO)

Die seit dem 25. Mai 2018 geltende Datenschutz-Grundverordnung stellt neue Herausforderungen an personenbezogene Daten verarbeitende Stellen, indem sie eine Strukturentscheidung für eine transparente Verarbeitung personenbezogener Daten trifft. Viele Themenbereiche der Verordnung wurden im Rahmen der Umsetzung kontrovers diskutiert, doch kaum ein Thema beherrschte die Diskussion derart nachhaltig, wie die Reichweite der Transparenzpflichten. In Verbindung mit der in Art. 5 Absatz 2 DS-GVO festgelegten Rechenschaftspflicht zwingen die Transparenzanforderungen der Verordnung nicht nur zur Umsetzung einzelner Pflichten, sie setzen vielmehr datenschutzkonforme Organisationsstrukturen und Prozesse und somit ein funktionstüchtiges Datenschutz-Management voraus. Wie dies von verantwortlichen Stellen zu leisten ist und welche Hilfestellungen von den europäischen Aufsichtsbehörden geleistet werden, soll Gegenstand dieser Darstellung sein.

I. Orientierungshilfen der Aufsichtsbehörden

Neben dem Wortlaut der Verordnung selbst lohnt sich der Blick in die auf europäischer Ebene abgestimmten Orientierungshilfen. Bereits zu der Zeit in der die Artikel-29-Datenschutzgruppe noch das entscheidende Fachgremium auf europäischer Ebene war wurden von den europäischen Aufsichtsbehörden für die vorliegend dargestellte Problematik zwei maßgebliche Guidelines erlassen, die vom Europäischen Datenschutzausschuss nach dessen Errichtung am 25. Mai 2018 bestätigt wurden.[1] Für den Bereich der Datenpannenmeldungen der Art. 33 und 34 DS-GVO geben die " Guidelines on Personal data breach notification under Regulation 2016/679 (WP250)" und für den Bereich der allgemeinen Informationspflichten der Art. 13 und 14 DS-GVO geben die "Guidelines on transparency under Regulation 2016/679 (WP260)" Orientierung. Beide Dokumente sind unter anderem auf Internetseiten von nationalen Aufsichtsbehörden zugänglich.[2] Diese Handreichungen geben auch zur praktischen Umsetzung der Verordnung wertvolle Informationen und werden durch die nationalen DSK-Kurzpapiere und individuelle Leitfäden der Aufsichtsbehörden ergänzt.

II. Die Datenpannenmeldung (Art. 33, 34 DS-GVO) als Prozess

Ist die notwendige Informationsbasis bezüglich des grundlegenden Systems der Datenschutz-Grundverordnung bei der verantwortlichen Stelle vorhanden, so können davon ausgehend in strukturierter und organisierter Weise auch die Transparenzpflichten erfüllt werden.

1. Meldung von Datenpannen an die Aufsichtsbehörde (Art. 33 DS-GVO)

Die Meldung von Datenpannen an die Aufsichtsbehörde nach Art. 33 DS-GVO und die Meldung von Datenpannen an die betroffenen Personen nach Art. 34 DS-GVO sollten hierbei als Prozesse betrachtet werden, die als solche in die Organisationsstruktur integriert und implementiert werden müssen. Dies gilt umso mehr als die grundsätzliche Frist zur Meldung von Datenpannen an die Aufsichtsbehörde nach Art. 33 DS-GVO nur 72 Stunden ab Bekanntwerden des Vorfalls beträgt. Liegt innerhalb dieser Frist das Wochenende, so kann es entscheidend darauf ankommen, ob vorab geklärt wurde, wer wann und an wen welche Berichtswege einhalten muss und welche Person innerhalb der Stelle die gesetzlich vorgeschriebene Risikoprüfung und schließlich die tatsächliche Meldung an die Aufsichtsbehörde vornimmt. Innerhalb dieser 72-stündigen Frist ist im Rahmen einer negativen Risikoprognose zu prüfen, ob die eingetretene Datenpanne „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt". Für die Durchführung der Risikoprüfung können andere bereits für die verantwortliche Stelle eingerichtete Risikoprüfungsprozesse fruchtbar gemacht werden. Die europäischen Guidelines weisen jedoch explizit auf die Unterschiede zu der Risikoprüfung im Hinblick auf die Prüfung von Datenpannen und der Risikoprüfung im Rahmen von Prozessen zur Datenschutz-Folgenabschätzung hin.[3] Orientierung können daher auch die bezüglich der Datenschutz-Folgenabschätzung abgestimmten Papiere geben.[4] Hat eine Stelle bereits einen solchen belastbaren Prüfprozess eingerichtet, so kann sie diesen ebenfalls für die Risikoprüfung bezüglich der Datenpannenmeldung nutzen. Hierbei ist nicht jede Datenpanne an die Aufsichtsbehörde zu melden. Die europäische Guideline gibt diesbezüglich in einer Tabelle Praxisbeispiele an die Hand und stellt dar, ob in einzelnen Fällen Meldungen an die Aufsichtsbehörde und/oder die betroffene Person erfolgen müssen. Im Fall des Diebstahls eines nach dem Stand der Technik verschlüsselten Datenträgers ist, wenn die personenbezogenen Daten noch an anderer Stelle im System (Backup) der verantwortlichen Stelle vorhanden sind, nach dem Europäischen Datenschutzausschuss weder eine Meldung an die Aufsichtsbehörde noch an die betroffene Person erforderlich.[5]

2. Meldepflicht gegenüber den betroffenen Personen

Art. 34 DS-GVO setzt hinsichtlich der Meldepflicht höhere Anforderungen als Art. 33 DS-GVO. An den Betroffenen muss nur eine Meldung erfolgen, wenn voraussichtlich ein "*hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen*" anzunehmen ist. Die beiden Meldepflichten stehen zueinander somit in einem Stufenverhältnis.

3. Faktoren innerhalb der Risikoprüfung

Sowohl im Rahmen der negativen Risikoprognose nach Art. 33 DS-GVO als auch nach der positiven Risikoprognose sind jedoch dieselben Faktoren zu berücksichtigen. Hierunter fallen spezifische Umstände des Falles (Wahrscheinlichkeit des Risikoeintritts, Schwere der Verletzung, Potentielle Auswirkungen etc.), die Art der Verletzung sowie die Natur, Sensibilität und Menge der betroffenen Daten. Zudem sind der Identifizierungsaufwand bezüglich einzelner Personen, die Schwere der Konsequenzen für Personen, der spezieller Charakter der betroffenen Personen, die Anzahl der betroffenen Personen wie auch die Natur und Rolle des Verantwortlichen innerhalb der Prüfung zu berücksichtigen.[6] Gerade für kleine Einheiten kann es sinnvoll sein, das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO als Arbeitsgrundlage um die für die Risikoprüfung relevanten Punkte zu erweitern und die Risikoprüfung von dieser Basis ausgehend zu erfüllen.

III. Informationspflichten (Art. 13, 14 DS-GVO) – strukturiertes Herangehen ist entscheidend

Eine weitere strukturelle und organisatorische Herausforderung stellt die Erfüllung der ▸

[1] Siehe die Auflistung aller am 25. Mai 2018 bestätigten Dokumente ei Edpb, Endorsement 1/2018, p. 1, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf <21.06.2018>.

[2] Siehe unter anderem https://www.baden-wuerttemberg.datenschutz.de/ds-gvo/ <21.06.2018>; https://www.lda.bayern.de/de/datenschutz_eu.html <21.06.2018>; https://datenschutz-hamburg.de/pages/art-29-working-papers/ <21.06.2018>.

[3] Article 29 Working Party, Personal data breach notification Guidelines on Personal data breach notification under Regulation 2016/679 (WP250), p.23.

[4] Siehe auf europäischer Ebene Article 29 Working Party, Data protection impact assessment Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248); siehe auf deutscher Ebene DSK, Kurzpapier Nr. 5, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO; es existieren ebenfalls weitere lesenswerte konkretisierende Handreichungen einzelner Aufsichtsbehörden, vgl. etwa https://www.cnil.fr/en/media <21.06.2018>.

[5] Article 29 Working Party, Personal data breach notification Guidelines on Personal data breach notification under Regulation 2016/679 (WP250), p. 31.

[6] Article 29 Working Party, Personal data breach notification Guidelines on Personal data breach notification under Regulation 2016/679 (WP250), p.23-26; siehe ebenfalls zur Risikoprüfung DSK, Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen.

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Informationspflichten der Art. 13 und 14 DS-GVO dar. Hierbei können Synergieeffekte genutzt werden. Viele der in diesen Vorschriften aufgezählten obligatorischen Informationsgehalte finden sich auch in den inhaltlichen Anforderungen an das Verzeichnis aus Art. 30 DS-GVO. Es ist daher sinnvoll, die eigenen Informationserklärungen aus dem Verzeichnis gemäß Art. 30 DS-GVO zu entwickeln. Es gibt jedoch nicht eine allgemeine alle Verarbeitungsprozesse der jeweiligen Stelle abdeckende Informationserklärung. Deshalb empfiehlt sich das Bilden von Anwendungsfällen, sogenannten "use cases". Solche Szenarien können beispielweise die Durchführung eines Bewerbungs- oder Einstellungsverfahrens oder auch der Vertragsschluss und die Vertragsabwicklung in der Kundenbeziehung sein. Für jeden dieser Anwendungsfälle gilt es eine standardisierte Informationserklärung zu entwickeln, wie sie Art. 13 DS-GVO für die Datenerhebung bei der betroffenen Person und Art. 14 DS-GVO für die Erhebung an anderer Stelle vorschreibt. Durch ein solches strukturiertes und effektives Vorgehen kann der zu investierende Arbeitsaufwand in einem vertretbaren und angemessenen Maß gehalten werden.

1. Informationen bei geschäftlichen Kontaktlisten

Aufgrund des allgemeinen Ansatzes der Verordnung gibt es mehrere Fälle, in denen die Umsetzbarkeit im Einzelfall diskutiert wurde. Gerade die oft in Unternehmen vorgehaltenen Geschäftskontakte oder Zuliefererlisten erfordern aufgrund ihrer teilweisen eine Vielzahl an Personen umfassenden Größe die Einrichtung standardisierter Informationsprozesse. Es kann daher sinnvoll sein, für Nachrichten an Kontakte, die in diesen Listen verarbeitet werden, vorgefertigte Vorlagen zu verwenden. So kann eine E-Mail-Vorlage erstellt werden, die unterhalb der Signatur die notwendigen Hinweise enthält. Gleichermaßen kann ein einheitliches Briefpapier mit datenschutzrechtlichen Hinweisen erstellt werden. In einem weiteren Schritt müssen die Mitarbeiter angewiesen werden für die Erstellung von Nachrichten an Kontakte aus diesen Listen die gefertigten Vorlagen zu verwenden. Entsprechendes kann beispielsweise in einem Mitarbeiterhandbuch festgehalten werden.

2. Die Internetseite als „Schnittstelle" mit der Außenwelt

Da die Internetseite des Verantwortlichen die Schnittstelle nach außen darstellt, wurden auch diesbezügliche Datenschutzhinweise diskutiert. Neben dem nicht erfüllten Auskunftsbegehren sind diese Datenschutzhinweise einer der zentralen Punkte, an dem ein nicht existentes Datenschutzmanagement der Außenwelt offenbar wird. Umso wichtiger ist es, auch diese Herausforderung anzugehen. Aufgrund des verspäteten Erlasses der ePrivacy-Verordnung, bezüglich der die Stellungnahme des Rates der Europäischen Union noch aussteht,[7] sind auch im Telemedienbereich vorrangig die Grundsätze der Datenschutz-Grundverordnung heranzuziehen.[8] In diesem Kontext ist von Bedeutung, dass über die Einbindung von Cookies in die jeweilige Seite informiert wird, auch wenn diese Cookies von Drittanbietern stammen. Ebenso ist über die Einbindung von Analytikprogrammen zu informieren. Je nach konkreter Ausgestaltung der Verarbeitungsprozesse besteht im Einzelfall weiterer Informationsbedarf, so beispielsweise im Fall der Weitergabe von personenbezogenen Daten zu Werbezwecken. Im Bereich der Social-Media-Plugins wäre es unter anderem wichtig, dass diese sicher in die Internetseite eingebunden sind. Dies kann durch die sogenannte „Doppel-Klick-Lösung" geleistet werden. Die Frage nach der Befugnis oder auch Rechtsgrundlage der Datenverarbeitung ist hierbei grundsätzlich separat von der Frage der Erfüllung der Transparenzanforderungen zu beurteilen. Eine transparente Datenverarbeitung alleine führt folglich nicht zu einem automatischen Vorliegen der notwendigen rechtlichen Befugnis.

Seit dem 25. Mai 2018 finden sich im Internet zahlreiche Datenschutzerklärungen und auch die Aufsichtsbehörden stellen entsprechende Informationen zur Verfügung, an denen man sich orientieren kann. Dennoch muss jeweils im Einzelfall geprüft werden, welche Verarbeitungen konkret durchgeführt werden und welche Komponenten genau in der Datenschutzerklärung enthalten sein müssen.

[7] Vgl. zum aktuellen Stand der Verhandlungen die Synopse des BayLDA, Synopse der ePrivacy-VO; abrufbar unter: https://www.lda.bayern.de/media/eprivacy_synopse.pdf <21.06.2018>.

[8] DSK, Positionsbestimmung vom 26. April 2018, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, S. 2; abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Positionsbestimmung-TMG.pdf <21.06.2018>.

III. Ausblick

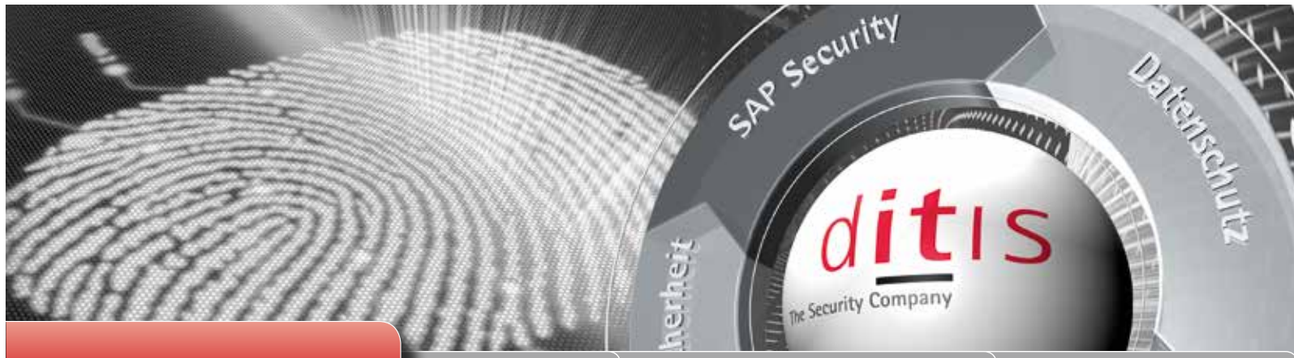
Mit der kontinuierlichen Anwendung der Datenschutz-Grundverordnung und der in diesem Rahmen ergehenden Entscheidungen wird zunehmend mehr Rechtssicherheit in diesem Bereich erzeugt werden. Auch die Abstimmungsarbeiten zwischen den Aufsichtsbehörden werden sowohl auf europäischer Ebene über den Europäischen Datenschutzausschuss und dessen Arbeitsgruppen als auch über die Arbeitskreise der deutschen Datenschutzkonferenz fortgesetzt werden. Sobald es in diesem Bereich weitere Ergebnisse gibt, werden die deutschen Aufsichtsbehörden darüber informieren. Auf diese Weise kann die neue Strukturentscheidung hinsichtlich der Verantwortlichkeiten im datenschutzrechtlichen System zielführend realisiert werden. Hierdurch werden Betroffene befähigt, ihre Rechtspositionen selbstbestimmt und aktiv durchzusetzen.

Über die Autorin

Maria Wilhelm
Stuttgart, Landesbeauftragter für den Datenschutz und die Informationsfreiheit, Referentin der Stabsstelle Europa

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Anzeige



DATENSCHUTZ | SAP SECURITY | INFORMATIONSSICHERHEIT | IT-SECURITY

Datenschutz-Manager

Das Datenschutzmanagementsystem für den DSB – EU ready

EU ready

> Sofort einsetzbares System um den Überblick im Datenschutz zu behalten und Risiken effektiv zu erkennen und zu behandeln
> Inhaltlich ausgearbeitete Struktur, ausgerichtet an gesetzlichen Vorgaben und internationalen Normen
> Verzeichnis von Verarbeitungstätigkeiten mit mehr als 220 beispielhaften Verarbeitungen inkl. dokumentiertem Schutzbedarf und anpassbaren Templates
> Logbuch zum einfachen und übersichtlichen Verwalten sowie nachhaltigem Dokumentieren der DS-Aufgaben, wie Anfragen, Prüfungen, Schulungen, Datenpannen, offenen Punkten, Terminen und Generieren von Tätigkeitsberichten
> Web-basierte Kollaborationsplattform zur Integration in Ihre Systemumgebung, optimiert für Microsoft SharePoint

JETZT AUCH IN ENGLISCH

BvD e.V. EuroPriSe Experts

ditis Systeme – Niederlassung der JMV GmbH & Co. KG Heidenheim • ein Unternehmen des Voith Konzerns
Lise-Meitner-Straße 15 • 89081 Ulm • Tel +49 731 509704 - 40 • E-Mail info@ditis.de • www.ditis.de

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

DIE ISO 27018 IM LICHTE DER DS-GVO

Stefan Staub

Ein wesentlicher Aspekt der DS-GVO und damit eine Neuheit im Datenschutzrecht ist der risikobasierte Ansatz. Dies und Art. 42 DS-GVO schlagen damit den Bogen zu Normen, die schon in der Vergangenheit das Risiko als zentrales Element behandelt haben. Insbesondere die Normenreihe der ISO-27000 Familie beschäftigt sich mit Risikomanagement im Umgang mit Informationen und schlägt ihrerseits den Bogen zum Datenschutz. Ein Mitglied dieser Normenfamilie soll hier kurz betrachtet werden.

Einleitung

Dem geneigten Leser ist sicher bereits Art. 42 DS-GVO ins Auge gefallen und – wer sich noch an die Zeit des BDSG erinnert – auch diese Rechtsnorm hatte den hehren Versuch gestartet ein Datenschutzaudit auf den Weg zu bringen (§9a BDSG-alt). Selbst Historiker werden keine antiken Reste eines solchen Datenschutzaudits vorfinden. Der Gesetzgeber hatte stets Wichtigeres zu regeln, als ein solches Gesetz zu erlassen.

Nun versucht es der europäische Normengeber ein erneutes Mal und bindet mehrere Parteien ein, um das Vorhaben auf den Weg zu bringen. Harren wir der Dinge, die da kommen werden…

Die ISO 27018

Bis zu diesem Zeitpunkt müssen wir jedoch nicht in Bewegungslosigkeit verfallen. Das internationale Gremium für Standards hat uns zumindest mit der ISO 27001 eine Norm an die Hand gegeben, mit der sich sehr gut und nicht nur behelfsmäßig auch der Datenschutz managen lässt. Für ein Teilgebiet – nämlich das Anbieten von öffentlichen Cloudlösungen im Bereich der Auftragsverarbeitung – bietet die ISO 27018 einen veritablen Ansatz eine zertifizierte Dienstleistung am Markt etablieren zu können.

Die DIN ISO/IEC 27018:2017-08 ist sozusagen eine Spezialnorm zur ISO 27002 und bietet konkrete Anforderungen zu technischen und organisatorischen Maßnahmen beim Betreiben eines ISMS nach ISO 27001. Damit eignet sich die DIN ISO/IEC 27018:2017-08 nicht für eine alleinige Umsetzung und kann nicht als alleinige Grundlage für eine Zertifizierung herangezogen werden. Sie beschreibt vielmehr sinnvolle und notwendige Maßnahmen im Kontext einer öffentlichen Cloudlösung als Auftragsverarbeitung. Die Norm ist analog den anderen ISO27xxx Normen aufgebaut und integriert sich die ISO 29100 (privacy framework).[1] Ebenso wie die Mutternorm ISO 27001 ist sie aufgeteilt in einen sog. Kapitelteil mit einer Einteilung von Maßnahmenkategorien und einem normativen Anhang, welcher die erweiterten Maßnahmen des Anbieters zum Datenschutz beschreibt.

Im ersten Teil der Norm werden insbesondere die Organisation der Informationssicherheit, diverse Kategorien von Sicherheit aber auch die datenschutzspezifischen Themen wie Lieferantenbeziehungen und Informationssicherheitsvorfälle (siehe dazu Art. 33 und Art. 34 DS-GVO) und BCM-Maßnahmen beschrieben (siehe Art 32 lit b) und c) DS-GVO). Dieser Teil dient also zunächst der Spezifizierung der Informationssicherheit beim Angebot einer öffentlichen Cloudlösung.

Der eigentliche datenschutzspezifische Teil wird im Anhang A abgebildet. Hierbei werden typische Pflichten eines Auftragsverarbeiters aufgezeigt und geregelt, ebenso wie die allgemeinen Prinzipien der Verarbeitung personenbezogener Daten wie Zweckbindung, Datenvermeidung und -sparsamkeit, Transparenz, Betroffenenrechte und Verantwortlichkeiten.

Kritische Betrachtung

Für den Datenschutzprofi wird die Norm keine neuen Erkenntnisse bieten und bei kritischer Betrachtung kann man sich des Eindrucks nicht erwehren, dass der Aufbau der Norm weder dem alten Datenschutzrecht und seiner Systematik noch dem Neuen folgt. Ob dies in der praktischen Umsetzung eine Relevanz entfaltet, kann sich erst im konkreten Umgang mit der Norm zeigen. Das Hauptwerk muss weiterhin die ISO 27001 bleiben. Darauf sei ein Augenmerk gelenkt, wenn Marktteilnehmer mit Aussagen wie „zertifiziert nach ISO 27018“ werben. Es kann nur nach ISO 27001 in Verbindung mit ISO 27018 auditiert und zertifiziert werden.

Ein weiterer Kritikpunkt - und dieser „ziert“ alle Normen - ist die Aktualität gegenüber gesetzgeberischen Aktivitäten. Es ergibt sich durch die komplexe internationale Zusammenarbeit, dass nur in größeren Abständen eine Neufassung verabschiedet werden kann. Im Zweifel schmälert dies auch die Aussagekraft eines veröffentlichten Zertifikats.

Bleibt die Lücke für andere Dienstleistungen, die unter den Art. 28 DS-GVO fallen. Hier muss man die Entwicklung weiterhin abwarten.

Aus meiner Sicht würde sich eine europäische und damit kleinere Lösung für die Zertifizierung nach Art. 42 DS-GVO anbieten. Eine solche Norm und das darüberliegende Regelwerk für Akkreditierung und Zertifizierung wären dann DS-GVO-konform, einheitlich in Europa und zumindest im Vergleich zu einer globalen Lösung schlagkräftiger und flexibler. Ob ein nationaler Alleingang dagegen zielführend ist, wage ich zu bezweifeln. M.E. wäre dies wieder der Weg zurück in mittelalterliche Kleinstaaterei.

Über den Autor

Stefan Staub
ist Mitbegründer und Geschäftsführer der Verimax GmbH. Zu seinen fachlichen Kernkompetenzen zählen der Datenschutz im Konzern, internationaler Datenschutz und die Implementierung von ISMS und BCM. Darüber hinaus berät er Geschäftsführungen und Vorstände zum Thema strategischer Datenschutz und Information Risk Management.

▶ www.verimax.de

[1] Hier sei auf die entsprechenden Seiten im Internet, z.B. beuth.de, hingewiesen.

Anzeige

- Interne & externe Datenschutzbeauftragte -

Sie suchen eine Haftpflicht-Versicherung? Sie möchten Ihre bestehende Police vergleichen?

Berufs-Haftpflichtversicherung für interne und externe DSB – in Zusammenarbeit mit dem BvD entwickelt

Als Berater schützen Sie Unternehmen vor Haftungsansprüchen - wir schützen Sie.

- exclusives Wording für BvD-Mitglieder (auf Berufsbild DSB zugeschnitten)
- Tätigkeit ‚Auditor für Datenschutz‘ beitragsfrei eingeschlossen
- niedrige Einsteigerprämie sowie professionelle Beratung

- inkl. DS-GVO
- hohe Deckungssummen zu verbesserten Konditionen

Für nähere Informationen rufen Sie uns gerne an: 06174 - 96843-0 oder unter www.bvdnet.de (Mitgliederbereich)

Butz - Versicherungsmakler GmbH Ansprechpartner: Herr Jared Butz Tel: 06174 - 96843-0 Fax: 06174 - 96843-29
info@butz-versicherungsmakler.de www.butz-versicherungsmakler.de

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN UNTER DER DS-GVO: HERANGEHENSWEISE UND AUSLEGUNGEN DER GESETZESTERMINOLOGIE IN BEZUG AUF DIE DATENSICHERHEIT

Jutta Sonja Oberlin und Gianni Crameri

I. Einleitung

Seit dem 25. Mai 2018 ist die DS-GVO mit all ihrer Wirkung in Kraft getreten. Unternehmen, welche unter die Anwendbarkeit fallen, mussten sich schon seit 2016 und müssen sich auch in Zukunft, mit den juristischen, sowie aber auch technischen Anforderungen der Regulation auseinandersetzen.

Hier reicht es nun nicht mehr, sich «nur» auf die juristische Komponente des Gesetzes zu verlassen sondern müssen die Gesetzesanwender stets die juristische, sowie auch die technische Komponente berücksichtigen. Dies bedeutet, dass Juristen, welche im Datenschutz arbeiten, sich immer mehr als Schnittstelle zwischen Gesetz und IT zu sehen haben. Sie interpretieren das Gesetz und können die Interpretation bestenfalls direkt in die Unternehmenspraxis umsetzen.

1. Bedeutung technischer und organisatorischer Maßnahmen in der DS-GVO

Datenschutzrechliche Sachverhalte verknüpfen immer häufiger rechtliche Aspekte mit den dazugehörigen IT-Aspekten.

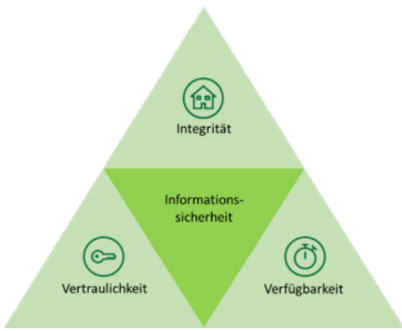
Der Hintergrund ist, dass Unternehmen bei Verstössen gegen Datensicherheitsbestimmungen mit bis zu 2% ihres globalen Jahresumsatzes bestraft werden können[1]. Dennoch besteht nur geringer Anlass zur Sorge, denn technische Präventionsmittel stehen bereits in den Startlöchern, welche auch den gesetzlichen Anforderungen standhalten können.

Zudem gibt es weitere technische Instrumente aus der juristischen «Zauberkiste», mit denen man unter Umständen eine gänzliche „Nichtanwendung" der Verordnung erwirken könnte. Hierbei ist es aber dringlichst zu empfehlen, dass die Rechtsanwender das Gesetz nicht so weit auslegen und im vernünftigen Masse die Risikoabschätzung abwägen.

Unter bestimmten Voraussetzungen, wie beispielsweise die Anwendung neuer Technologien, welche voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben[2], verlangt die die DS-GVO von Unternehmen eine Risikobeurteilung gemäß Art. 25 Abs. 1 DS-GVO, welche noch vor der Implementierung neuer digitaler Datenverabeitungsmethoden umgesetzt werden muss. Eine solche Risikobeurteilung, vom Gesetzgeber auch als «Privacy by Design» bezeichnet, sollte entsprechend gründlich, in Form eines Assessmentprotokolls, dokumentiert werden. Dies stellt somit einen formellen Teil eines Sicherheitskonzeptes dar.[3] Das Gesetz definiert hierbei keine expliziten Mindestanforderungen, so dass der Rechtsanwender im Sinne des Verhältnismässigkeitsprinzips den Begriff der Angemessenheit für sich auslegen muss. Diese Auslegung darf stets im Rahmen des risikobasierten Ansatzes geschehen, bei welchem Klassifizierung der Daten, die Verwendung bestimmter Technologien, die Risiken für das Datensubjekt, Umstände und Zwecke der Verarbeitung eine Rolle spielen.

Die Datensicherheit ist vor allem durch die technischen und organisatorischen Maßnahmen bestimmt, welche vom Verantwortlichen gemäss Art. 24 DS-GVO zu implementieren, kontrollieren und nachzuweisen sind.

Grundsätzlich ist Datensicherheit[4] unter gesonderten Prinzipien sicherzustellen. Diese Prinzipien beziehen sich auf die technischen Maßnahmen, welche im besten Fall den folgenden drei Schlüsselattributen entsprechen: Vertraulichkeit, Integrität und Verfügbarkeit.



Prinzipien der Informationssicherheit[5]

Wie in der Abbildung zu sehen ist, sind die Maßnahmen der Informationssicherheit nur dann effektiv, wenn diese komplett, mit den drei Schlüsselattributen, in den verschiedenen Sicherheitsmechanismen integriert werden. Sicherheitsmechanismen bzw. konkrete Maßnahmen können einerseits physische Kontrollen sein, wie z.B. Schlösser, Überwachungskameras, organisatorische Maßnahmen, wie die Meldung eines Verstosses und Training, oder technischen Maßnahmen, wie Firewalls, Antivirus Software und Access Logs.[6]

Im Gesetz[7] werden zudem die auslegungsbedürftigen Mindestmaßnahmen genannt, welche ein angemessenes Schutzniveau bieten sollen. Zu beachten ist hier, dass diese Mindestmaßnahmen aus Art. 32 DS-GVO nicht konkretisiert sind und vor allem nicht den technischen Standard bzw. Grad der einzelnen Maßnahme aufzeigen. So gibt es beispielsweise verschiedene Verschlüsselungstechniken, welche sodann auf ihre Angemessenheit hin beurteilt und implementiert werden müssen.

Im Folgenden der Maßnahmenkatalog aus Art. 32 DS-GVO:

- Pseudonymisierung und Verschlüsslung personenbezogener Daten;
- Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Datenverarbeitungssystemen und -diensten[8];
- Fähigkeit zur Wiederherstellung von personenbezogen Daten bei physischen oder technischen Zwischenfällen in kurzer Zeit;
- Überwachungs- und Kontrollmaßnahmen mit dem Ziel die Wirksamkeit ergriffener Maßnahmen regelmäßig zu evaluieren[9].

Je nach Risikoeinschätzung und Evaluation der Angemessenheitsfrage kann hier von „state of the art technical and organisatorial measures" gesprochen werden. ▶

[1] Vgl. WYBITUL TIM, EU-Datenschutz-Grundverordnung in der Praxis – Was ändert sich durch das neue Datenschutzrecht, S. 19. Andere Datenschutzverletzungen können auch mit bis zu 4% des globales Jahresumsatzes bestraft werden.

[2] Siehe dazu Art. 35 DS-GVO.

[3] Vgl. LEPPERHOFF NIELS, Mehr gesetzliche Pflichten für IT-Verantwortliche – Konsequenzen aus der neuen EU-Datenschutz-Grundverordnung, S.46.

[4] Engl: Information Security.

[5] In Anlehnung an … https://www.researchgate.net/file.PostFileLoader.html?id=583b21fe96b7e4163460a1f5&assetKey=AS%3A433099327709184%401480270334665.

[6] Vgl. SWIRE PETER/AHMAD KENESA, Foundations of Information Privacy and Data Protection, S. 77.

[7] Art. 32 Abs. 1 DS-GVO

[8] Vgl. Art. 32 Abs. 2 DS-GVO.

[9] Vgl. GOLA PETER, DS-GVO – Datenschutz-Grundverordnung VO (EU) 2016/679, S. 131.

„State of the art"[10] bedeutet in diesem Fall, dass jeweils die fortschrittlichsten technischen Maßnahmen getroffen werden, um die Datensicherheit zu gewährleisten. Dabei kann es sich um die fortschrittlichsten Verschlüsselungstechniken, Zugriffs- und Zugangskontrollen, Firewalls usw. handeln.

Die Norm EN45030 definiert den „Stand der Technik" wie folgt[11]:

> *„Stand der Technik: Entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, soweit Produkte, Prozesse und Dienstleistungen betroffen sind, basierend auf entsprechenden gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung."*

2. Wichtige Maßnahmen zur Sicherstellung notwendiger Datensicherheit

Die wichtigsten Maßnahmen zur Datensicherheit sind die Pseudonymisierung, Verschlüsselung und Anonymisierung. Diese werden im Folgenden näher erläutert:

Die Verschlüsselung und Anonymisierung von Daten sind wichtige Techniken, um verschiedenste Anforderungen der DS-GVO umzusetzen. Eine dieser Anforderungen ist in den Grundsätzen für die Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 lit. f DS-GVO zu finden, welcher besagt, dass Daten nur in der Weise verarbeitet werden dürfen, wenn eine angemessene Sicherheit personenbezogener Daten, sowie der Schutz vor unbefugter und unrechtmässiger Verarbeitung durch geeignete technische und organisatorische Maßnahmen gewährleistet wird. Als solche angemessene technische Sicherheit kann beispielsweise eine „state of the art"-Verschlüsselungsmethode verstanden werden, welche Daten vor unrechtmässiger Verarbeitung schützen soll.

Das Verarbeiten von Daten unter der DS-GVO, umfasst nach Art. 4 Ziff. 2 sämtliche Vorgänge, mit oder ohne Hilfe automatisierter Verfahren, welche im Zusammenhang stehen mit dem Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Verbreiten, Bereitstellen, Abgleichen, Verknüpfen, Einschränken oder aber auch das Löschen und Vernichten.

2.1 Pseudonymisierung

Gemäß Art. 4 Ziff. 5 DS-GVO umschreibt das „Pseudonymisieren" Verarbeitungsvorgäng von personenbezogenen Daten in einer solchen Weise, dass diese nicht mehr einem bestimmten Datensubjekt (d.h. einer spezifischen betroffenen Person) zugeordnet werden können, ohne dass zusätzliche Informationen bereitgestellt werden. Letztere werden bei dieser Technik gesondert gespeichert und aufbewahrt. Sie unterliegen besonderen technischen, sowie organisatorischen Maßnahmen, um eine Zuordnung der personenbezogenen Daten natürlicher Personen zu vermeiden. Im Gegensatz zu «Anonymisierung» werden Daten nicht absolut und unwiderruflich «unkenntlich» gemacht, sondern vielmehr so entkoppelt, dass eine Zuordnung zu einer natürlichen Person – ohne weitere Angaben - nicht möglich ist.

Verarbeitungsvorgänge im Sinne der Pseudonymisierung beinhalten Segregationskennungen (z. B. Name, Foto, E-Mail-Adresse, Telefonnummer) und andere Daten (z. B. Kontostand, Kreditwürdigkeit). Die Identifizierung beispielsweise von Kontoinhabern ist nur mit einer sogenannten «Mapping»-Tabelle möglich, mit der Pseudonyme ihren entsprechenden Werten zugeordnet werden können.

Dies bedeutet, dass es sich bei der Pseudonymisierung um eine reversible Datenschutztechnik handelt.

Pseudonyme können beispielsweise durch einen Zufallszahlengenerator erzeugt werden.

Trotz der Umschreibung in Art. 4 Ziff. 5 DS-GVO besteht eine gewisse Unsicherheit, ob pseudonymisierte Daten als anonymisiert oder doch als personenbezogen gelten. Hierzu bestehen unterschiedliche Auslegungsansätze. Nach dem bisher noch theoretischen, **relativen Auslegungsansatz**[13], können pseudonymisierte Daten nicht mehr als personenbezogene Daten betrachtet werden, jedoch auch nicht als anonymisierte Daten. Dies ist laut der Artikel-29-Arbeitsgruppe ein „häufiger Fehler"[14], welcher bei der Beschreibung solcher Techniken auftritt. Im Gegensatz dazu bilden die Aussagen und Stellungnahmen des EU-Gesetzgebers sodann den **absoluten Auslegungsansatz**. Dieser besagt, dass pseudonymisierte Daten stets personenbezogene Daten sind. Erwägungsgrund 26 DS-GVO statuiert zugleich, dass, wenn es auch nur schon theoretisch möglich sei Daten einer natürlichen Person zuzuordnen[15], diese als Informationen über eine identifizierbare natürliche Person angesehen werden müssen.[16] Nach diesem absoluten Ansatz gemäß Art. 6 Abs. 4 lit. e DS-GVO ist die Pseudonymisierung nur eine geeignete Schutzmaßnahme und keine Möglichkeit die Anwendbarkeit des Gesetzes zu umgehen.

Pseudonymisierte Daten, welche nicht mehr einer identifizierten oder identifizierbaren natürlichen Person zugerechnet werden können, minimieren „nur" das Risiko für die betroffenen Personen und helfen den Verantwortlichen und Datenverarbeitern einschlägige Datenschutzbestimmungen zu erfüllen.

Um pseudonymisierte Daten, welche in ihrer Urform offensichtliche personenbezogene Daten waren, in einer gesetzeskonformen Weise in einer «Cloud» zu speichern, dürfen dem Cloud-Provider diese Daten nicht in der Urform vorliegen, denn dann hätte dieser die Möglichkeit die Daten zu lesen oder aber auch die Pseudonymisierung umzukehren und somit auf personenbezogene oder gar spezielle Kategorien von Daten zuzugreifen.

2.2 Datenverschlüsselung (Data Encryption)

Neben der Pseudonymisierung existieren weitere reversible Datenverarbeitungsverfahren – mit anderen Worten Datenverschlüsselungsverfahren - mit denen sensible oder personenbezogene Daten in nicht-personenbezogene Daten umgewandelt werden können.

Möglich ist auch, dass das Pseudonym das Ergebnis der Verschlüsselung darstellt, welches durch Anwendung eines kryptographischen Algorithmus entsteht. Die Identifikatoren, welche es zur Verschlüsselung benötigt, können mit Hilfe eines geheimen Entschlüsselungskeys («decryption keys») generiert werden. Verschlüsselte personenbezogene Daten sind eine technische Möglichkeit, um nicht-autorisierten Personen den Zugriff auf personenbezogene Daten zu verwehren. Ziel ist es, dass nur eine berechtigte Person in der Lage ist, die beispielsweise in der Cloud gespeicherten Daten zu entschlüsseln. Diese Datenverarbeitungstechnik scheint eine der vielversprechenden Lösungen zu sein, um einen angemessenen Datenschutz insbesondere in Cloud-Computing-Umgebungen zu gewährleisten. Wenn ein Verantwortlicher die Daten vor dem Hochladen in einer Cloud verschlüsselt, werden die Daten aus der Sicht des Verantwortlichen als personenbezogene Daten angezeigt (sozusagen in der Urform), da dieser den decryption key besitzt.[17]

Um personenbezogene oder sensible Daten über Datenverschlüsselung sicherheits-konform in eine Cloud zu übertragen, ist es wichtig, dass nur der Datenverantwortliche den geheimen decryption key[18] besitzt. Ohne diesen kann der Datenverarbeiter[19] die Daten nicht ohne weiteres lesen. Stets muss auch der Fall eines «Trouble Shootings» bedacht werden. Unter Umständen erfordert ein Trouble Shooting den Zugriff des Auftragsverarbeiters (beispielsweise eines Cloud Providers) auf die Klardaten, um feststellen zu können in welchem Ausmaß oder ob überhaupt Daten beschädigt sind. In einem solchen Fall muss der Cloud Provider Zugriff auf die Daten des Verantwortlichen bekommen, um Daten zu reparieren oder auf Richtigkeit einzusehen. Hier würde „state of the art" bedeuten, dass der Auftragsverarbeiter nicht ohne weiteres, auch nicht im Falle eines Trouble Shootings, auf die Daten des Verantwortlichen zugreifen kann. Der Prozess des Datenzugriffes sollte für beide Parteien einen mehrstufigen Authentifizierungsprozess darstellen, welcher nach mehreren positiven Bestätigungen und autorisierten Zugangsberechtigungen, dem Auftragsverarbeiter der decryption key bereitgestellt wird. Dieser muss sodann nur für die Zeit des Trouble Shootings dem Auftragsverarbeiter übertragen werden und nach dem Trouble Shooting neu codiert werden.

Beispielsweise bietet die Microsoft Custom Lockbox eine vollständige Kontrolle des Verantwortlichen über die eigenen, in der Cloud gehosteten, Daten. Diese Lockbox ermöglicht eine nahezu komplette Vermeidung von Interaktionen zwischen Microsoft Mitarbeitern und Daten des Verantwortlichen. Microsoft bezeichnet dies als „Zero-Steady-Access". Dies bedeutet, dass kein Microsoft Mitarbeiter einen ständigen Zugriff auf die Daten in der Cloud hat. ▶

[10] „Stand der Technik"

[11] LEPPERHOFF NIELS, Das IT-Sicherheitskonzept in der DS-GVO, S. 16.

[12] Vgl. SPINDLER GERALD/SCHMECHEL PHILIPP, Personal Data and Encryption in the European General Data Protection Regulation, S. 3.

[14] Siehe hierzu: Art.-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, 0829/14/DE, WP216, S. 26:

„Annahme, dass ein pseudonymisierter Datenbestand anonymisiert ist: Häufig gehen für die Verarbeitung Verantwortliche davon aus, dass die Entfernung oder Ersetzung von einem oder mehreren Merkmalen ausreicht, um einen Datenbestand zu anonymisieren. Zahlreiche Beispiele belegen, dass dies nicht der Fall ist. Die einfache Änderung der ID verhindert nicht, dass Angreifer eine betroffene Person identifizieren, wenn der Datenbestand nach wie vor Quasi-Identifikatoren enthält oder die Werte anderer Merkmale noch immer geeignet sind, eine Person zu identifizieren. In vielen Fällen kann eine Person in einem pseudonymisierten Datenbestand ebenso einfach identifiziert werden wie im ursprünglichen Datenbestand. Es sollten zusätzliche Schritte unternommen werden, bevor ein Datenbestand als anonymisiert betrachtet wird, wie beispielsweise die Entfernung und Generalisierung von Merkmalen, die Löschung der Originaldaten oder zumindest eine starke Aggregation der Daten."

[15] Bzw. diese zuordbar machen zu können.

[16] Erwägungsgrund 28 Satz 1 DS-GVO.

[17] Vgl. HON KUAN/KOSTA ELENI/MILLARD CHRISTOPHER/STEFANATOU DIMITRA, Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation, S. 10.

[18] Falls Dritte in der Lage sind, Daten zu entschlüsseln, nicht aber der Verantwortliche, besteht Uneinigkeit darüber, ob die DS-GVO für diesen Verantwortlichen anwendbar ist.

[19] Z.B. Cloud Anbieter.

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Falls ein Microsoft Mitarbeiter nun doch für den Fall eines Trouble Shootings Zugang zu den Daten benötigt, ist hier ein mehrstufiger Akkreditierungs- und Sicherheitsprozess vorgesehen, bei welchem sowohl ein verantwortlicher Mitarbeiter von Microsoft, als auch explizit der Kunde[20] zustimmen müssen. Der Kunde, der auch gleichzeitig Datenverantwortlicher ist, kann diese Anfrage jederzeit ablehnen. Falls jedoch Zugang gewährt wird, ist dieser zeitlich limitiert - „Just-in-time access".

In der DS-GVO wird der Begriff "Verschlüsselung" selbst nicht definiert, aber dennoch von mehrere Bestimmungen wie ein Schutzinstrument gegen Datenschutzverstösse angesehen

> *„... für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schliessen unter anderem folgendes ein: (a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten ..."*[21].

Gemäss Art. 34 Abs. 3 lit. a DS-GVO betreffend der Umsetzung von „geeignete technische und organisatorische Massnahmen" ist die Benachrichtigung der Datensubjekte, welche von einer Verletzung des Schutzes personenbezogener Daten betroffen sind, gemäß Abs. 1 der Norm[22] nicht erforderlich, wenn die folgende Bedingung erfüllt ist:

> *"der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere auf solche, durch die personenbezogene Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung."*

Conclusio:

Wir schliessen daraus, dass im Falle eines Verstoßes mit entsprechender Verschlüsselung die Benachrichtigung an die betroffene Person wegen einer Verletzung der persönlichen Daten, nicht erforderlich ist.

3. Rechtmässigkeit der Datenverarbeitung

Die Rechtmässigkeit der Datenverarbeitung ist vornehmlich der Hauptgrund für den Einsatz von Verschlüsselungetechniken, insbesondere wenn die Organisation personenbezogene Daten verarbeiten muss, ohne die Bestimmungen von Art. 6 Abs. 1 lit. a bis f DS-GVO zu erfüllen.[23] Gemäss Art. 6 Abs. 4 lit. e DS-GVO ist eine rechtmässige Datenverarbeitung möglich, indem

> *„[...] geeignete Schutzmechanismen verwendet werden, die Verschlüsselung oder Pseudonymisierung umfassen können."*

Die Verarbeitung spezieller Kategorien von Daten gemäss Art. 9 Abs. 1 DS-GVO wird nicht in einem äquivalenten Artikel wie Art. 6 Abs. 4 lit. e DS-GVO aufgearbeitet.

Gemäß der **absoluten juristischen Auslegungsmethode**[24] ist die rechtmäßige Verarbeitung spezieller Kategorien von Daten nicht möglich unter der Verwendung „geeigneter technischer und organisatorischer Maßnahmen" – beispielsweise Verschlüsselung. Der **relative Ansatz** würde es jedoch ermöglichen, sensible Daten in der Cloud zu speichern, wenn die Verschlüsselung auf höchstem technischen Niveau «state-of-the-art» vorhanden ist.

Der relative Ansatz verlangt hinsichtlich der Verschlüsselungsmethode und der daraus resultierenden Ergebnisse, dass der Verschlüsselungsgrad[25], d.h. die Art der Verschlüsselung, ausreichend berücksichtigt wird. Der Verschlüsselungsgrad muss auf dem neuesten Stand der Technik[26] sein, damit das Risiko eines Datenschutzverstoßes bzgl. einer unbefugten Verarbeitung als äußerst unwahrscheinlich zu qualifizieren ist. Eine absolute Sicherheit gibt es dabei aber nie.

Das Sicherheitsniveau wird insbesondere durch folgende Parameter determiniert:

1. Die Stärke des Verschlüsselungsalgorithmus;
2. Die Länge des Verschlüsselungskeys («encryption keys»)[27];
3. Die Sicherheit des Schlüsselverwaltungsprozesses.

Gemäß diesem relativen Auslegungsansatz gelten „state of the art" verschlüsselte Daten den anonymisierten Daten als äquivalent. Folglich gelten die Datenschutzbestimmungen der DS-GVO nicht als anwendbar, sofern es unwahrscheinlich ist, dass der Datensatz von einer Person entschlüsselt wird, die nicht den decryption key besitzt.

Für die praktische Umsetzung der neuen Anforderungen stellt sich vor diesem Hintergrund die Frage, welcher Verschlüsselungsgrad gewählt werden muss, um die Anwendbarkeit der DS-GVO zu vermeiden. Hier gilt es sich frühzeitig mit den verschiedentlichen Möglichkeiten vertraut zu machen und gegebenenfalls externe Beratung einzuholen.

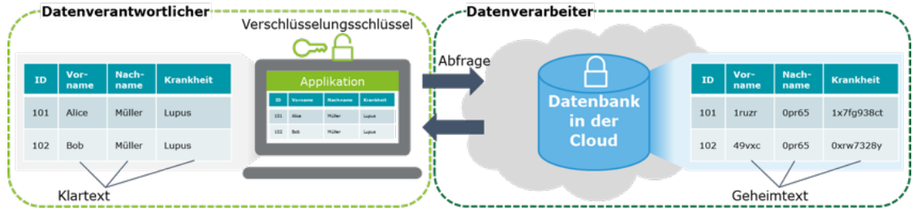
4. "State of the Art" Verschlüsselung

Moderne Verschlüsselungstechnologien ermöglichen heutzutage ohne größeren Aufwand eine Verschlüsselung auf Applikationsebene. Das bedeutet, dass Daten nur dann in ihrer Urform dargestellt werden, wenn sie auch tatsächlich in diesem Format benötigt werden. Ansonsten liegen dem Auftragsverarbeiter die Daten nur verschlüsselt vor. Auf diese Weise wird eine Trennung zwischen dem Datenverantwortlichen und dem Auftragsverarbeiter hergestellt. Am besten lässt sich die Funktionswiese einer modernen Verschlüsselungstechnologie anhand der nachstehenden Darstellung erklären.

mationen von Personen mit dem Nachnamen Müller zu suchen. Die Suchabfrage beginnt, indem die Applikation den Suchbegriff «Müller» mit Hilfe des Verschlüsselungskeys verschlüsselt. Der verschlüsselte Suchbegriff wird nun über das (öffentliche) Internet zur Datenbank des Drittanbieters geschickt. Die Datenbank wird nach dem Suchbegriff abgesucht. Falls die Suche erfolgreich war, übermittelt die Datenbank über das öffentliche Internet vier Datenfelder (ID, Vorname, Nachname und Krankheit) an die Applikation zurück. Im vorliegenden Beispiel werden jedoch nur die Datenfelder «Vorname», «Nachname» und «Krankheit» verschlüsselt übermittelt, während das Datenfeld «ID» weiterhin unverschlüsselt versendet wird. Sobald die Daten nun die Applikationsebene erreichen, werden sie mit Hilfe des decryption keys entschlüsselt und dem Benutzer, hier dem Auftragsverarbeiter, in der Urform angezeigt.

Der große Vorteil dieses Verfahren ist, dass die Daten sowohl während der Übertragung als auch während der Speicherung in der Datenbank stets verschlüsselt und nicht im Klartext einsehbar sind. Daher kann nur der Datenverantwortliche die Daten im Klartext sehen, nicht jedoch der Datenverarbeiter. Der Verschlüsselungskey bleibt während des ganzen Prozesses im Besitz des Datenverantwortlichen, wodurch die Sicherheit des Schlüsselverwaltungsprozesses gewährleistet ist.

Beim Betrachten der Darstellung fällt auf, dass



Funktionsweise einer modernen Verschlüsselungstechnologie

Die Darstellung beschreibt eine Suchabfrage an eine Cloud-Datenbank, welche von einer Drittpartei gehostet ist (z.B. Cloudprovider). Die Anfrage erfolgt mithilfe einer Applikation, welche unter der Kontrolle des Datenverantwortlichen steht. In diesem Beispiel verwendet die Anwenderin die Applikation, um nach Krankheitsinfor-

der Geheimtext in der Spalte «Nachname» sowohl für Alice wie auch Bob gleich ist (hier «0pr65»). Der Geheimtext in der Spalte «Krankheit» ist für Alice und Bob jedoch unterschiedlich, obwohl beide Im Klartext den Eintrag «Lupus» haben. Diese unterschiedliche Darstellung zeigt zwei verschiedene Verschlüsselungsarten ▸

[20] Verantwortliche.

[21] Art. 32 Abs. 1 lit. a DS-GVO.

[22] Vgl. Art. 34 Abs. 1 DS-GVO „(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung."

[23] 1. Zustimmungserklärung 2. Vertragserfüllung 3. Gesetzliche Verpflichtungen 4. Schutz lebenswichtiger Interessen 5. Allgemeines Interesse 6. Berechtigtes Interesse.

[24] Auch absoluter Auslegungsansatz genannt.

[25] Sicherheitsstufe.

[26] Z.B. AES256.

[27] Als Referenz hierzu: CAHSOR GUIDO/SORGE CHRISTOPH, in: BORGES GEORG/ MEENTS GEERT, Cloud Computing, gibt an, dass die Verwendung der 128-Bit-Schlüssellängen der AES-Verschlüsselung einen solchen Angriff nahezu unmöglich machen würde und daher unwahrscheinlich ist.

auf: die deterministische Verschlüsselung und die zufällige Verschlüsselung. Die deterministische Verschlüsselung (verwendet für den Dateneintrag «Nachname») generiert immer denselben Geheimtext für jeden angegebenen Klartext. Bei der zufälligen Verschlüsselung wird hingegen stets ein anderer Geheimtext generiert, auch wenn der Klartext derselbe ist (hier der Eintrag «Müller»). Die zufällige Verschlüsselung bietet eine höhere Sicherheit, ist jedoch mit Nachteilen wie bspw. fehlenden Such- oder Gruppierungsmöglichkeiten verbunden.

"State of the Art" Verschlüsselungstechnologien unterstützen normalerweise die aktuellen Verschlüsselungsalgorithmen wie zum Beispiel AES128 und AES256. AES steht für Advanced Encryption Standard. Die nachfolgende Zahl gibt Aufschluss über die Länge des Verschlüsselungskeys, in diesem Beispiel 128 bit bzw. 256 bit (1 Bit entspricht einer Ziffer von entweder «1» oder «0»; 128 Bit Algorithmen setzen sich veteris paribus aus einer Folge von 128 1-ern und 0-ern zusammen). Beide Verschlüsselungsalgorithmen sind in den USA zugelassen, um staatliche Dokumente der zweithöchsten (AES128) und höchsten (AES256) Geheimhaltungsstufe zu verschlüsseln.

Falls jemand versucht den Verschlüsselungskey von Daten, welche mit Hilfe von AES256 Verschlüsselungstechniken verschlüsselt wurden, zu «knacken», bspw. mit Hilfe einer sogenannten «Brute-Force»-Methode (ausprobieren aller Möglichkeiten) und des besten Supercomputers (Tianhe-2) unrechtmässig zu entschlüsseln, würde es im Durchschnitt $9.63^{*}10^{52}$ Jahre dauern (man beachte, dass das Alter des Universums auf $1.4^{*}10^{10}$ Jahre geschätzt wird).

4.1 Conclusio Verschlüsselung

Durch die Verschlüsselung kann ein angemessenes Maß an «Anonymisierung» erreicht werden. Es werden keine persönlichen Daten in einer Cloud gespeichert, solange der Auftragsverarbeiter nicht im Besitz des Schlüssels ist – zumindest wird dies so unter dem relativen Auslegungsansatz subsumiert. Unternehmen müssen daher sicherstellen, dass die genannten Sicherheitsstufen eingehalten werden. Der relative Ansatz besagt, dass angemessene Verschlüsselungstechniken zu der Möglichkeit einer Nichtanwendbarkeit der DS-GVO führen könnten, falls diese nach dem neusten Stand der Technik durchgeführt wird. So exemplarisch die Forschungsergebnisse[29] von Prof. Dr. Gerald Spindler von der Universität Göttingen. Darin wird die Anwendbarkeit der DS-GVO durch den Einsatz einer „state-of-the-art"-Verschlüsselung verneint.[30] Einige Elemente der DS-GVO können als absoluter Ansatz für den materiellen Anwendungsbereich der DS-GVO interpretiert werden. Dieser absolute Ansatz stellt jedoch keine absolute Sicht im rechtlichen Sinne dar, solange der EuGH und die EU-Kommission keine Stellungnahme bzw. Entscheid abgegeben haben, die den materiellen Anwendungsbereich erweitert und die These hinsichtlich der Nicht-Anwendbarkeit «State-of-the-Art» -verschlüsselter Daten untermauert.

Bis dahin müssen alle betroffenen Unternehmen ihren Grad der Verschlüsselung ermitteln und die damit verbundenen Risiken (beispielsweise in einer Datenschutz-Folgenabschätzung) beurteilen. Dazu gehört auch die Beurteilung des technischen Grads ihrer Verschlüsselung.

5. Anonymisierte Daten

Neben der Pseudonymisierung und der Verschlüsselung möchten wir eine dritte Form der Datensicherheit im Kontext dieses Beitrags vorstellen: Die Anonymisierung. Diese stellt eine irreversible Datenverarbeitungstechnik dar.

Anonymisierten Daten finden bei Anonymisierung von Identifikatoren Anwendung, d.h. wenn alle Elemente, die möglicherweise einen Rückschluss auf die Identität der Personen zulassen, entfernt oder dauerhaft verändert werden (z. B. durch Löschen oder Aggregieren von Daten). In diesen Fällen können diese Daten nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden. Solche Daten gelten nicht mehr als Gegenstand der DS-GVO, da die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten und die Daten schlichtweg auch nicht mehr als personenbezogene Daten angesehen werden. Damit werden Informationen, die keine Rückschlüsse auf identifizierte oder identifizierbare natürliche Personen zulassen, von den neuen EU-Regelungen ausgenommen. Diese Ausnahme ist beispielsweise wichtig für empirische Projekte, Forschung und Studien, da die Verordnung nicht für die Verarbeitung anonymisierter Daten im Rahmen von statistische Erhebungen oder für andere Forschungszwecke Anwendung findet.[31]

6. Schlussfolgerungen für Unternehmen

Die DS-GVO stellt für viele Unternehmen ein datenschutzrechtlicher Einschnitt dar, der mit einem enormen Mehraufwand verbunden ist. Gleichzeitig erhöhen die Anforderungen und Maßnahmen zur Gewährleistung einer ständigen Datensicherheit die Komplexität der gesamthaften Umsetzung des Gesetzes. Für die meisten Unternehmen ergeben sich vor diesem Hintergrund weitergehende Aufgaben.

In einem ersten Schritt sollten sie zunächst einen Abgleich ihres Sicherheitslevels mit dem aktuellen Stand der Technik vornehmen, um gegebenenfalls Nachbesserungsbedarf zu ermitteln und die Lücken sodann schließen zu können. Sofern die Sicherheitslevel angepasst werden müssen ist zu entscheiden, ob dem relativen oder dem absoluten Auslegungsansatz gefolgt werden soll. Sofern der relative Ansatz gewählt wird, muss die IT-Abteilung des Unternehmens sicherstellen, dass der Verschlüsselungsgrad hoch genug ist, um ein ähnliches Niveau wie bei der Anonymisierung zu erreichen.

Der Entscheid zugunsten eines Ansatzes sollte auf einem risikobasierten Ansatz beruhen, der die spezifischen Auswirkungen für die gesamte Organisation bewertet und abwägt. Dabei spielen die technischen Gegebenheiten eine sehr große Rolle. In der Praxis zeigt sich bislang, dass diese Entscheidung von größerer Komplexität geprägt ist und hohes Fach- bzw. Expertenwissen erfordert. Experten können dabei helfen unter einem Risiko basierten Ansatz die richtige Verschlüsselungstechnik auszuwählen und zu implementieren.

Eine weiterer Komplexitätsgrad ergibt sich durch den Datenaustausch mit Ländern ausserhalb der EU[32]. Werden Daten in solche Länder transferiert, müssen zusätzlich gemäß Art. 46 DS-GVO rechtliche Garantien gewährleistet sein. Dies kann mit EU-Standardvertragsklauseln bzw. Binding Corporate Rules (Datentransfers innerhalb einer Unternehmensgruppe) erfolgen. Auch hier empfiehlt sich die frühzeitige Beratung durch Datenschutzexperten.

Über die Autoren

Jutta Sonja Oberlin

CIPM, CO (Universität Augsburg), zertifizierte Datenschutzbeauftragte, Master of Compliance, studierte Rechtswissenschaften an der Universität Zürich (UZH) ist Managerin im Cyber Security Team bei der Deloitte AG in Zürich. Auch doziert sie zum Thema EU Datenschutz und BDSG an der Universität Augsburg. Ihre Expertise umfasst die Beratung von datenschutzrechtlichen Sachverhalten und Problematiken unter diversen Regulationen wie die DS-GVO und weiteren internationalen Bestimmungen.

Gianni Crameri

ist Assistant Manager im Cyber Security Team bei der Deloitte AG in Zürich. Er hat umfangreiche Erfahrungen in der Life-Science- und Fertigungsindustrie gesammelt. Er war verantwortlich für mehrere Security Assessments kritischer Applikationen bei einem führenden Pharmaunternehmen und unterstützte diverse Kunden bei der Entwicklung einer globalen IT-Sicherheitsstrategie. Auch umfasst seine Expertise die Beratung im Bereich Datenschutz. Durch sein technisches Know-How ist es ihm möglich die gesetzlichen Anforderungen in die Praxis umsetzen und er fungiert so als eine Schnittstelle zwischen Recht und IT.

▶ www2.deloitte.com

Deloitte.

[29] Die Forschungsarbeiten, welche zu diesen Ergebnissen führten, wurden im 7. Rahmenprogramm der Europäischen Union (RP / 2007-2013) im Rahmen der Finanzhilfevereinbarung Nr. ICT-609611 (PRAXIS) evaluiert.

[30] SPINDLER GERALD/SCHMECHEL PHILIPP, Personal Data and Encryption in the European General Data Protection Regulation, S. 1.

[31] Vgl. Erwägungsgrund 26 zur DS-GVO.

[32] Sog. Drittstaaten.

DATENSCHUTZPRAXIS

„VIDEOBEWEIS“ AUCH IM STRASSENVERKEHR? – RECHTLICHE UND PRAKTISCHE KONSEQUENZEN DER BGH-ENTSCHEIDUNG ZUM EINSATZ VON DASHCAMS

Dr. Wolf-Tassilo Böhm und Isabelle Brams

Zweck und Probleme von Dashcams im Straßenverkehr

Die Zulässigkeit von Videoaufzeichnungen mittels sog. „Dashcams“ ist schon seit längerer Zeit ein kontrovers diskutiertes Thema. Unter Dashcams versteht man kleine Videokameras, die zumeist am Armaturenbrett (Dashboard) oder Rückspiegel eines Fahrzeugs befestigt werden und aus der Perspektive des Fahrers das Verkehrsgeschehen aufzeichnen. Sie dienen dazu, insbesondere den Hergang von Unfällen und andere Vorkommnisse im Straßenverkehr zu Beweiszwecken festzuhalten.

Der praktische Nutzwert von Dashcams liegt auf der Hand. Frei nach dem Sprichwort, „ein Bild sagt mehr als tausend Worte“ könnten audiovisuelle Aufzeichnungen aufwendige Beweisverfahren bei Haftungsprozessen vielfach entbehrlich machen. Dies gilt insbesondere für zeit- und kostenintensive Sachverständigengutachten.

Es überrascht somit nur wenig, dass sich Dashcams einer immer größeren Beliebtheit erfreuen. Einer aktuellen Umfrage des Branchenverbandes Bitkom zufolge besitzen 8% der Befragten bereits eine Dashcam, während weitere 13% sich in Zukunft auf jeden Fall eine anschaffen wollen und weitere 25% dies in Erwägung ziehen.[1]

Der Einsatz von Dashcams stellt die Nutzer jedoch vor datenschutzrechtliche Probleme, da das Aufzeichnen des Straßenverkehrsgeschehens in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung der anderen Verkehrsteilnehmer eingreift. Denn diese werden regelmäßig gegen ihren Willen, ohne ihre Kenntnis oder jedenfalls ohne Möglichkeit sich hiergegen zu verwehren, gefilmt. Ferner setzen Dashcams auch Arbeitnehmer im Transport- oder Logistikgewerbe bzw. die Fahrer von Dienstwagen einer Form der Überwachung am Arbeitsplatz aus.

Grundsatzurteil des BGH

Der Bundesgerichtshof (BGH) hat am 15. Mai 2018 ein Urteil erlassen, das wegweisende Ausführungen zum Einsatz von Dashcams im Straßenverkehr enthält.[2]

In dem vom BGH entschiedenen Fall waren zwei Verkehrsteilnehmer beim Abbiegen kollidiert. Der genaue Unfallhergang war zwischen den Parteien streitig. Die Dashcam-Aufzeichnung des Klägers legte nahe, dass den Kläger an der Unfallverursachung kein Verschulden traf. Die Vorinstanzen hatten die Aufzeichnungen jedoch nicht als zulässiges Beweismittel erachtet. Das permanente Aufzeichnen des Straßenverkehrs sei rechtswidrig. Daher könnten die Aufzeichnungen auch nicht im Prozess verwertet werden.[3]

Der BGH stimmte den Vorinstanzen nunmehr dahingehend zu, dass der Einsatz der Dashcam im vorliegenden Fall datenschutzrechtlich unzulässig gewesen sei. Das bloße Beweisinteresse des Autofahrers rechtfertige keine permanente und anlasslose Überwachung des gesamten Straßenverkehrs.

Der BGH zog daraus jedoch andere Schlüsse als die Vorinstanzen. Die Aufzeichnungen seien vor Gericht als Beweismittel verwertbar. Eine datenschutzwidrige Beweiserhebung führe nicht automatisch auch zu einem Beweisverwertungsverbot im Zivilprozess. Vielmehr sei über die Frage der Verwertbarkeit in jedem Einzelfall gesondert zu entscheiden. Das Prozessgericht habe eine umfangreiche Interessenabwägung vorzunehmen, die sämtliche Umstände des Einzelfalls berücksichtige. Im vorliegenden Fall fiel die Abwägung zugunsten des geschädigten Klägers aus.

Der BGH kam somit zu dem Schluss, dass die Dashcam-Aufzeichnungen zugunsten des Klägers zu verwerten seien. Diese Entscheidung wird für die Praxis voraussichtlich weitreichende Folgen haben. Aus dem Urteil lassen sich insofern drei wesentliche Erkenntnisse ableiten:

Mehr Rechtssicherheit und mehr Risiken

Bis zur Entscheidung des BGH hatten Instanzgerichte vielfach uneinheitliche Entscheidungen zur datenschutzrechtlichen Zulässigkeit und Verwertbarkeit von Dashcam-Aufzeichnungen erlassen.[4] Das Urteil des BGH sorgt insofern für mehr Rechtssicherheit. Allerdings verwies der BGH ausdrücklich darauf, dass die Frage der Verwertbarkeit von Dashcam-Aufzeichnungen im Einzelfall auf der Grundlage einer Interessenabwägung zu beantworten ist. Eindeutige Kriterien für die Interessenabwägung gibt der BGH aber nicht vor. So bleibt der Einsatz von Dashcams für Privatpersonen und Unternehmen weiterhin mit erheblichen Risiken verbunden.

Datenschutzwidrigkeit anlassloser und permanenter Aufzeichnungen

Der BGH stellt ausdrücklich klar, dass das anlasslose und permanente Aufzeichnen des Straßenverkehrs mittels einer Dashcam regelmäßig datenschutzrechtlich unzulässig ist. Es fehlt insofern an einem datenschutzrechtlichen Erlaubnistatbestand.

Die Entscheidung des BGH erging noch zur Rechtslage vor Inkrafttreten der DS-GVO. § 6b Abs. 1 Nr. 3 BDSG a.F. enthielt zwar einen Erlaubnistatbestand für Videoaufzeichnungen öffentlich zugänglicher Räume (zu denen auch der öffentliche Straßenverkehr zählt). Die Norm

setzte jedoch grundsätzlich voraus, dass die verantwortliche Stelle ein überwiegendes Interesse an der Datenverarbeitung geltend machen konnte. Daran wird es beim dauerhaften Einsatz von Dashcams wohl im Regelfall fehlen. Insbesondere kann das bloße Beweisinteresse des Autofahrers den anlasslosen und permanenten Eingriff in die Persönlichkeitsrechte der anderen Verkehrsteilnehmer nicht rechtfertigen.

Diese Grundsätze lassen sich auch auf die Rechtslage unter der DS-GVO übertragen. Zwar sieht auch das BDSG n.F. einen Erlaubnistatbestand für bestimmte Formen der Aufzeichnungen vor (vgl. § 4 BDSG n.F.). Die Norm setzt aber ebenfalls eine Interessenabwägung im Einzelfall voraus, die in Fällen anlassloser und permanenter Aufzeichnungen wohl im Regelfall nicht zugunsten des Autofahrers ausfallen würde.

Die datenschutzrechtliche Zulässigkeit von Dashcam-Aufzeichnungen könnte anders zu beurteilen sein, wenn Dashcams das Verkehrsgeschehen nicht dauerhaft aufzeichnen, ▸

[1] bitkom: „Jeder Zweite für Dashcam-Pflicht“, Pressemitteilung vom 6. April 2018 (online verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Jeder-Zweite-fuer-Dashcam-Pflicht.html).

[2] BGH, Urteil vom 15. Mai 2018 – VI ZR 233/17, BeckRS 2018, 8602.

[3] Vgl. AG Magdeburg, Urteil vom 19. Dezember 2016 – 104 C 630/15; LG Magdeburg, Urteil vom 5. Mai 2017 – 1 S 15/17, BeckRS 2017, 144696.

[4] Vgl. beispielhaft LG Frankenthal, Urteil vom 30. Dezember 2015 – 4 O 358/15, NJOZ 2016, 1195; OLG Nürnberg – Hinweisbeschluss vom 10. August 2017 – 13 U 851/17, NJW 2017, 3597; LG Rottweil, Urteil vom 20. Februar 2017 – 1 O 104/16, BeckRS 2017, 119419; LG Traunstein, Urteil vom 1. Juli 2016 – 3 O 1200/15, ZD 2017, 239.

DATENSCHUTZPRAXIS

sondern nur punktuell den Unfallzeitpunkt. So existieren beispielsweise Dashcams, die nur für einen voreingestellten Zeitraum Aufzeichnungen anfertigen und diese dann immer wieder überschreiben (sog. „Loop"-Aufzeichnungen). Diese Dashcams speichern die Aufzeichnungen nur dann, wenn der Fahrer abrupt abbremst oder der Airbag des Autos ausgelöst wird. Zwar werden auch in diesen Fällen die Persönlichkeitsrechte anderer Verkehrsteilnehmer berührt. Der Eingriff wiegt aber wegen der kurzen Aufzeichnungsdauer weniger schwer.[5] Es spricht daher Vieles dafür, dass Gerichte und Datenschutzaufsichtsbehörden diese Form der Aufzeichnung wohl eher als datenschutzrechtlich zulässig erachten könnten.

Verwertbarkeit rechtswidriger Dashcam-Aufzeichnungen

Aus der Rechtswidrigkeit der Beweiserhebung folgt im Zivilprozess nicht automatisch ein prozessuales Verwertungsverbot.[6] Über die Frage der Verwertbarkeit ist stets auf Grundlage einer umfassenden Interessens- und Güterabwägung nach Maßgabe der Umstände des Einzelfalls zu entscheiden. Auch im Hinblick auf die Verwertbarkeit von Dashcam-Aufzeichnungen ist dies die richtige Lösung. Pauschale Wertungen würden den Umständen des Einzelfalls nicht hinreichend Rechnung tragen.

Im Rahmen der Abwägung sind die Interessen des Beweisführers, der sich auf die Dashcam-Aufzeichnungen stützen möchte, und die gegenläufigen Interessen des Beweisgegners zu einem angemessenen Ausgleich zu bringen. Der Beweisführer muss sich nach der Entscheidung des BGH in einer Art „Beweisnot" befinden. Dabei kommt es auch darauf an, ob dem Beweisführer weitere Beweismittel, wie beispielsweise Zeugen, zur Verfügung stehen.

Rechtsfolgen für die Verwender von Dashcams

Der BGH hat keinen Freibrief für den Einsatz von Dashcams erteilt. Vielmehr müssen Privatpersonen und Unternehmen, die Dashcams nutzen wollen, umfassende datenschutzrechtliche Vorgaben einhalten, um sich nicht erheblichen Haftungsrisiken auszusetzen. So müssen sie unter anderem umfangreiche technische und organisatorische Vorkehrungen treffen. Zu den datenschutzrechtlich erforderlichen Maßnahmen kann auch die Benennung eines Datenschutzbeauftragten (Art. 37 Abs. 1 lit. b) DS-GVO) sowie die Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 Abs. 3 lit. c) DS-GVO) zählen. Dashcam-Aufzeichnungen sind auch im Verzeichnis der Verarbeitungstätigkeiten und im Rahmen des Löschkonzepts zu berücksichtigen. Bislang fehlen klare Vorgaben, wie Autofahrer und Unternehmen datenschutzrechtliche Transparenz- und Hinweispflichten gegenüber den gefilmten Verkehrsteilnehmern erfüllen können.

Es ist nicht auszuschließen, dass die zuständigen Datenschutzaufsichtsbehörden Zuwiderhandlungen in Einzelfällen mit entsprechenden Bußgeldern sanktionieren.[7] Im Extremfall kann die datenschutzrechtswidrig erlangte Aufzeichnung sogar strafbar sein, etwa wenn das Videomaterial im Internet veröffentlicht wird (vgl. § 201a StGB sowie §§ 22, 33 Abs. 1 KunstUrhG).

Auf diesen Umstand hat auch der BGH explizit hingewiesen.

Von besonderer Bedeutung sind die datenschutzrechtlichen Anforderungen für Unternehmen, die ihre Dienstwagenflotte mit Dashcams ausrüsten wollen. Hierbei steht vielfach nicht nur das Beweisinteresse im Vordergrund. Mittels Dashcams-Aufzeichnungen könnten Unternehmen auch angestellte Berufskraftfahrer und andere Nutzer von Dienstwägen kontrollieren. Dabei wäre es dem Arbeitgeber grundsätzlich möglich, das gesamte Fahrverhalten des Mitarbeiters zu kontrollieren, z.B. die gewählte Fahrtroute, Pausenzeiten oder das allgemeine Verkehrsverhalten (etwa abruptes Abbremsen, dichtes Auffahren oder Geschwindigkeitsüberschreitungen). Dass ein solches Vorgehen Mitarbeiter einem erheblichen Überwachungsdruck aussetzen könnte, liegt auf der Hand. Es ist insoweit damit zu rechnen, dass Gerichte Überwachungsmaßnahmen mittels Dashcams als schwerwiegenden Eingriff in die Persönlichkeitsrechte der betroffenen Mitarbeiter werten würden.

Überwachungsmaßnahmen am Arbeitsplatz waren in Vergangenheit schon vielfach Anlass für arbeitsgerichtliche Verfahren. Dies gilt etwa für die Videoüberwachung am Arbeitsplatz[8] oder Torkontrollen[9]. In jüngster Vergangenheit hat sich das Bundesarbeitsgericht (BAG) auch mit dem verdeckten Einsatz von sog. Keylogger-Programmen[10] befasst.[11]

Gerade das zuletzt zitierte Urteil des BAG weist Parallelen zu einer möglichen Überwachung von Mitarbeitern mittels Dashcams auf. So befand das BAG, dass der anlasslose und zeitlich nicht begrenzte Einsatz von Keylogger-Programmen einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Arbeitnehmer darstelle und somit nicht mit datenschutzrechtlichen Vorgaben vereinbar sei. Hieraus gewonnene Erkenntnisse unterlägen einem Beweisverwertungsverbot.[12] Es ist wohl damit zu rechnen, dass das BAG bei Überwachungsmaßnahmen mittels Dashcams ähnliche Maßstäbe anlegen würde.

Fazit

Die Entscheidung des BGH sorgt für mehr Klarheit und Rechtssicherheit beim Einsatz von Dashcams im Straßenverkehr. Die anlasslose und pauschale Aufzeichnung des Verkehrsgeschehens mittels einer Dashcam dürfte regelmäßig datenschutzwidrig sein. In diesem Fall drohen Bußgelder wegen Datenschutzverstößen, Schadensersatzforderungen und andere Nachteile. Autofahrer und Unternehmen müssen sich vor diesem Hintergrund die Frage stellen, ob und wie sie den Einsatz von Dashcams datenschutzkonform gestalten können, um Haftungsrisiken möglichst zu minimieren. Wollen Unternehmen Dashcams in dienstlich genutzten Fahrzeugen einsetzen, sind zudem einschlägige Informations- und Mitbestimmungsrechte der Arbeitnehmervertretungen zu beachten.

Datenschutzrechtswidrig erlangte Aufzeichnungen führen aber nicht automatisch auch zu einem prozessualen Beweisverwertungsverbot. Vielmehr bedarf es einer Interessenabwägung im Einzelfall. Im Rahmen der Abwägung finden nicht nur die Beweisinteressen des Beweisführers, sondern auch die Intensität des Eingriffs in die Persönlichkeitsrechte des Beweisgegners Berücksichtigung.

Über die Autoren

Dr. Wolf-Tassilo Böhm

ist Senior Associate bei Hogan Lovells Frankfurt und berät Unternehmen im Datenschutzrecht, bei arbeitsrechtlichen Fragen und zu Compliance. Er verfügt über umfangreiche Erfahrung insbesondere bei beschäftigtendatenschutzrechtlichen Themen und dem Einsatz von IT im Arbeitsumfeld.

Isabelle Brams

ist Associate im Arbeits- und Datenschutzrechtsteam bei Hogan Lovells Frankfurt. Sie berät deutsche und international tätige Unternehmen im Zusammenhang mit allen Fragen des Datenschutzrechts.

▶ http://hoganlovells-blog.de

[5] Vgl. der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz zu Dashcams (online verfügbar unter: https://www.datenschutz.rlp.de/de/themenfelder-themen/dashcams/).

[6] Prütting, in: Münchener Kommentar ZPO, 5. Aufl. 2016, § 284 Rn. 66.

[7] So bei einer Privatperson, die ca. 56.000 Straßenverkehrsverstöße Dritter gemeldet hatte und 2014 damit begann, eine Dashcam im Verkehr einzusetzen, OLG Celle, Beschluss vom 4. Oktober 2017 – 3 Ss (OWi) 163/17, ZD 2018, 85.

[8] BAG, Urteil vom 27. März 2003 – 2 AZR 51/02, NZA 2003, 1193.

[9] BAG, Urteil vom 13. Dezember 2007 – 2 AZR 537/06, NZA 2008, 1008.

[10] Keylogger-Programme sind dazu konzipiert, die Tastenanschläge des Benutzers über die Tastatur seines Endgeräts zu protokollieren.

[11] BAG, Urteil vom 27. Juli 2017 – 2 AZR 681/16, NZA 2017, 1327.

[12] BAG, Urteil vom 27. Juli 2017 – 2 AZR 681/16, NZA 2017, 1327.

DATENSCHUTZPRAXIS

BAYERISCHES VERWALTUNGSGERICHT ENTSCHEIDET ÜBER EINSATZ VON FACEBOOK-MARKETING-TOOL

Kristin Benedikt

Fast jede Website setzt Tools von Drittanbietern ein. Mithilfe der Tools erhoffen sich Betreiber von Websites die Reichweite zu messen, die Benutzerfreundlichkeit zu steigern, Kunden zu gewinnen oder über Werbeeinnahmen den Dienst zu finanzieren. Doch spätestens seit dem 25. Mai 2018 ist die Verunsicherung groß, ob und unter welchen Bedingungen solche Dienste datenschutzkonform eingesetzt werden dürfen. Jetzt gibt es zumindest teilweise Klarheit. Pünktlich zur Geltung der DS-GVO entschied ein bayerisches Verwaltungsgericht über den datenschutzkonformen Einsatz eines Werbe-Tools.

1. Worum es in der Entscheidung geht

Das Bayerische Landesamt für Datenschutzaufsicht hatte schon vor einiger Zeit den Einsatz eines Marketing-Tools von Facebook geprüft. Nach Ansicht der Behörde setzten einige Unternehmen das Marketing-Werkzeug „Facebook Custom Audience über die Kundenliste“ rechtswidrig ein. Zu den häufigsten Verstößen zählten u.a., dass

- die Datenschutzbestimmung keine oder fehlerhafte Informationen zum Einsatz des Tools enthielten,
- kein Opt-Out-Verfahren zur Verfügung gestellt wurde und
- der Einsatz des Marketing-Tools weder auf eine wirksame Einwilligung des Betroffenen gestützt werden konnte, noch eine Rechtsgrundlage den Einsatz des Werbe-Tools erlaubte.

Das Ergebnis der Prüfung war überraschend, denn die Aufsichtsbehörden haben in der Vergangenheit wiederholt auf die Anforderungen für einen zulässigen Einsatz hingewiesen.[1]

Nachdem die Prüfung ausgewertet wurde, setzten die meisten Unternehmen die Anforderungen der Datenschutzaufsichtsbehörde um oder stellten die Datenverarbeitung ein. Nur wenige Unternehmen waren anderer Meinung und sahen keinen Verstoß gegen geltendes Datenschutzrecht. Daraufhin erließ die Aufsichtsbehörde eine Anordnung und verbot den weiteren Einsatz des Werbe-Tools und forderte auf, die laufenden Werbe-Kampagnen zu beenden.

2. Wie das Gericht entschied

Gegen diese Anordnung klagte ein Unternehmen. Nunmehr liegt eine Entscheidung im Eilverfahren vor, in der das Gericht die Auffassung der Datenschutzaufsicht bestätigt: das Marketing-Tool wurde rechtswidrig eingesetzt.[2]

Zunächst führte das Gericht in technischer Sicht aus, dass das Hash-Verfahren SHA-256 nicht geeignet sei, die Kundendaten zu anonymisierten. Diese Aussage kann auch auf andere Verfahren übertragen werden, wie z.B. dem Offline-Tracking, bei dem die MAC-Adressen in Hash-Werte umgewandelt werden.

Die Konsequenz: Wenn das Hash-Verfahren nicht zu einer Anonymisierung führt, handelt es sich weiterhin um personenbezogene Daten, sodass sämtliche Anforderungen des Datenschutzes zu beachten sind.

Außerdem entschied das Gericht, dass:

- zwischen Facebook und dem werbetreibenden Unternehmen keine Auftragsverarbeitung vorliegt, weil Facebook weisungsunabhängig ist und über die wesentlichen Verarbeitungsschritte selbst entscheidet,
- aus diesem Grund das Hochladen der Kundenliste eine Übermittlung darstellt und einer Rechtsgrundlage oder einer Einwilligung bedarf,
- Verantwortliche den Einsatz des Tools nicht auf die Interessenabwägung stützen können, weil die Interessen der Betroffenen überwiegen.

Daraus folgt, dass ein rechtmäßiger Einsatz nur nach voriger informierter Einwilligung des Betroffenen zulässig ist.

Über Facebook Custom Audience können Verantwortliche Werbekampagnen auf Facebook veröffentlichen. Dazu erstellt das Unternehmen eine Liste von Kunden oder Interessenten. Die Liste enthält personenbezogene Daten wie z.B. Name, Wohnort, Telefonnummer und E-Mail-Adresse und wird im Facebook-Konto des Unternehmens hochgeladen. Facebook gleicht die Kundenliste mit sämtlichen Facebook-Nutzern ab, um zu ermitteln, welcher Facebook-Nutzer auch Kunde des Unternehmens ist. Im Anschluss startet das Unternehmen eine Werbekampagne und kann über Facebook optional eine Zielgruppe für diese Werbekampagne festlegen. Nun wird die Kampagne Facebook-Nutzern angezeigt, die entweder auch Kunde des Unternehmens sind bzw. zur Zielgruppe der Werbekampagne gehören.

Welche Facebook-Nutzer die Werbung erhalten, erfährt das Unternehmen nicht. Lediglich die Facebook-Nutzer können in ihrem Facebook-Profil nachvollziehen, welche Werbung sie erhalten. Ein Geheimnis bleibt auch, wieso ein bestimmter Nutzer in einer konkreten Zielgruppe aufgenommen wurde und weshalb er die Werbung angezeigt bekommt.

3. Was das für andere Tools bedeutet

Weit verbreitet ist die Auffassung, dass Verantwortliche für Werbezwecke sämtliche Online-Tools, insbesondere Tracking-Tools einsetzten dürfen, ohne eine Einwilligung des Betroffenen einzuholen. Begründet wird dies häufig damit, dass in Erwägungsrund 47 der DS-GVO Direktwerbung als berechtigtes Interesse ausdrücklich genannt ist. Aus diesem Grund gehen viele Verantwortliche davon aus, dass Tracking-Tools gem. Art. 6 Abs. 1 lit. f) DS-GVO rechtmäßig seien und eine Einwilligung des Betroffenen nicht erforderlich ist. Doch diese Schlussfolgerung ist nicht korrekt.

Verantwortliche sollten sich bewusst machen, dass Art. 6 Abs. 1 lit. f) DS-GVO eine umfangreiche Interessenabwägung voraussetzt. Im Grunde handelt es sich um eine drei-stufige Prüfung, bei der folgendermaßen vorzugehen ist:

1. Berechtigte Interessen des Verantwortlichen ermitteln, z.B. Interesse eines Online-Shops an Werbung für gezielte Sonderangebote,
2. Interessen oder Grundrechte des Betroffenen ermitteln, z.B. Interesse, einen Online-Dienst zu nutzen, ohne dass ein webseitenübergreifendes Nutzungsprofil erstellt wird,
3. Interessen gegeneinander abwiegen, z.B. überwiegt das Interesse des Betroffenen, wenn anhand des Nutzungsverhaltens individuelle Preise festgelegt werden und der Betroffene die Kriterien für die Preisbildung nicht kennt.

Für die Interessenabwägung gelten auch nach der DS-GVO dieselben Grundsätze wie schon nach der Datenschutz-Richtlinie. Verantwortliche können sich daher noch an der Stellungnahme der Art.-29-Gruppe zum Begriff des „berechtigten Interesses“ orientieren.[3] ▸

[1] Bayerisches Landesamt für Datenschutzaufsicht, Pressemitteilung vom 4. Oktober 2017 zu Facebook Custom Audience bei bayerischen Unternehmen; Allgemeine Hinweise und Anforderungen für Verantwortliche zum Einsatz von Facebook Custom Audience.

[2] Beschluss des VG Bayreuth vom 8. Mai 2018, Az.: B 1 S 18.105.

[3] Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verantwortung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, S. 39 ff.

4. Was noch zu berücksichtigen ist

Neben der Entscheidung des Verwaltungsgerichts ist beim Einsatz von Werbe-Tools vor allem die Entscheidung des Europäischen Gerichtshofs zu „Facebook-Fanpages" relevant. Der EuGH entschied, dass Betreiber einer Facebook-Fanpage gemeinsam mit Facebook datenschutzrechtlich verantwortlich sind.[4]

Die Aufsichtsbehörden werden sich nun mit der Frage auseinandersetzen müssen, ob und wieweit die Entscheidung auf andere Sachverhalte im Internet übertragbar ist. Konkret geht es dabei um die Einbindung von Drittinhalten wie Schriftarten, Kartendiensten, Videos, Social-Plugins oder den Einsatz von Zählpixeln für Werbezwecke.

Einen wichtigen Hinweis dazu gibt es bereits: Der Generalanwalt hat in seinem Schlussantrag in Sachen Facebook-Fanpages klargestellt, dass es „keinen grundlegenden Unterschied zwischen dem Fall eines Fanpage-Betreibers und dem des Betreibers einer Website, der den Code eines Webtracking-Dienstleisters in seine Website einbindet" gibt.[5]

Würden die Aufsichtsbehörden dieser Auffassung künftig folgen, hätte das weitreichende Konsequenzen, denn nahezu jede Website nutzt mittlerweile Dienste von Drittanbietern bzw. bindet Tracking-Code ein.

5. Was Verantwortliche jetzt dringend tun sollten

Verantwortliche sollten beide Entscheidungen unbedingt zum Anlass nehmen und den derzeitigen Einsatz sämtlicher Tools auf Websites prüfen. Überprüft werden sollte insbesondere, ob

- die Datenverarbeitung nur aufgrund einer Einwilligung zulässig ist,
- die Einwilligung die neuen Anforderungen der DS-GVO erfüllt, vor allem muss sichergestellt sein, dass keine Nutzungsdaten erhoben werden bevor der Nutzer eingewilligt hat,
- die Informationspflichten gem. Art. 12 ff. DS-GVO erfüllt sind und
- ein Opt-Out-Verfahren zur Verfügung steht und technisch korrekt implementiert ist.

Diese Anforderungen wurden zwar konkret für das Marketing-Tool „Facebook-Custom-Audience" aufgestellt. Es handelt sich aber um allgemeingültige Pflichten, die auch für andere Werbe-Tools gelten.

Denn eines sollten sich Verantwortliche verdeutlichen: Im Gegensatz zu IT-Sicherheits- oder Berechtigungskonzepten, die nur über ein internes Audit geprüft werden können, können Verstöße gegen die o.g. Anforderungen von jedermann - egal ob von Behörden, Wettbewerbern oder Betroffenen geprüft werden. Die Wahrscheinlichkeit, dass Verstöße festgestellt werden, ist somit ungleich höher.

Über die Autorin

Kristin Benedikt
Leiterin Referat 4 (Internet, Telemedien, Apps) im Bayerischen Landesamt für Datenschutzaufsicht

Der Artikel gibt die persönliche Auffassung der Autorin wieder.

[4] EuGH C-210/16.

[5] Schlussanträge des Generalsanwalts Yves Bot, vom 24. Oktober 2017, Rechtssache C-210/16, Rn. 69.

Anzeige

2018

BvD-Herbstkonferenz Datenschutz

24. - 26.10.2018
im STEIGENBERGER HOTEL GRAF ZEPPELIN - STUTTGART

FACHGESPRÄCHE I EXPERTENWISSEN I DIALOGPLATTFORM I DISKUSSIONEN

Steigenberger Graf Zeppelin
199,00 € / ÜF Stichwort BvD-Herbstkonferenz - abrufbar bis 27.08.2018
Reservierung: 0711/20480
reservations@stuttgart.steigenberger.de
Die Zimmer können bis 1 Woche vor Anreise kostenfrei storniert werden.
Parkgebühren werden nicht übernommen.

Hinweis: Reservieren Sie frühzeitig, in der Woche ist in Stuttgart Messe und die Zimmerverfügbarkeit ist eingeschränkt.

Gemeinsame Veranstaltung von:

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

BayLDA

BvD e.V. DATENSCHUTZ GESTALTEN

DATENSCHUTZPRAXIS

REIFEGRADMODELL ZUR DARSTELLUNG DER TOM

Dipl.-Ök. Stephan Rehfeld, scope & focus Service-Gesellschaft mbH, Hannover

Die toM (technische und organisatorische Maßnahmen) werden im Datenschutzrecht zur Beschreibung des Datenschutzniveaus in der eigenen Organisation benötigt und dann auch zur Kommunikation des erforderlichen Datenschutzniveaus bei Verträgen zur Auftragsverarbeitung. Wir haben in Deutschland im öffentlichen und nicht-öffentlichen Bereich nunmehr seit Jahrzehnten Praxiserfahrungen mit den toM, haben aber noch keine praktikable Lösung bei der Anwendung der toM gefunden.

Ein Ausweg aus dieser Misere kann der Einsatz eines Reifegradmodells bieten. Der Einsatz des VDA Information Self Assessments dient hier als Ideengeber. Ein aktuelles Projekt des BITKOM soll im Laufe des Jahres als Best Practice dienen, wie dann ein solches Informationssicherheits-Audit auf den Datenschutz angewendet werden kann.

Bisherige Praxis

Unter BDSG-2001 wurde in der Praxis vom Datenschutzbeauftragten der verantwortlichen Stelle häufig irgendeine Checkliste ausgewählt und konsequent eingesetzt. Mögliche Vorlagen waren zum Beispiel:

- Checkliste der GDD (Dr. Münch)
- Checklisten der Aufsichtsbehörden
- Anhang A der ISO 27001
- IT-Grundschutzkataloge unter Beachtung der Einschränkung der Tabelle „Maßnahmen und Datenschutz-Kontrollziele zu Baustein 1.5 Datenschutz“

Hierbei wurde das Kriterium der Erforderlichkeit des § 9 BDSG-2001 bei einer Maßnahmenauswahl häufig gar nicht betrachtet. Auch eine Bestimmung des Schutzzwecks wurde nicht vorgenommen. Aus diesem Grund konnte durch den Datenschutz auch keine Maßnahmenauswahl getroffen, stattdessen lediglich der IST-Zustand in der Organisation beschrieben werden. Häufig konnte auch beobachtet werden, dass eine Checkliste der toM durch die Datenschutz-Abteilung parallel zu anderen Regelungen zur Informationssicherheit gepflegt wurde.

Fazit zur bisherigen Praxis:

- Bei der Maßnahmenauswahl (toMs) muss unbedingt risikoorientiert vorgegangen werden, da sonst eine Maßnahmenauswahl nur zufällig das erforderliche Datenschutzniveau abdeckt. Sollten Maßnahmen getroffen werden, die unter dem erforderlichen Datenschutzniveau liegen, wurden nicht die erforderlichen Investitionen ergriffen und es drohen bei einem Datenschutzvorfall oder einer -prüfung Bußgelder. Sollten Maßnahmen ergriffen worden seien, die über dem erforderlichen Datenschutzniveau liegen, dann wurde zu viel investiert.
- Es sollen für den Bereich der Informationssicherheit der toMs nur Checklisten verwendet werden, die auch in der EDV der Organisation verwendet werden. Die Pflege dieser Informationen soll an die EDV delegiert werden, damit hier kein zusätzlicher Pflegeaufwand entsteht und die Checkliste immer aktuell ist. Es bietet sich hier an, auf nationale oder internationale Standards zurückzugreifen.

Beschreibungsart und -tiefe

Da dem Datenschutzbeauftragten in den Checklisten zu den toM in Extremfällen nur Stichworte zur Verfügung gestellt wurden, waren die Beschreibungen der toM in der Vergangenheit oft mangelhaft. In den heutigen Verträgen zur Auftragsverarbeitung können noch diese archaischen, einsilbigen Beschreibungen gefunden werden. Hier ein Praxisbeispiel (Auszug):

Zugriffskontrolle

- Verwaltung von Berechtigungen
- Differenzierte Berechtigungen
- Profile
- Rollen
- Dokumentation von Berechtigungen

Sehr interessant dürfte eine Auslegung dieser toM in einem Schadenfall oder durch ein Gericht werden. Wie soll zum Beispiel die Maßnahme „Profile“ beim Einsatz von Mobiltelefonen ausgelegt werden? Was bedeutet „differenzierte Berechtigungen“ in der Praxis?

Fazit zur bisherigen Praxis:

- Es sollten nur Checklisten zur Dokumentation der toMs eingesetzt werden, die auf gut dokumentierten Maßnahmenkatalogen basieren, damit möglichst keine oder wenige Auslegungsfragen entstehen.

Auswahl von toM für Auftragsverarbeitungen

Die verantwortliche Stelle hat nunmehr das eigene Datenschutzniveau mit Hilfe einer willkürlich gewählten toM-Checkliste einigermaßen erfolgreich beschrieben. In der Praxis fordert der Auftraggeber vom Auftragnehmer die toM an und akzeptiert sie oder auch nicht. Teilweise bitten Auftraggeber den Auftragnehmer eigene Checklisten zu den toM auszufüllen, damit ein Vergleich der vom Auftragnehmer getroffenen Maßnahmen und der vom Auftraggeber geforderten Maßnahmen erleichtert wird. Allerdings wird hier nur die Zuordnung der Maßnahmen erleichtert, eine Auswertung des Maßnahmenniveaus muss hier immer noch manuell durch den Auftraggeber durchgeführt werden.

Ein Prozess zur Auswahl eines Auftragnehmers kann nun folgendermaßen aussehen:

1. Beide Parteien müssen unabhängig voneinander ihre toM beschrieben haben.
2. Beide Parteien können nun ihrer toM abgleichen:

Auftraggeber	Auftragnehmer
Beschreibung der erforderlichen toMs	Beschreibung der ergriffenen toMs

3. Sollte die toMs vom Auftraggeber und vom Auftragnehmer deckungsgleich sein oder das Schutzniveau beim Auftragnehmer eventuell sogar größer sein als gefordert, kann aus Sicht des Datenschutzes kontrahiert werden.

Fazit zur bisherigen Praxis:

- Damit die getroffenen und geforderten Maßnahmen einfacher verglichen werden können, sollen die Maßnahmen
- in einer identischen Reihenfolge beschrieben werden und für die Maßnahmenausgestaltung sollte
- ein einfach zu vergleichendes System angewendet werden (Levels-Definitionen).

Audits am Beispiel des VDA ISA

Als Grundlage für die Beschreibung der Informationssicherheit im VDA ISA 4.x dient der Anhang A der ISO/IEC 27001:2013. Es wird also die aufgestellte Forderung erfüllt, dass ein gut dokumentierter Standard eingesetzt wird und dass dieser Standard auch in EDV-Abteilungen akzeptiert wird. Auf Basis einer Risikoanalyse wurde allerdings nur eine begrenzte Anzahl an Maßnahmen aus dem Anhang A ausgewählt. Zusätzlich wurden Maßnahmen ergänzt, die in dem Anhang A nicht vorhanden sind. Insgesamt enthält der Anhang A 133 Maßnahmen. Im VDA ISA werden aber nur ca. 51 Maßnahmen abgefragt.

Anpassung der Maßnahmenliste an den konkreten Anwendungsfall

Diese Liste von 51 Maßnahmen muss noch weiter für den konkreten Anwendungsfall angepasst werden. So ist eine Maßnahme „Schutzmaßnahmen im Anlieferungs- und Versandbereich“ natürlich nicht sinnvoll, wenn es keine physische Anlieferung und es keinen physischen Versand gibt. Damit nun aber die ISA-Listen vergleichbar bleiben, werden aus den Listen keine Maßnahmen gestrichen, stattdessen wird der sogenannte Zielreifegrad auf null gesetzt. Somit bleibt die Zuordnung der Maßnahmen in den Katalogen identisch, die Maßnahme wird aber aus der Bewertung herausgenommen.

Aufbau der Maßnahmen

Alle Maßnahmen sind identisch aufgebaut. Dies soll am Beispiel der Maßnahme 6.3 des VDA ISA erläutert werden.

Die Maßnahmenumsetzung wird als Frage dargestellt:

Inwieweit gibt es eine Richtlinie zur Nutzung von mobilen Endgeräten und deren Remote Zugriff auf Daten der Organisation?

Anschließend wird eine Referenz auf den Anhang A der ISO/IEC 27001:2013 zur weiteren Erläuterung gegeben:

(Referenz zu ISO 27001: Control A6.2.1 und A6.2.2)

Danach wird das Ziel dieser Frage klar definiert:

Der Umgang mit mobilen Endgeräten - insbesondere in ungeschützten Umgebungen - ist mit erhöhten Risiken verbunden (z. B. Verlust, Diebstahl, Infektion mit Malware). Damit die auf dem Gerät abgelegten Informationen geschützt sind, müssen technische Schutzmaßnahmen umgesetzt werden. Weiterhin sollten die Mitarbeiter auf die Gefahren im Umgang mit mobilen Endgeräten sensibilisiert werden.

Anschließend werden die zur Maßnahmenerfüllung erforderlichen Aspekte nach Schutzbedarfen beschrieben:

Hierzu muss gehören:

+ Die Nutzung von mobilen Endgeräten (z. B. Smartphones, Notebooks) ist geregelt.

Hierzu sollte gehören:

+ Eine Richtlinie unter Berücksichtigung der folgenden Aspekte ist erstellt:

- Registrierung mobiler Endgeräte

- Anforderungen an den physischen Schutz (u. a. gegen Diebstahl, Ausspähen von Informationen)

- Einschränkungen bei der Installation von Software

- Anforderungen an die Versionierung von Software für mobile Endgeräte und das zugehörige Patch-Management

- Zugangsbeschränkungen zu bestimmten Informationsdiensten

- Verschlüsselungstechniken

- Datensicherung (Backup)

- Schutz vor Schadsoftware

- Remote Löschverfahren

- Nutzung von Web-Services und Web Apps

- Verfahren bei Verlust des mobilen Endgeräts

+ Unterzeichnung einer Verpflichtungserklärung durch die Nutzer zum Umgang mit Besonderheiten bei der Arbeit mit mobilen Endgeräten in Abhängigkeit des Schutzbedarfs, wie z. B. Diebstahlschutz, Installation von Software, Verhinderung der Einsehbarkeit auf Informationen selbst (Sichtschutz), Verwendung einer geschützten Umgebung (z.B. geschlossener Raum, kein öffentlicher Ort), Umgang mit Authentifizierungsmitteln.

Hierzu kann gehören:

Keine.

Zusätzlich bei hohem Schutzbedarf:

Keine.

Zusätzlich bei sehr hohem Schutzbedarf:

Keine.

Neben den Aspekten werden Reifegrade nach Level bewertet:

Reifegrade:

Der VDA ISA sieht vor, dass die Umsetzung mittels eines Reifegrad-Modells bewertet wird, die in diesem Tabellenblatt definiert werden.

Vereinfacht sind die Reifegrade wie folgt abgestuft:

Level 0: Die Umsetzung der Anforderungen ist unvollständig. Es existiert kein Prozess bzw. der Prozess erreicht nicht die erforderlichen Ergebnisse.

Level 1: *Die je nach Schutzbedarf der Informationen notwendigen Anforderungen sind durchgeführt. Ein Prozess existiert und lässt erkennen, dass er funktioniert. Er ist jedoch nicht vollständig dokumentiert. Es kann daher nicht sichergestellt werden, dass er immer funktioniert.*

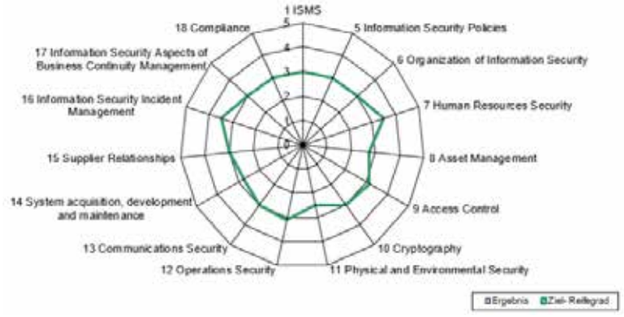
Level 2: *Der Prozess zur Erreichung des Ziels ist gesteuert. Er ist dokumentiert und Nachweise (z. B. Dokumentationen) sind vorhanden.*

Level 3: *Der Prozess zur Erreichung des Ziels ist etabliert, die Prozesse sind verknüpft, um existierende Abhängigkeiten abzubilden. Die Dokumentation ist aktuell und wird gepflegt.*

Level 4: *Anforderungen aus Level 3, darüber hinaus finden Messungen der Ergebnisse (z. B. KPI) statt und machen den Prozess somit vorhersagbar.*

Level 5: *Anforderungen aus Level 4, darüber hinaus werden zusätzliche Ressourcen (z. B. Personal und Geld) optimierend eingesetzt. Es findet eine kontinuierliche Verbesserung des Prozesses statt.*

Diese Reifegrade können dann durch den Anwender graphisch ausgewertet werden:



Ausblick: Arbeitskreis des BITKOM

Aktuell passt eine Arbeitsgruppe in des BITKOM einen entsprechenden toM-Katalog auf Basis internationaler Normen auf den Datenschutz an, mit den beschriebenen Zielen:

- Möglichkeit des risikoorientierten Einsatzes des toM-Kataloges
- Akzeptanz auch in der EDV-Abteilung für den Bereich der Informationssicherheit
- Rückgriff auf einen gut dokumentierten Maßnahmenkatalog
- Einfache Auswertung der Ergebnisse

Die Arbeitsergebnisse werden voraussichtlich im Herbst dieses Jahrs vorliegen.

Über den Autor

Stephan Rehfeld
Externer Datenschutzbeauftragter
der scope & focus Service-Gesellschaft mbH

▶ www.scope-and-focus.com

scope & focus
Service-Gesellschaft mbH

DATENSCHUTZPRAXIS

DAS NEUE DATENSCHUTZRECHT DER KATHOLISCHEN KIRCHE

Steffen Pau und Stephanie Melzow

Die Katholische Kirche in Deutschland wendet mit dem „Gesetz über den Kirchlichen Datenschutz (KDG)" ein eigenes Datenschutzrecht für die kirchlichen Stellen an. Sie hat – ebenso wie die Evangelische Kirche Deutschlands mit ihrem „Gesetz über den Datenschutz der Evangelischen Kirche in Deutschland" (DSG-EKD) – von der Möglichkeit des Art. 91 Abs. 1 DS-GVO Gebrauch gemacht und ein eigenes Datenschutzrecht für die kirchlichen Einrichtungen erlassen.

Trotz der Ähnlichkeiten zur DS-GVO sollten sich betriebliche Datenschutzbeauftragte mit den neuen Regelungen des KDG vertraut machen, da dieses Gesetz die Rechtsgrundlage in den kirchlichen Einrichtungen ist, für die sie benannt sind.

Rechtlicher Rahmen

Bis zum 24. Mai war in den kirchlichen Einrichtungen der Katholischen Kirche die „Anordnung über den kirchlichen Datenschutz (KDO)" anwendbar, die zusammen mit einigen Spezialregelungen die datenschutzrechtlichen Sachverhalte der kirchlichen Stellen regelte.

Damit die Kirchen im Bereich des Datenschutzes auch weiterhin ihr durch das Grundgesetz garantiertes Selbstbestimmungsrecht wahrnehmen können, ist in Art. 91 DS-GVO die Möglichkeit für die Kirchen enthalten, schon bestehende Datenschutzregelungen an die neuen Vorgaben der DS-GVO anzupassen und mit dieser „in Einklang" zu bringen. Dies ist mit der Überarbeitung der KDO zum neuen KDG geschehen.

Damit stellt das KDG zukünftig die Grundlage für den Umgang katholischer Einrichtungen mit personenbezogenen Daten dar.

Daneben gibt es nach § 57 KDG weitergeltende datenschutzrechtliche Regelungen der jeweiligen (Erz-)Diözese in anderen kirchlichen Gesetzen, soweit diese den Regelungen des KDG nicht entgegenstehen.

Grundlagen des KDG

Da sich das KDG im Einklang mit der DS-GVO befindet, sind auch die Grundlagen und Grundprinzipien des Datenschutzes in beiden Gesetzen gleich. Auf wenige Besonderheiten sei hier hingewiesen:

§ 2 Abs. 3 KDG erinnert daran, dass die Wahrung des Beicht- und Seelsorgegeheimnisses und anderer dort genannter Verschwiegenheitspflichten unberührt bleiben.

Der Anwendungsbereich des KDG bezieht in § 3 KDG alle kirchlichen Stellen ein, unabhängig davon, ob es sich um verfasst kirchliche Stellen (z.B. die Diözesen oder die Kirchengemeinden) oder um Einrichtungen der Caritas handelt. Auch kirchliche Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und sonstige kirchliche Rechtsträger ohne Rücksicht auf ihre Rechtsform sind vom Anwendungsbereich umfasst.

Bei den Begriffsdefinitionen sind die „besonderen Kategorien personenbezogener Daten" in § 4 Nr. 2 KDG definiert. Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft gilt dabei nicht als besondere Kategorie personenbezogener Daten (vgl. § 4 Nr. 2 Satz 2 KDG).

Bei der Einwilligung erscheint das KDG mit seinem Schriftformerfordernis in § 8 Abs. 2 Satz 1 KDG strenger als die DS-GVO, die in Art. 7 Abs. 1 DS-GVO vorgibt, dass der Verantwortliche die Einwilligung nachweisen können muss.

Inwieweit hier im täglichen Umgang mit der Einwilligung wirklich Unterschiede bestehen werden, wird sich zeigen. Zu beachten ist dabei aber, dass § 8 Abs. 2 Satz 1 KDG als Ausnahme von dem Schriftformerfordernis selbst „eine andere Form" der Einwilligung auf Grund besonderer Umstände vorsieht und die Nachweispflicht der DS-GVO wahrscheinlich in vielen Fällen auch zu einer textlichen oder schriftlichen Fassung der Einwilligung führen wird.

Betriebliche Datenschutzbeauftragte

Für den Bereich der verfassten Kirche sind nach dem KDG zwingend betriebliche Datenschutzbeauftragte zu benennen (vgl. § 36 Abs. 1 KDG). Die anderen kirchlichen Stellen haben einen solchen gemäß § 36 Abs. 2 KDG zu benennen, wenn entweder mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind oder die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, die eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Personen erfordern oder die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 KDG besteht.

Selbst für den Fall, dass keine gesetzliche Benennungspflicht eines betrieblichen Datenschutzbeauftragten besteht, hat der Verantwortliche die Erfüllung der datenschutzrechtlichen Vorgaben in anderer Weise sicherzustellen (§ 36 Abs. 8 KDG).

Die betrieblichen Datenschutzbeauftragten sind den Leitungen der Einrichtungen unmittelbar zu unterstellen, sind in ihrer Aufgabenwahrnehmung weisungsfrei und dürfen wegen der Erfüllung ihrer Aufgabe nicht benachteiligt werden, § 37 Abs. 1 KDG. Sie wirken auf die Einhaltung datenschutzrechtlicher Vorschriften hin. Um dies zu erreichen ist die Beratung des Verantwortlichen von großer Bedeutung. Außerdem gehört es zu den Aufgaben des betrieblichen Datenschutzbeauftragten, die Mitarbeiter, welche mit der Verarbeitung personenbezogener Daten beschäftigt sind, mit den Erfordernissen zur Einhaltung des Datenschutzes vertraut zu machen.

Für betroffene Personen ist der betriebliche Datenschutzbeauftragte stets unmittelbare Anlaufstelle (vgl. § 37 Abs. 3 KDG). Er genießt Kündigungsschutz nach § 37 Abs. 4 KDG soweit keine außerordentliche Kündigung in Betracht kommt. Der Verantwortliche stellt sicher, dass der betriebliche Datenschutzbeauftragte durch die Wahrnehmung anderer Aufgaben und Pflichten nicht in einen Interessenkonflikt gerät (vgl. § 37 Abs. 5 KDG).

Die betrieblichen Datenschützer unterstützen die Leitungen der Einrichtungen wie bisher bei der Erfüllung ihrer Pflichten zur Beachtung gesetzlicher Vorgaben. Damit die Datenschutzbeauftragten ihre Aufgaben erfüllen können, sind sie in die betrieblichen Prozesse und Informationsflüsse einzubinden. Um ihre Aufgaben, welche sich detailliert aus § 38 KDG ergeben, wahrnehmen zu können, bedarf es der bereits erwähnten Fachkunde. Um diese zu erwerben und zu erhalten sollte es den betrieblichen Datenschutzbeauftragten stets ermöglicht werden sich weiterzubilden.

Meldung an die Datenschutzaufsicht

Sofern zukünftig Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten auftreten, sind diese unter den Voraussetzungen des § 33 KDG an die Datenschutzaufsicht zu melden. Die möglicherweise notwendige Meldung des Sachverhaltes an die betroffenen Personen regelt § 34 KDG. Hier stellen die Diözesandatenschutzbeauftragten auch die Möglichkeit zur Meldung der Sachverhalte über deren Internetseiten bereit. ▸

Auftragsverarbeitung

Schließt eine kirchliche Einrichtung einen Auftragsverarbeitungsvertrag, so hat sie ihre Pflichten in den Vertrag einzubringen. Dies bedeutet, dass im Vertrag auf die Regelungen des KDG Bezug genommen wird. Sollte der nichtkirchliche Auftragnehmer der Auftragsverarbeitung eine rein KDG-bezogene Auftragsverarbeitungsregelung nicht mittragen, so sind lösungsorientierte Wege zu suchen, den Verpflichtungen beider Vertragspartner gerecht zu werden.

Datenschutzaufsicht

Die Katholische Kirche hat eigene Datenschutzaufsichtsbehörden im Sinne von Art. 91 Abs. 2 DS-GVO mit den Diözesandatenschutzbeauftragten an der Spitze eingerichtet.

Die kirchlichen Datenschutzaufsichten sind im KDG für ihren Zuständigkeitsbereich mit vergleichbaren Befugnissen ausgestattet wie die Landesdatenschutzbeauftragten. Sie beraten die kirchlichen Einrichtungen, bearbeiten Beschwerdefälle und führen Prüfungen in den kirchlichen Einrichtungen durch.

Dabei haben immer mehrere (Erz-)Diözesen einen gemeinsamen Diözesandatenschutzbeauftragten bestellt. Daneben hat die Deutsche Ordensobernkonferenz zwei gemeinsame Ordensdatenschutzbeauftragte für die Aufsicht über die päpstlichen Orden in Deutschland bestellt. Eine aktuelle Liste mit den Anschriften der Diözesandatenschutzbeauftragten ist auf der folgenden Seite hinterlegt: www.dbk.de (Über uns > VDD > Dokumente)

Rechtsweg

Jede natürliche oder juristische Person hat die Möglichkeit gegen einen sie betreffenden Bescheid der Datenschutzaufsicht den gerichtlichen Rechtsweg zu beschreiten (vgl. § 49 KDG). Ebenso kann eine nicht mit dem KDG in Einklang stehende Verarbeitung von personenbezogenen Daten gerichtlich überprüft werden, wenn die nach dem Gesetz zustehenden Rechte der betroffenen Person verletzt wurden.

Einzelheiten zum Gerichtsverfahren regelt die „Kirchliche Datenschutzgerichtsordnung (KDSGO)". Diese Gerichtsordnung sieht ein Gericht erster Instanz (das Interdiözesane Datenschutzgericht) und ein Gericht zweiter Instanz (das Datenschutzgericht der Deutschen Bischofskonferenz) vor und regelt die Einzelheiten zur Einleitung und Durchführung des Verfahrens vor diesen Gerichten.

Fazit

Das kirchliche Datenschutzrecht ist mit der EU-Datenschutz-Grundverordnung in Einklang gebracht worden. Es bestehen im Detail Unterschiede, die in der täglichen Arbeit beachtet werden müssen.

Als extern benannter betrieblicher Datenschützer können viele Kenntnisse aus dem Bereich der DS-GVO bei der Bearbeitung von Sachverhalten nach dem KDG herangezogen werden.

Die Diözesandatenschutzbeauftragten stellen über ihre Internetseiten viele Informationen, Praxishilfen, Formulierungshilfen, Checklisten und Muster zum kirchlichen Datenschutz zur Verfügung. Sie beantworten im Rahmen ihrer beratenden Tätigkeit auch gerne Fragen der betrieblichen Datenschutzbeauftragten.

Hinweis auf Praxishilfen/Arbeitshilfen/Muster:

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands gibt eine Schriftenreihe „Praxishilfen" zum Umgang mit den Bestimmungen des neuen KDG heraus. Derzeit sind 16 Themen der Schriftenreihe veröffentlicht. Aktuell sind 18 Broschüren zu den zentralen Themen des KDG vorgesehen. Sie sollen als erste Orientierung dienen, wie nach Auffassung der Diözesandatenschutzbeauftragten das neue Gesetz in der Praxis angewendet werden sollte. Die Broschüren stehen zum Download auf der Homepage des Katholischen Datenschutzzentrums unter Infothek zur Verfügung:

www.katholisches-datenschutzzentrum.de

Außerdem erweitert das Katholische Datenschutzzentrum das Informationsangebot auf der Homepage ständig. Zum Beispiel findet sich dort eine Liste mit häufig gestellten Fragen rund um das Thema KDG und weitere Informationen in Arbeitshilfen oder Mustern.

Über die Autoren

Steffen Pau

Jurist, Leiter des Katholischen Datenschutzzentrums in Dortmund und Diözesandatenschutzbeauftragter für die nordrhein-westfälischen (Erz-)Bistümer.

Stephanie Melzow

Juristin, Referentin im Katholischen Datenschutzzentrum Dortmund

- info@kdsz.de
- www.katholisches-datenschutzzentrum.de

Katholisches Datenschutzzentrum

29

PRIVACYSOFT

Die modulare Software-Plattform für alle Aufgaben im Datenschutzmanagement.

DAS DSB-MULTI-TOOL
FÜR DEN DATENSCHUTZ NACH EU-DSGVO

Datenschutzdokumentation | Vorlagen und Checklisten | Vorgangsmanagement | Online-Schulungen

Datenschutz Know-how seit 1996

Projekt 29 GmbH & Co. KG | Ostengasse 14 | 93047 Regensburg | www.privacysoft.de

Privacysoft ist eine Marke von Projekt 29 GmbH & Co. KG

DATENSCHUTZPRAXIS

SESSION TRACKING: SO KÖNNEN IHRE USER „MAN-IN-THE-MIDDLE-ATTACKEN“ STOPPEN

Dennis Okpara, Al Lakhani, Calvin Hoenes, Dr. Daniel Schellenberg

Zusammenfassung

Fragen Sie sich auch immer mal wieder wie Sie Ihr Identitäts- und Authentifizierungs-Management auf das höchste Sicherheits-Niveau bringen? Das ist nicht ganz einfach, insbesondere wenn Sie eine Vielzahl von Usern haben, da Sie diese nicht alle gleichzeitig aktiv schützen können. Was, wenn jemand Ihren Usern die Zugangsdaten „weg-phisht“? Oder was tun Sie, wenn einer Ihrer User Opfer einer sogenannten „Man-in-the-Middle-Attacke“ (MitM-Attacke) wird? Und was passiert, wenn Ihr Zugangsmanagement nicht den strengen Richtlinien wie bspw. der DS-GVO entspricht?

Viele Unternehmen stellen von 1-Faktor-Authentifizierung (1FA) auf Multi-Faktor-Authentifizierung (MFA) um, um Richtlinien wie bspw. der DS-GVO zu entsprechen und Hackerangriffe besser abwehren zu können. Das ist grundsätzlich ein guter Schritt. Aber wenn sich nun doch jemand bei Ihnen „einhackt“, wäre es dann nicht großartig, wenn Ihre User das selber feststellen könnten und dann auch noch diese Verbindung des Hackers unterbrechen könnten? Genau das ermöglicht Session Tracking. Und deshalb ist MFA mit Session Tracking der einfachen MFA ohne Session Tracking weit überlegen. Durch MFA mit Session Tracking – auch “kontinuierliche MFA” – wird sowohl der Zugangspunkt Ihrer User gesichert als auch jede einzelne Session kontrollierbar gemacht. Somit können Sie „Man-in-the-Middle-Attacken“ (MitM-Attacken) stoppen.

Dieser Artikel erklärt was Session Tracking ist und warum Sie es zusammen mit MFA einsetzen sollten, um „kontinuierliche MFA“ zu erreichen.

Multi-Faktor-Authentifizierung (MFA): was ist das eigentlich?

MFA ist nach der Definition von NIST „ein Authentifizierungssystem, das mehr als einen Faktor zur erfolgreichen Authentifizierung einsetzt.“[1] Dabei gibt es 4 unterschiedliche Authentifizierungsfaktoren:

1. Wissen (z.B. Ihr Passwort, also etwas, was Sie wissen),
2. Besitz (z.B. Ihr Smartphone, also etwas, was Sie haben),
3. Inhärenz oder Biometrie (z.B. Ihr Fingerabdruck also etwas, was Sie sind) oder
4. ein kontextabhängiges Attribut (z.B. ein Ort, an dem Sie sich gerade aufhalten wie bspw. ein bestimmtes Bürogebäude).

Wenn Sie als User lediglich einen Faktor zur Authentifizierung verwenden müssen, also bspw. die Eingabe eines Passwortes, um sich in Ihrem PC einzuloggen, ist dies eine 1-Faktor-Authentifizierung (1FA). Wenn Sie mehrere Faktoren einsetzen müssen, handelt es sich um 2-Faktor- oder Multifaktorauthentifizierung. Ein Bsp. für Multi-Faktor-Authentifizierung (MFA) ist, wenn Sie zusätzlich zur Eingabe Ihres Passwortes bspw. einen 6-stelligen Token per SMS erhalten und diesen ebenso eingegeben müssen.

Warum ist Session Tracking so effektiv?

Session Tracking ist die Fähigkeit, eine aktivierte Session (oder Verbindung) zu kontrollieren. D.h. die Anwenderin kann sehen welche Verbindungen aktiv sind und kann außerdem auf mögliche Ereignisse reagieren. Bspw. könnte ein User eine Verbindung, manchmal sogar fernbedient, beenden. Dies kann dann wertvoll sein, wenn ein User eine Verbindung erkennt, die nicht durch ihn selbst gestartet wurde. Somit kann eine durch einen Hacker aktivierte Verbindung sofort unterbrochen werden und so möglicherweise ein großer Schaden für den User oder den Serviceanbieter abgewendet werden. Dies ist ohne Session Tracking nicht möglich. Ein Hacker könnte sich Ihre Zugangsdaten stehlen und dann unbemerkt in Ihrem Account agieren. Selbst wenn Sie es bemerken würden, haben Sie als User ohne Session Tracking keine Möglichkeit die Verbindung des Hackers sofort zu unterbrechen. Session Tracking ermöglicht auch dies. Bei der Kombination von MFA mit Session Tracking spricht man von „kontinuierlicher MFA“. Ein Beispiel für eine kontinuierliche MFA ist IDEE OneClick (www.getidee.de). Bei dieser Lösung kann die Anwenderin sich sicher einloggen (Webseite oder mobile App) und jede Session beobachten und auch mit ihrem Handy wieder fernbeenden.

Welche Typen von Session Tracking gibt es?

Man kann Session Tracking in 3 Typen einordnen: Physisches Session Tracking, In-System Session Tracking und fernbedientes Session Tracking.

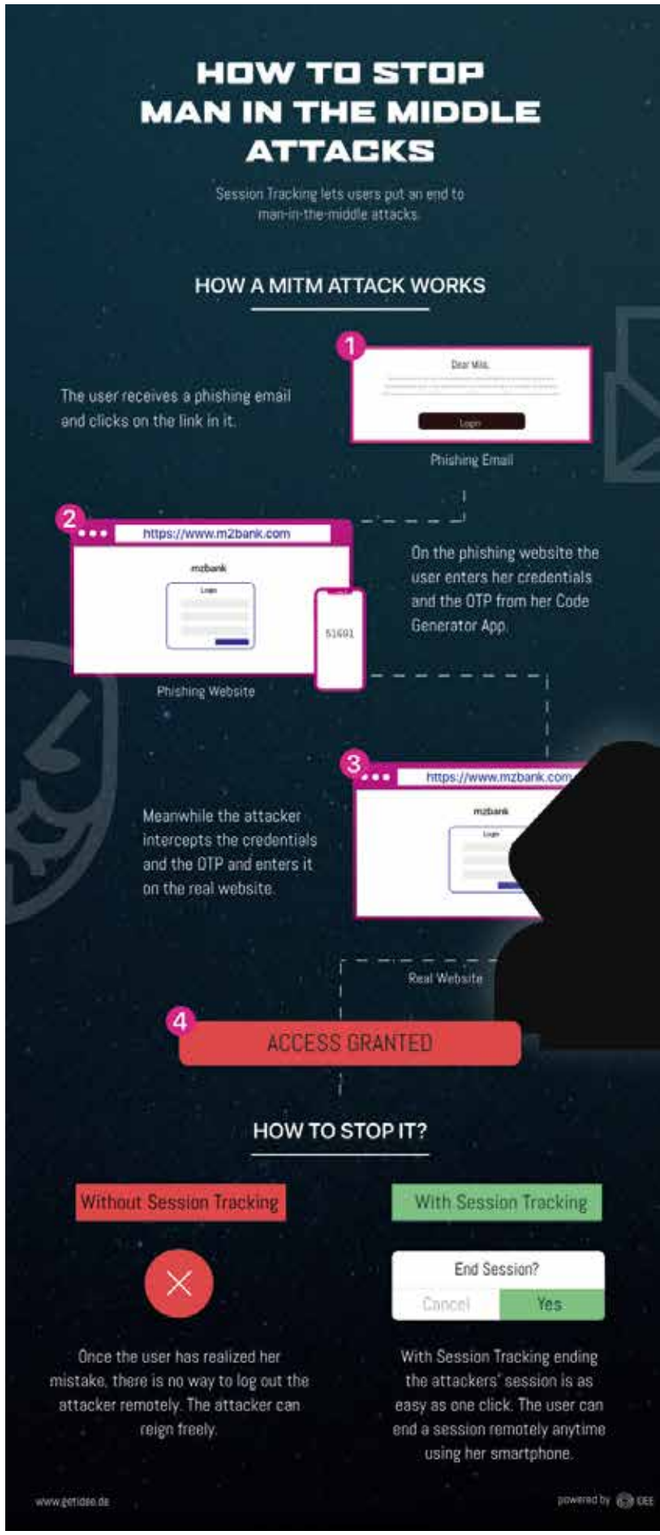
Physisches Session Tracking sind solche Lösungen, die voraussetzen, dass ein Hardware-Token aktiviert bleibt. Bspw. der Einsatz einer Smart Card für das PC-Login, bei der die Smartcard mit dem PC authentifiziert verbleiben muss. Sobald die Smartcard entfernt wird, wird die Session beendet.

In-System Session Tracking sind die Lösungen bei denen die Anwenderin sich in einen Webservice wie bspw. Facebook einloggen muss, bevor sie die authentifizierte aktive Session sehen und verwenden kann.

Fernbedientes Session Tracking sind die Lösungen, bei denen die Anwenderin eine Session tracken und beenden kann, ohne physisch mit dem System verbunden zu sein. Fernbedientes Session Tracking ist die einzige Kategorie, bei der die Anwenderin einen unautorisierten Zugriff sofort bemerken und darauf reagieren kann. Insbesondere können durch fernbedientes Session Tracking Phishing-Angriffe vermieden sowie Man-in-the-Middle-Attacken gestoppt werden.

MFA – Sicherheitsschwächen und -risiken

Session Tracking erhöht die Sicherheit von ▸



[1] https://pages.nist.gov/800-63-3/

Verbindungen immens.Ohne Session Tracking können MFA-Lösungen auf herkömmliche Art und Weise gehackt werden. Hardware Token, Software Token / Einmalpasswörter, Push-Benachrichtigungen, Smartcard, Biometrie, FIDO U2F und kontextbasierte Lösungen sind ohne sicheres Session Tracking verwundbar.

Die meisten Faktoren können auf herkömmliche Weise relativ einfach durch Social Engineering wie Phishing oder Spear-Phishing, Keylogger, Screen Capture, MitM-Attacken, Diebstahl oder durch Ausnutzen von Schwächen in der Authentifizierungslösung kompromittiert werden.

Vorteile von Session Tracking in Kombination mit MFA: „kontinuierliche MFA“

Session Tracking ist eines der wichtigsten Sicherheits-Features, die jede MFA-Lösung anbieten sollte, um den „State of the Art“ an Sicherheitsniveau zu erreichen. Session Tracking bietet der Anwenderin nicht nur die nutzerfreundlichen Möglichkeiten, ihre Session zu monitoren und fernbedient zu beenden, sondern Session Tracking ist die aktuellste und einzige Methode Phishing und Man-in-the-Middle-Attacken zu blockieren. Ohne Session Tracking kann eine Anwenderin gar nicht feststellen, ob ihre Zugangsdaten gestohlen wurden und fremd eingesetzt werden. Mit herkömmlichen Lösungen kann die Anwenderin nicht einmal zu dem Zeitpunkt, zu dem sie feststellt, dass eine verdächtige Aktivität in ihrem Konto stattfindet, etwas unternehmen, um diese bösartige Attacke zu stoppen oder zu blockieren.

Die Autoren dieses Artikels empfehlen für hohes Sicherheitsniveau den Einsatz von kontinuierlicher MFA, also dem Einsatz von Session Tracking in Kombination mit MFA.

IDEE OneClick mit kontinuierlicher MFA

IDEE GmbH bietet starke Authentifizierung & Blockchain-Identitäts-Lösungen. IDEEs starke Authentifizierungslösung heißt IDEE OneClick. Mit IDEEs OneClick und der kontinuierlichen MFA haben User immer Kontrolle über ihre Sessions. Die Anwenderin kann entscheiden, welches Device den Zugang autorisieren kann. Ebenso kann sie unautorisierten Zugang sofort in Echtzeit feststellen und kann sowohl Phishing- als auch Man-in-the-Middle-Attacken sowie Replay-Attacken blockieren.

Dieser innovative Ansatz von IDEE zur sicheren Authentifizierung ermöglicht während einer gesamten Session immer das gleiche, höchste Niveau an Sicherheit, Anwenderfreundlichkeit und Privatsphäre. Dies wird u.a. erreicht, weil IDEE Passwörter, Benutzernamen und Tokens komplett ersetzt.

IDEE OneClick unterstützt Challenge-Response-Verfahren, digitale Logon-Zertifikate, sichere PUSH-Authentifizierung, „on-the-fly-one-time-key-Erstellung“ (OTK), ohne dabei die geheimen Schlüssel oder „Seeds“ auf dem Authentifizierungs-Server oder auf dem Smartphone zu speichern. Das bedeutet, dass in dem ungewöhnlichen Fall einer Datenschutzverletzung des Authentifizierungsservers oder der OneClick-App keine Anwender-Geheimnisse exponiert werden würden.

Mit IDEE OneClick wird das Risiko der unsicheren Speicherung von Anwenderschlüsseln auf dem Authentifizierungsserver eliminiert. Die Anwenderin kontrolliert ihre Daten immer vollständig selbständig.

Keine Passwörter! Keine Benutzernamen! Keine Tokens!

Lernen Sie mehr über starke Authentifizierung, sichere Autorisierung & Blockchain-Identität auf www.getidee.de.

[2] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[3] http://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

[4] https://www.silicon.co.uk/security/ss7-flaw-banks-211127?utm_source=2017-05-05&rutm_medium=email&rutm_campaign=uk_silicon&referrer=nl_uk_silicon&rt=s5bd57d24df776266acbacb29d2994419183528rp0s=content-regular_4_textContent&inf_by=5791b32bdf1911250occb4c2

[5] https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/

[6] https://pages.nist.gov/800-63-3/

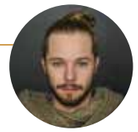
[7] https://breakdev.org/evilginx-advanced-phishing-with-two-factor-authentication-bypass/

[8] https://www.onelogin.com/blog/may-31-2017-security-incident

Über die Autoren

Dennis Okpara
Security Engineer, IDEE GmbH. Dennis hat einen Masterabschluss in Information Security von der Royal Holloway, University of London.

Al Lakhani
CEO & Gründer der IDEE GmbH. Vorher gründete und führte Al die Forensic Investigation Practice bei Alvarez & Marsal weltweit. Er arbeitete auch für E&Y und PWC. Al hat an der Universität von Texas in Austin Computer Science studiert.



Calvin Hoenes
UX Engineer, IDEE GmbH. Calvin hat einen Bachelorabschluss von der LMU in München in Computer Science.

Dr. Daniel Schellenberg
VP Germany der IDEE GmbH. Arbeitete früher bei der Adcuram Group, Alvarez & Marsal und Roland Berger Strategy Consultants mit einem Fokus auf Restrukturierung und Value Enhancement für Private Equity Portfoliounternehmen. Daniel studierte an der ebs in Oestrich-Winkel und promovierte an der Universität zu Potsdam.

▶ www.getidee.de

Welche technischen Schwachstellen haben Authentifizierungs-Faktoren?

Passwörter können durch Brute-Force-Angriffe überwunden werden oder mit Hilfe von Sniffing, Social Engineering, Malware oder sogar durch Diebstahl vom Backend des Service Providers geknackt werden. Verizons „2017 Data Breach Investigation Report“[2] stellt fest, dass 81% aller Datenschutzverletzungen in 2017 entweder durch gestohlene oder schwache Passwörter verursacht wurden.
SMS wurde als Methode einen Authentifizierungscode durch den „Signalling System #7-Breach“ (SS7) als unsicher gebrandmarkt[3/4], als die SMS zu einer durch Hacker kontrollierte Nummer umgeleitet wurde. Außer dem SS7-Breach kann eine SMS durch eine bösartige App auf einem Mobiltelefon gelesen werden. „Spear Phishing“ kann wie beim durchgesickerten NSA-Report[5] dazu eingesetzt werden, den Code von der Anwenderin zu bekommen. Außerdem können SMS sogar auf einem gesperrten Telefon gelesen werden. Deshalb hat NIST SMS in ihren Digitalen Identitätsrichtlinien[6] als unsicherer herunter gestuft.
Tokens / Einmal-Passwörter (EP) sind für unterschiedliche Attacken anfällig. Bei der Eingabe des Einmal-Passworts (EP) auf dem Webservice kann es durch Phishing, Man-in-the-Middle-Attacken, Keylogger oder Screen Capture abgefangen werden. Das von Kuba Gretzky entwickelte Evilginx[7] ist ein Beispiel hierfür. Ebenso kann der Schlüssel zur Erstellung des gemeinsamen Schlüssels, den man zur Erstellung eines EPs benötigt, kann ebenso gestohlen werden. Außerdem besteht das Risiko, dass ein EP vom Backend eines Service Providers entwendet wird wie bspw. im OneLogin-Breach[8].
Biometrische Authentifikatoren können zwar schwieriger gestohlen werden, bieten aber auch einige Sicherheitslücken für Hacker. Falls eine biometrische Authentifizierung fehlschlagen sollte, ermöglichen es die meisten biometrischen Authentifizierungslösungen, mit Hilfe eines Passwortes oder eines Recovery Keys ein Konto wieder herzustellen. Manchmal wird als alternativer Faktor eine registrierte Emailadresse oder eine Telefonnummer verlangt. Da in diesem Fall dieser alternative Faktor eingesetzt wird, um den biometrischen Faktor zurückzusetzen, hängt das Sicherheitsrisiko von der Sicherheit des Recovery Keys ab. Falls der Recovery Key in Form eines Passworts, eines SMS-Codes, einer Email oder ähnlichem eingesetzt wird, handelt es sich zwar um eine nutzerfreundliche, aber unsichere Lösung. Dann bestehen nämlich die oben beschriebenen Schwachstellen.
Auch der Einsatz eines *FIDO U2F Hardware Tokens* als zweiten Faktor kann diese Probleme aufweisen. Beim U2F wird die Domain der Anwenderin geprüft. Ein Angreifer könnte einen gestohlenen U2F Token einsetzen, falls der erste Faktor, wie bspw. ein Passwort, abgefangen wird, um so Zugang zum Konto der Anwenderin zu bekommen.
In jedem der oben beschriebenen Fälle erhält eine Anwenderin Zugang zu bspw. einer Webseite oder einem PC, wenn die unterschiedlichen Faktoren erfolgreich validiert werden. Allerdings ist es für die Anwenderin nicht möglich festzustellen, ob ein kompromittierter Faktor eingesetzt wurde, d.h. ein Faktor, der von einem Hacker manipuliert wurde. Anders ausgedrückt, obwohl MFA den Hackern das Handwerk erschwert, kann MFA weder Phishing- noch Man-in-the-Middle-Attacken stoppen.

AUFSICHTSBEHÖRDE

DATENSCHUTZ MACHT SELBSTBEWUSST

Kinder fordern besseren Datenschutz für ihre Generation

Mehr Kinderangebote im Internet ohne Werbung und Suchmaschinen für Kinder - das sind zwei Forderungen, die Schülerinnen und Schüler der Kastanienbaum-Grundschule aus Berlin nach einem Workshop aufstellten. Auf der Dialog-Konferenz „Datenschutz für Kinder“ wiederholten sie ihre Forderungen – und stellten an die Fachleute jede Menge weiterer Fragen, zum Beispiel: „Warum sammeln Unternehmen überhaupt Daten?“

Zu der Konferenz unter dem Motto „Ich sehe Daten, die Du nicht siehst …“ hatte die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, mit dem BvD, dem Verein „Deutschland sicher im Netz“ und dem Institut für Medienforschung und Medienpädagogik der Technischen Hochschule Köln am 3. Juli in der Landesvertretung Niedersachsen beim Bund geladen.

Im Mittelpunkt standen bei aller Datenschutz- und Digital-Kompetenz der Fachleute die rund 60 Schülerinnen und Schüler, die sich in einem Projekttag auf den Tag vorbereitet und dabei viel gelernt hatten. „Ich wusste nicht, dass WhatsApp zu Facebook gehört“, sagte die 11-jährige Kalina. Aber selbst wenn sie jetzt ihren Account löschen würde - „blieben meine Daten wahrscheinlich weiter gespeichert“, sagt sie. Sie und ihre Klassenkameradinnen fanden den Projekttag wichtig – und toll, dass sie zur Veranstaltung, durch die „Wissen macht Ahh“-Moderator Ralph Caspers geführt hatte, eingeladen worden waren.

Alita darf mit ihren zehn Jahren noch kein WhatsApp benutzen, das haben ihr die Eltern verboten. Sie behilft sich unter anderem mit dem sozialen Video-Dienst HangOut. Nach dem Workshop im Rahmen der BvD-Initiative „Datenschutz geht zur Schule“ ist sie gar nicht mehr so sicher, ob sie WhatsApp überhaupt noch will. Die gleichaltrige Bele hat zwar kein Smartphone, sitzt aber dennoch täglich am Computer ihrer Eltern – oder an der Playstation.

Kalina, Alita und Bele haben Eltern und teils ältere Geschwister, die nach Einschätzung der Kinder in Sachen Datenschutz fit sind. Das ist nicht selbstverständlich. Für den Leiter der Deutsch-Skandinavischen Gemeinschaftsschule Berlin, Jacob Chammon, sind die Eltern sogar die „schwierigsten Partner“ im Netzwerk der Datenschutz-Erziehung. Sie statten ihre Kinder mit Handies und Smartphones aus, aber die Schule solle die Aufklärung über Datenschutz und digitale Entwicklung leisten, kritisierte er. Dabei müssten alle daran arbeiten, Kinder zu kritischen, bewussten und mündigen Nutzern der neuen Medien zu entwickeln.

BvD-Mitglieder besuchen seit 2009 ehrenamtlich im Rahmen der Initiative „Datenschutz geht zur Schule“ Klassen ab Stufe 5 sowie berufsbildende Schulen. Sie klären darüber auf, wie die Kinder und Jugendlichen sich vor Datenklau und Datenmissbrauch schützen und mit der Verarbeitung ihrer personenbezogenen Daten umgehen können. Seit Jahren steigt die Nachfrage nach Sensibilisierungsveranstaltungen, „aber wir können das nicht mehr stemmen“, sagte BvD-Vorstandsvorsitzender Thomas Spaeing auf dem Podium. Er plädierte für eine Verstetigung von Medienbildung und Datenschutz im Unterricht, für entsprechende Weiterbildungen für Lehrkräfte und eine bessere Ausstattung an den Schulen.

Die ehrenamtlichen Dozenten der Initiative „Datenschutz geht zur Schule“ des BvD lieferten mit den speziell für die Schulen aufbereiteten Materialien eine „Inspiration“, sagte der Medienbeauftragte der Kastanienbaum-Grundschule, Alexander Baldus. „Allerdings müssten sie an die Bedürfnisse und Bedingungen der jeweiligen Klassen angepasst werden.“

Auch seiner Erfahrung nach „wissen die Eltern oft gar nicht Bescheid“. Deshalb schweben ihm Eltern-Schüler-Abende zum Thema Datenschutz per Smartphone, Tablet und Computer vor. Und er ist hoffnungsvoll, dass in einigen Jahren das Thema Datenschutz und Umgang mit Daten Eingang in die Rahmenlehrpläne finden werde.

Seine Schülerinnen und Schüler nahmen derweil in den Pausen an einer „Datenschutz-Rallye“ teil, an Stationen, wo sie ihr Wissen testen, Passwörter checken und Fotos fürs Internet auswählen konnten. Dabei zeigten sich die Kinder und Jugendlichen durchaus versiert. Das beeindruckte auch Andrea Voßhoff.

Die Konferenz habe viel mehr gebracht, als sie erhofft hatte, sagte sie zum Abschluss. Eine Konferenz zum Thema „Datenschutz für Kinder“ sei unter der Mitwirkung von Kindern „genau das Richtige“ gewesen. Durch die intensive Vorbereitung an den Schulen sei bei dem Thema „viel mehr rausgekommen, als wir es theoretisch auf einer Tagung hätten diskutieren können“. Besonders hob sie die Forderungen der Schülerinnen und Schüler nach mehr Datenschutz für Kinder im Internet hervor – und ihren Wunsch, sich bei Problemen an Ansprechpartner werden zu können.

Dass Jungs übrigens in Sachen Internet und Datenschutz mehr wüssten als Mädchen, weisen Kalina, Alita und Bele weit von sich. „Nee, echt nicht“, sagt Bele selbstbewusst. Und Kalina fühlt sich mittlerweile in Sachen Datenschutz kompetenter als ihr älterer Bruder.

BvD-News Redaktion

Foto: ©DSIN (Deutschland sicher im Netz)

AUFSICHTSBEHÖRDE

DER SPUR DER DATEN FOLGEN

„Projekt Freiheit 2.0“ in Stuttgart

Baden-Württembergs Datenschutzbeauftragter Stefan Brink und der Konzept-Künstler Florian Mehnert realisierten in Stuttgart die Kunstinstallation „Freiheit 2.0“. Mit einer Tracking-App und dazugehöriger Ausstellung, einer bunten „Datenspur“ durch die Innenstadt, der Umfirmierung von Geschäften und einem Symposium luden sie Bürger und Verbraucher ein, über Freiheit im Zeitalter von Big Data zu diskutieren. Der BvD war als Partner und Sponsor mit dabei.

Für Kinder war sie eine Roller-Bahn, für Radfahrer Wegemarkierung und für viele Erwachsene eine ungewohnte bunte Spur durch Stuttgarts belebtes Gerberviertel. Die farbigen Kreidespuren auf den Bürgersteigen liefen von 26 Geschäften, die auf ihren Firmenschildern den Namen „Freiheit“ trugen sowie von der katholischen Kirche St. Maria auf den Hauptstraßen zusammen und führten als breite Kreidebahn zum Kunst- und Kulturort StadtPalais.

Brink und sein Team hatten vor der Eröffnung des Partizipations-Projekts am 2. Juni die Kreidebahnen mit Künstler Florian Mehnert früh morgens aufgemalt. 50 Kilometer Farbstreifen zeichneten sie auf die Bürgersteige. Dabei kamen sie mit vielen Passanten und Geschäftsleuten ins Gespräch.

> *„Das war schon eine tolle Gelegenheit, mit den Anwohnern über Datenströme und Datenspuren im Internet zu sprechen“, sagte Brink.*

Der Austausch, die Teilhabe der Stuttgarter und aller Menschen, die sich für die Spuren, die wir täglich per Smartphone oder Computer im Internet hinterlassen, stand im Mittelpunkt des Kunst-Projekts, dass gleich vier Opitonen zum Mitwirken anbot. Mehnert hatte zum einen eine Self-Tracking-App entwickelt, mit der Interessierte anonymisiert ihre täglichen Wege aufzeichnen lassen konnten. Diese Wege projizierte er auf eine Karte, die er online unter

freiheit2-0.de/Tracking.html

veröffentlichte. Im StadtPalais projezierte er die Karten als Installation auf drei Leinwände, wo sie als abstrakte Formen und Muster sichtbar wurden.

Zudem gewann Mehnert 26 Geschäfte für das Projekt. Für sie entwickelte er Firmenschilder nach dem bestehenden Design, ergänzte sie jedoch um den Begriff „Freiheit“ im Firmennamen. So entstanden „Möbel für Freiheit“, ein „Barber Shop of Freedom“, ein Kino der Freiheit und eine „Drogerie der Freiheit“. An der Kirche St. Maria wehte die Fahne des Projekts „Freiheit 2.0“, „weil wir einen Raum für das Aushandeln von Partizipationsprozessen anbieten wollen“, wie Pastoralreferent Andreas Hofstetter-Sttraka sagte.

Die Schilder waren erst auf den zweiten Blick erkennbar. Mehnert ging es um eine „subtile Veränderung“, wie er den BvD News sagte. Wie die Datenspuren selbst sei die Veränderung nahezu unsichtbar und dennoch bezeugten sie eine „einschneidende Veränderung“.

Mit seinem Kunst-Konzept rannte Mehnert in Stuttgart offene Türen ein. Brink und er kennen sich bereits seit 2015. Als Brink nach seinem Amtsantritt in Stuttgart Datenschutz zum „Kulturgut“ ausrief, erinnerte er sich an Mehnerts Ansatz, mit Kunst Menschen zur Reflexion über Datenschutz und Datenströme anzuregen.

> *„Bei der Umstellung auf die Datenschutz-Grundverordnung (DS-GVO) informierten wir vor allem Unternehmen, Verbände und Vereine“, sagte Brink. „Aber die Bürgerinnen und Bürger, für die die neuen Regeln eigentlich gemacht wurden, kamen dabei eindeutig zu kurz“, sagte er vor der Eröffnung des Projekts.*

Deshalb sei er von Anfang an von dem Partizipationsprojekt begeistert gewesen. Auch das Kulturamt und das StadtPalais als zentraler Veranstaltungsort zogen mit. Und der (BvD).

Er unterstützte „Freiheit 2.0“ als Sponsor und mit einem Vortrag von BvD-Vorstandsvize Jürgen Hartz unter dem Titel „Nicht alles was geht - geht!“ über die Grenzen und datenschutzkonforme Anwendungen von Mitarbeiter-Überwachung und Compliancefragen.

> *„Datenschutz will keine Entwicklungen verhindern, sondern die Beteiligten beraten und bei der datenschutzkonformen Umsetzung unterstützen, damit für Verbraucher und Wirtschaft kein Schaden entsteht“, sagte Hartz.*

Das unterstrichen auch Brink und Mehnert.

> *„Wir wollen keine politische Diskussion über Datenschutz, sondern wir wollen die Menschen unterstützten, sich selbst eine Meinung zu bilden und über Datenschutz, Datenströme und Datenspuren im Internet zu refkletieren“, sagte Mehnert.*

Bei den Bürgerinnen und Bürger Stuttgarts zumindest stieß die Aktion auf breite Beteiligung.

> *„Das zeigt, dass die Information darüber, was mit unseren Daten passiert, noch viel intensiver werden muss“, sagte Brink.*

Und Mehnert ergänzt:

> *„Datenschutz braucht Demokratie und ein neues Ausverhandeln unserer persönlichen Freiheiten vor dem Hintergrund von Big Data und seinen Geschäftsmodellen.“*

Brink: „Datenschützer sind keine Technologie-Feinde“ (Interview)

Datenschutz greifbar und Datenströme sichtbar machen - das war das Ziel des Projekts Freiheit 2.0, das Baden-Württembergs oberster Datenschützer Stefan Brink gemeinsam mit dem Konzeptkünstler Florian Mehnert in Stuttgart realisierte. Neben Vorträgen, Diskusions-Panels und Formate mit Bürgerbeteiligung führten vom 2. bis 24. Juni bunte Leitlinien durch die Stadt zum Hauptveranstaltungsort, dem Stuttgarter StadtPalais. 26 Unternehmen und eine Kirche nahmen teil.

Die Aktion verstand sich als Kunstinstallation mit begleitenden Kolloquium, „denn über Kunst lässt sich das abstrakte Thema Datenschutz viel besser transportieren als über eine Behörde“, sagte Brink im Interview mit den BvD-News. Er hatte den baden-württembergischen Konzeptkünstler Florian Mehnert bereits 2015 kennengelernt, gemeinsam entwickelten sie das Konzept für Freiheit 2.0.

> *„Wichtig war, die Themen Datenschutz, Big Data oder Datenschutz-Grundverordnung nicht aus Sicht der Verantwortlichen, sondern aus der Perspektive der Betroffenen und Verbraucher anzubieten“, sagt Brink.*

Für ihn ist Datenschutz ohnehin ein Kulturgut, dass in unterschiedlichen Kulturkreisen ganz anders verstanden wird. „Auch wie Datenschutz praktiziert wird, ist eine Frage des kulturellen Kontextes“, sagte Brink. So sei die Videoüberwachung öffentlicher Räume in den USA wenig strittig, weil dort die Frage der Privatheit sich auf das eigene Haus oder die eigene Wohnung als Rückzugsort des Invididuums bezöge. In Deutschland hingegeben gebe es die Vorstellung einer Privatheit im öffentlichen Raum. ▸

Foto: © Christina Denz

Deshalb werde hierzulande die Aufzeichnung von Videos an öffentlichen Plätzen ganz anders wahrgenommen.

Brink selbst zog mit Mehnert und seinem Team aus und malte die bunten Linien in Stuttgart am frühen Morgen auf.

> *„Das war eine tolle Gelegenheit, mit den Menschen ins Gespräch zu kommen und zu erklären, dass Datenschutz für sie gemacht ist - nicht als Technik-Verhinderer", sagte er.*

Wichtig ist für Brink, sich mit den neuen Kommunikationsformen etwa in den Sozialen Medien auseinanderzusetzen und den Nutzern Hilfestellungen und Tipps zu geben. „Wir Datenschützer sind keine Bilderstürmer", sagt er. Es gehöre zur informationellen Selbstbestimmung der Menschen aller Altersgruppen, zu entscheiden, welche Kommunikationsformen sie wählten. „Dabei wollen wir die Leute unterstützten, dass sie dort nicht in Datenschutz-Fallen tappen."

BvD-News Redaktion

Foto: © Christina Denz

Weiterführende Informationen auf der BvD-Website oder im BvD-Blog unter:

https://www.bvdnet.de/freiheit-2-0-was-hat-big-data-mit-freiheit-zu-tun/

Florian Mehnert: Eine soziale Skulptur für den Datenschutz

Der Konzept-Künstler Florian Mehnert beschäftigt sich seit der Jahrtausendwende mit Fragen von Datenspuren und Datenschutz. „Damals haben mich alle ausgelacht, wenn ich sagte, dass wir auf der Google-Maschine durch unsere Suchanfragen etwas über uns verraten", sagte er den BvD-News.

Der Anstoß für die Beschäftigung mit der Veränderung von Privatsphäre erlebte Mehnert durch die NSA-Affäre, ausgelöst durch den „Whistleblower" Edward Snowden. Mit seinen „Waldprotokollen", bei denen Mehnert Menschen im Wald aufnahm, sorgte er 2013 für Aufsehen. „Ich wollte zeigen, was passiert, wenn wir keine Privatsphäre mehr haben", sagte Mehnert.

Seine Arbeit „Freiheit 2.0" versteht er als „soziale Skulptur", die entsteht, in dem viele Menschen teilhaben, ihre Bewegungsdaten über die gleichnamige APP per GPS anonymisiert aufzeichnen lassen und diese als farbige Routen in eine virtuelle Landkarte eingespeist werden. Mittlerweile zeigen Mehnerts Karten abstrakte Netzwerke über ganz Europa hinweg.

„Nur wenn die Bürgerinnen und Bürger mitmachen, kann daraus Kunst werden", sagt er. Als politische Arbeit versteht er „Freiheit 2.0" aber nicht. „Wir wollen nicht agitieren, nicht etwas verbieten oder fordern. Vielmehr sollen die Leute selbst über ihre Haltung reflektieren".

Den Begriff der Freiheit sieht Mehnert im Zug der Datenschutzdebatten vernachlässigt. „Wir reden längst nicht mehr von Freiheit, sondern nur noch von Schutz vor Datenkraken", sagt er. Das zeigt auch die Versionsnummer 2.0. „In der Wirtschaft sind wir längst bei Industrie 4.0 angekommen, da hinken wir mit der Auseinandersetzung des Freiheitsbegriffs hinterher."

OHNE VERTRAUEN GEHT ES NICHT

Klaus Müller

Die Weisheit „Vertrauen zu gewinnen dauert Jahre, es zu verlieren Sekunden" ist gerade im digitalen Zeitalter bedeutender denn je. Leider muss man aber inzwischen feststellen: In der digitalen Welt wurde Vertrauen nicht über Jahre geschaffen, sondern über Jahre hinweg zerstört. Ein Grund ist die Wildwestmanier, mit der bisweilen personenbezogene Daten verarbeitet wurden.

Trotzdem sind viele Menschen überrascht, wie skrupellos Unternehmen, wie beispielsweise Facebook und Cambridge Analytica, mit ihren Daten umgehen. Und die bisherigen Erkenntnisse dürften nur die Spitze des Eisbergs sein. Vor dem britischen Parlament gab eine ehemalige Geschäftsführerin von Cambridge Analytica zu Protokoll, dass das Unternehmen mit einer Vielzahl von Apps Daten von Facebook erfasst hat. Daher gehe sie davon aus, dass die Zahl der betroffen Nutzer weitaus höher liegt.

Inzwischen wurden von Facebook neben Cambridge Analytica auch mehrere andere Unternehmen gesperrt, die auf der Plattform Apps anboten. Das Unternehmen CubeYou sammelte zum Beispiel über eine App, getarnt als wissenschaftliches Quiz, Daten von Millionen Menschen für Marketing-Zwecke. Die Anzahl vergleichbarer Apps könnte nach Expertenschätzungen in die Tausende gehen.

Es ist zu vermuten, dass diese Daten missbräuchlich verwendet wurden – die Ermittlungen der britischen Datenschutzbehörde werden hier Klarheit liefern. Es ist auch zu vermuten, dass Facebook diesem Missbrauch tatenlos zugesehen hat.

Im Zuge der Berichterstattung kamen in den vergangenen Wochen noch eine Reihe weiterer kritischer Praktiken ans Licht:

Über die Facebook-Suchfunktion war es möglich, öffentliche Profilinformationen automatisiert im großen Stil abzugrasen. Das Unternehmen selbst geht davon aus, dass die Daten aller 2,2 Milliarden Nutzer durch Dritte erfasst wurden.

Außerdem wurde bekannt, dass Facebook aktiv auf die Inhalte von privaten Nachrichten zugreift, die von Nutzern zum Beispiel über den Messenger

verschickt werden. Besonders kritisch ist aber, dass die Datensätze von Cambridge Analytica nach Facebook-Angaben auch die Inhalte von Nachrichten der betroffenen Personen enthalten konnten.

Darüber hinaus soll Facebook über Jahre hinweg auf die Telefon und SMS-Protokolle der Nutzer von Android-Telefonen zugegriffen haben – selbst wenn diese Kommunikation nicht über Facebook geführt wurde. Natürlich waren davon nicht allein die Besitzer der Telefone, sondern alle ihre Kontakte betroffen, die davon selbstverständlich nichts wussten.

Diese Fälle von Datenmissbrauch sind exemplarisch, Ausnahmen sind sie gewiss nicht. Die Einschätzung der beteiligten Unternehmen fällt indes einfach aus: Der Verkauf der Daten von App-Betreibern an Cambridge Analytica sei rechtswidrig gewesen. Es wäre ein Fehler gewesen, nicht früher über die Verarbeitung der Daten durch Cambridge Analytica zu informieren. Außerdem hätten Nutzer ja ▸

GESELLSCHAFT

grundsätzlich der Datenverarbeitung durch Dritte mit den Geschäftsbedingungen zugestimmt.

Nicht nur Verbraucherschützer bezweifeln, dass diese Einwilligungen tatsächlich wirksam waren. Erst vergangenes Jahr bestätigte das Kammergericht Berlin die Auffassung des Verbraucherzentrale Bundesverbands (vzbv), dass in Facebooks App-Zentrum die Nutzer nicht ausreichend über Umfang und Zweck der Datenweitergabe informiert werden.

Facebook und Datenschutz schließen sich aus

Facebook hat angekündigt, Apps überprüfen zu wollen und neue Datenschutzeinstellungen einzurichten. Gleichzeitig muss aber klar sein, dass neue Datenschutzeinstellungen kaum helfen werden, da Facebook aufgrund seines Geschäftsmodells selbst der größte Datensammler ist.

Facebook hat ein System aufgebaut, das dem Datenschutz diametral entgegensteht. Dieses System bietet keine Transparenz. Weder Facebook selbst noch Nutzerinnen und Nutzer scheinen hierüber ansatzweise eine Kontrolle zu haben. Gleichzeitig wäscht das Unternehmen seine Hände in Unschuld.

Damit steht Facebook leider nur beispielhaft für eine Denkweise und Haltung, die sich bei vielen Digital-Unternehmen breit macht. Auch im Online-Werbemarkt wurde ein ähnliches System geschaffen, bei dem die Datenflüsse kaum noch kontrollierbar sind. Kaum ein Webseitenbetreiber kann sagen, zu welchen Zwecken die Daten verwendet werden, die die auf seiner Seite eingebundenen Plugins und Tracking-Dienste sammeln, und wer alles darauf zugreifen kann.

Seit Jahren warnen viele zivilgesellschaftliche Akteure davor, dass es große Risiken birgt, wenn die Interessen von Verbrauchern im Internet nachverfolgt und umfassende Profile gebildet werden. Seit Jahren wird ihnen entgegen gehalten, dass Unternehmen doch ordentlich mit den Daten umgehen würden und dass personalisierte Werbung harmlos sei.

Der Skandal um Cambridge Analytica zeigt nun aber, zu welchen Zwecken solche Profile missbraucht werden können: Von der Manipulation von Individuen, der Steuerung von gesellschaftlichen Stimmungen, Kampagnen, in denen wissentlich falsch informiert wird, bis hin zur Beeinflussung von Wahlergebnissen. Dies ist nicht nur eine Gefahr für einzelne Verbraucher, sondern auch für unseren gesellschaftlichen Zusammenhalt und unsere Demokratie.

Nur wenig Verbraucher vertrauen der digitalen Wirtschaft

Es ist also nicht verwunderlich, dass es um das Vertrauen von Verbrauchern in die digitale Wirtschaft nicht gut bestellt ist. Der Branchenverband Bitkom hat zu der Frage repräsentative Umfragen durchgeführt – zuletzt im Jahr 2017, also noch vor dem Facebook-Skandal. Demnach vertraute nur jeder Dritte Internetnutzer in Deutschland der digitalen Wirtschaft beim Umgang mit personenbezogenen Daten. Mit nur 15 Prozent brachten Nutzer schon damals sozialen Netzwerken das geringste Vertrauen den entgegen.

Knapp drei Viertel der Befragten befürchteten zudem, dass ihre Computersysteme durch Schadprogramme infiziert würden. Und über die Hälfte der Befragten sorgte sich davor, dass persönliche Daten ohne ihr Wissen genutzt und weitergeben werden könnten.

Spätestens diese Zahlen, die den gravierenden Vertrauensverlust belegen, hätten ein Weckruf sein sollen. Und der Vertrauensverlust hat Konsequenzen: Zwei Drittel der Internetnutzer gaben gegenüber dem BITKOM an, dass sie aus Sicherheitsgründen auf bestimmte Online-Aktivitäten verzichten. Etwa jeder Zweite versendet keine vertraulichen Informationen oder wichtigen Dokumente per E-Mail.

Diese Zahlen sind dramatisch. Zwar werden diese Dienste und Anwendungen derzeit trotzdem verwendet. Wirtschaften mit Weitblick sieht jedoch anders aus. Denn die Menschen handeln nicht so, weil ihnen der Schutz ihrer Persönlichkeit egal wäre. Die Nutzung moderner Kommunikationsmittel und vieler digitaler Dienste ist heutzutage eine notwendige Bedingung für eine Teilhabe am gesellschaftlichen Leben. Kurz gesagt: Sie haben heute gar keine andere Wahl. Gleichzeitig haben Verbraucher aber kaum mehr die Möglichkeit, ihre Privatsphäre zu schützen.

Die derzeitige Situation im Netz, in der es heute faktisch keine Privatsphäre mehr gibt, ist nicht tragbar. Darüber sind sich Verbraucher, zivilgesellschaftliche Organisationen, Aufsichtsbehörden, die Europäische Kommission und das Europäische Parlament einig.

Digitale Produkte und Anwendungen bieten fraglos viele Chancen. Diese Chancen werden wir aber auf Dauer nur in vollem Umfang realisieren können, wenn die Menschen solchen Diensten und Technologien tatsächlich vertrauen. Daher ist Vertrauen in der digitalen Welt unerlässlich.

Die Datenschutzgrundverordnung ist ein erster wichtiger Schritt

Um diese Probleme anzugehen, wären beispielsweise die Anpassungen des Wettbewerbs- und Kartellrecht wichtig. Aber auch die Reformen beim Datenschutz und bei der Vertraulichkeit der Kommunikation sind wesentliche Bausteine. Auch wenn Vieles beim Alten bleibt, gibt es doch einige wichtige Neuerungen:

Die EU-weite Harmonisierung durch die Datenschutzgrundverordnung (DS-GVO) ist ein großer Gewinn für Verbraucher in Europa, aber auch für Unternehmen. Ganz im Geiste eines einheitlichen europäischen Binnenmarkts senken diese gemeinsamen Datenschutzregelungen Kosten für Unternehmen und schaffen Rechtssicherheit. Gleichzeitig wird durch die europaweit einheitliche Anwendung künftig verhindert, dass Unternehmen mit ihrem Firmensitz in die EU-Länder mit dem niedrigsten Datenschutzniveau ausweichen können. In der Vergangenheit war dies eine große Hürde für Verbraucher bei der Durchsetzung ihrer Rechte.

Das Marktortprinzip schafft darüber hinaus Klarheit, welches Recht gegenüber internationalen Unternehmen ohne Sitz in Europa anwendbar ist. Die europäischen Datenschutzgesetze schaffen damit gleiche Bedingungen für alle Marktakteure. Das ist besonders wichtig in der digitalen Welt und ihrem grenzüberschreitenden Charakter.

Auch die Stärkung der Einwilligung durch die Datenschutzgrundverordnung ist richtig. Denn oft war unklar, ob die Einwilligung zur Datenverarbeitung tatsächlich eine echte Wahlfreiheit darstellte. Problematisch ist dabei insbesondere auch die mangelnde Verständlichkeit von Datenschutzerklärungen. Oder auch sogenannte Take-it-or-leave-it-Ansätze, bei denen Verbraucher mit einer Einwilligung pauschal einer Vielzahl von Verarbeitungen zustimmen sollten. Diesen Problemen soll mit der Datenschutzgrundverordnung begegnet werden.

Dass einige große Unternehmen die Vorgaben der Datenschutzgrundverordnung, wie beispielsweise das Kopplungsverbot, zu ignorieren scheinen, ist dabei sehr kritisch zu bewerten. Immerhin: Hier wurden bereits erste Beschwerden gegen Unternehmen wie Facebook, Google, Apple, Amazon, LinkedIn, Instagram und WhatApp bei den Aufsichtsbehörden eingereicht – und auch der vzbv wird die Praktiken überprüfen.

Ein zweiter Schritt ist nötig: Die ePrivacy-Verordnung

Um die Probleme des digitalen Marktes zu lösen und das Vertrauen von Verbrauchern zu stärken, ist die DS-GVO alleine aber nicht genug. Die Vorschriften der DS-GVO müssen konkretisiert werden – etwa durch die ePrivacy-Verordnung, die derzeit in Brüssel verhandelt wird. Die DS-GVO stellt dabei eine rote Linie dar, hinter der die ePrivacy-Verordnung in keinem Fall zurückbleiben darf.

Viele Ansätze der ePrivacy-Verordnung sind gut und richtig. So sollen künftig sogenannte „Over-The-Top-Kommunikationsanbieter“ (OTT), wie beispielsweise der Facebook Messenger oder Skype, von der ePrivacy-Verordnung erfasst werden. Bisher fallen nur klassische Telekommunikationsanbieter unter die Regelungen. Dies stellt aber wegen des Bedeutungszuwachses der neuen Kommunikationsdienste kein ausreichendes Schutzniveau mehr dar.

Richtig ist auch, dass künftig eine Verarbeitung von elektronischen Kommunikationsinhalten oder Verbindungsdaten nur auf Grundlage eines gesetzlichen Erlaubnistatbestands oder mit Einwilligung aller betroffenen Nutzer möglich sein soll. Eine Verarbeitung der Informationen auf Basis einer durch die Unternehmen vorgenommenen Abwägung zwischen ihren berechtigten Interessen und den schutzwürdigen Interessen der Verbraucher sollte in diesem sensiblen Bereich nicht zulässig sein. Aber der Schutz darf nicht bei den Kommunikationsdaten aufhören. Die Geräte von ▸

GESELLSCHAFT

Verbrauchern sind – wie es der verstorbene Vizepräsident des Bundesverfassungsgerichts Winfried Hassemer einmal formulierte – so etwas wie ein ausgelagertes Gehirn. Durch die hohe Relevanz der auf Endgeräten gespeicherten Informationen für die Persönlichkeit und Privatsphäre der Nutzer und den damit einhergehenden Gefahren ergibt sich ein hohes Schutzbedürfnis für diese Informationen.

Wenn Unternehmen also künftig auf die Endgeräte der Nutzer zugreifen wollen, um etwa Standortinformationen abzurufen oder um die Interessen der Nutzer im Internet nachzuvollziehen, muss es eine freiwillige und informierte Einwilligung der Verbraucher für jeden konkreten Fall geben. Besonders eingriffsintensive Praktiken sollten verboten werden. Schon bisher war nach EU-Recht eine Einwilligung der Nutzer notwendig, wenn Daten auf ihren Endgeräten gespeichert oder von diesen abgerufen wurden. Dieses Recht ist in Deutschland allerdings bisher nicht richtlinienkonform umgesetzt worden.

Wenn sich die deutsche Bundesregierung im EU-Rat nun dafür ausspricht, Anbietern zu erlauben, die Nutzung ihrer Angebote von einer solchen Einwilligung abhängig zu machen, ist das nicht akzeptabel. Damit unterläuft sie die DS-GVO und spielt großen Unternehmen wie Google und Facebook in die Hände. Denn den Konzernen würde es aufgrund ihrer Marktmacht leichter als kleineren Anbietern fallen, ihren Nutzern eine solche Einwilligung abzuringen.

In der ePrivacy-Verordnung sollten außerdem die Prinzipien des „data protection by design and by default" auch für Hersteller von Kommunikationssoftware verbindlich festgeschrieben werden. Eine Eurobarometer-Umfrage der EU-Kommission zeigt klar, dass sich Verbraucher datenschutzfreundliche Voreinstellungen ihrer Kommunikationssoftware wünschen. 90 Prozent der Internetnutzer in Deutschland sprachen sich für solche Voreinstellungen in ihren Webbrowsern aus. Die Umfrage zeigt auch, dass besonders Ältere, Personen mit niedrigerer Bildung sowie Menschen, die das Internet wenig verwenden, seltener Änderungen der Datenschutzeinstellungen ihrer Software vornehmen. Datenschutzfreundliche Voreinstellungen schützen also in erster Linie besonders verletzliche Verbrauchergruppen. Umso bedauerlicher ist es, dass sich die Bundesregierung nicht für datenschutzfreundliche Voreinstellungen von Webbrowsern einsetzt.

Chancen der neuen Datenschutz-Regelungen

Die Geschehnisse der vergangenen Monate verleiten dazu, den Fokus auf Facebook zu richten. Zur Wahrheit gehört jedoch auch: Die neuen Regelungen betreffen jedes Unternehmen und jede Institution, die personenbezogene Daten verarbeiten. Die derzeitigen Reformen im Bereich des Datenschutzes und der Vertraulichkeit der Kommunikation sind ohne Zweifel eine gesamtgesellschaftliche, gewaltige Herausforderung. Es wird auch Geschäftsmodelle geben, die grundlegend überdacht oder gar aufgegeben werden müssen.

Aber die Reformen bieten auch Chancen: Nach der DS-GVO wird die ePrivacy-Verordnung die bisherigen Regelungen für die Vertraulichkeit der Kommunikation EU-weit vereinheitlichen, konkretisieren und der Datenschutzaufsicht endlich Mittel zur effektiven Durchsetzung des Rechts an die Hand geben.

Außerdem führen hohe Standards dazu, dass Produkte über ihre Qualität und nicht lediglich über ihren Preis bewertet werden. Beispiele in den Bereichen der Produktsicherheit oder der IT-Sicherheit zeigen, dass dies Innovation begünstigen kann. Darüber hinaus schaffen hohe Standards Vertrauen. So ist Deutschland wegen seines Datenschutzniveaus der weltweit beliebteste Cloud-Standort für Unternehmen.

Normalerweise begünstigen Innovationen immer Kunden. In den vergangenen Jahren verschob sich dies im Falle der digitalen Welt jedoch weg von den Nutzern hin zu den Werbetreibenden. Durch die europäischen Neuregelungen könnte sich dieses Ungleichgewicht wieder auflösen und Wege für neue, datenschutzfreundliche Geschäftsmodelle öffnen. Wichtig dabei ist, dass sich Europa nicht zu sehr an den Geschäftsmodellen der Amerikaner orientiert, sondern eigene Visionen entwickelt.

So sind in den vergangenen Jahren und Monaten auch viele neue Startups entstanden, die auf die DS-GVO und die ePrivacy-Verordnung reagieren. Für den Online-Bereich zeigen beispielsweise bereits verschiedene europäische Unternehmen, dass es Alternativen zu Werbung gibt, die auf invasivem Tracking beruht und in die Privatsphäre der Nutzer eingreift. Darunter sind Suchmaschinenanbieter, die mit kontextbezogener Werbung oder gesponsorten Links arbeiten und Entwickler von angebotsübergreifenden Abomodellen. Es gibt aber auch ein Unternehmen aus der Ad-Tech-Branche, das ein System entwickelt, mit dem auf Basis bisheriger Strukturen die Daten von tatsächlich einwilligenden Nutzern vermarktet werden können, die Daten der anderen Nutzer jedoch geschützt bleiben.

Es ist klar, dass es diese Geschäftsmodelle in der Vergangenheit schwer hatten. Denn bisher funktionierte es ja auch mit einem System, bei dem die Gewinne abgeschöpft, aber die Kosten für die Gesellschaft externalisiert wurden. Doch diese Unternehmen mit ihren neuen Visionen zeigen, dass es Gegenentwürfe gibt. Der Markt wird Lösungen auf die geänderten Rahmenbedingungen finden. Dies stellt besonders eine Chance für innovative europäische Unternehmen dar.

Die DS-GVO und die ePrivacy-Verordnung sind die Gelegenheit, das verlorene Vertrauen in die digitale Gegenwart und Zukunft wieder herzustellen. Das wird eine Grundbedingung für den Erfolg datenintensiver Geschäftsmodelle in Europa sein. Denn nur so können die Chancen der Digitalisierung in vollem Umfang realisiert werden.

Über den Autor

Klaus Müller
Vorstand Verbraucherzentrale Bundesverband (vzbv)

Anzeige

GESELLSCHAFT

DATENSCHUTZSCHULUNG – AUF DIE INNOVATIVE ART

Dr. Niels Lepperhoff und Dipl. Ing. Harald Mais

Selten hat ein Thema landesweit so hohe Wellen geschlagen, wie das Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO). Es wurde viel spekuliert und manches vollkommen fehlinterpretiert. Doch die seit Monaten anhaltende Debatte rund um die DS-GVO ist auch ein ausgesprochen überzeugendes Plädoyer für ein absolut effizientes Lernformat.

Sensibilisieren für den Datenschutz:

Eine anspruchsvolle Aufgabe

Mitarbeiter zum Thema Datenschutz zu sensibilisieren und zu schulen war schon immer eine anspruchsvolle Aufgabe und wird es auch weiterhin sein. Die Verantwortung für diese Schulungen liegt grundsätzlich bei der Unternehmens- oder Behördenleitung. In der Regel sind Datenschutzbeauftragte an der Gestaltung und teilweise auch an der Durchführung der Schulungen beteiligt – oft sogar maßgeblich. Häufig werden sie von Unternehmen schon im Vorfeld zu Meetings eingeladen, in denen sie die Neuerungen der DS-GVO zunächst kurz verdeutlichen und dann die Präsenzschulungen dazu gemeinsam planen. So professionell diese Kooperation auch sein mag, so sehr verursacht sie zusätzliche Arbeit. Arbeit in einer Phase, in der ein Datenschutzbeauftragter eines zweifelsfrei nicht hat: Zeit.

Aus alt mach neu?

Nicht selten wird von Datenschutzbeauftragten verlangt, „mal kurz zu erzählen, was sich mit der DS-GVO denn so alles ändert“ – manches Mal zwischen Tür und Angel und wenn möglich, „bitte in fünf Minuten.“ Eine Wunschvorstellung, die so und auf die Schnelle nicht erfüllt werden kann – und natürlich auch nicht erfüllt werden sollte, da zu vieles Wichtige auf der Strecke bleiben könnte. Und auch wenn diese Forderung unverkennbar auf die Neuerungen der DS-GVO zielt, zeigt die Erfahrung doch, dass eine nicht zu unterschätzende Zahl an Geschäftsführern und Mitarbeitern das alte Datenschutzrecht kaum bis gar nicht kannte. Für den Datenschutzbeauftragten bedeutet das: Noch bevor die Neuerungen aufgezeigt werden können, steht eine Erläuterung der alten Datenschutzprinzipien und -grundlagen an. Eine weitere, zusätzliche und zeitraubende Arbeit.

Ausschlaggebend ist die Zielgruppe

Welche Datenschutzprinzipien und -grundlagen in der Praxis tatsächlich relevant sind, hängt zudem von dem Tätigkeitsfeld und Verantwortungsbereich der jeweiligen Person ab. Bei einem Geschäftsführer steht eventuell Art. 5 mit starker Betonung der Rechtmäßigkeit und Rechenschaft im Zentrum. Die Mitarbeiter der Marketingabteilung brauchen vielleicht hingegen eine Mixtur aus Zweck, Rechtsgrundlage und Löschfrist – mit dem wichtigen Bestandteil, dass die Informationspflichten nach Art. 13 und 14 DS-GVO umzusetzen sind und insbesondere § 7 UWG nicht vergessen werden sollte. Genau diese beiden Beispiele zeigen: Es gibt nicht die eine, allgemeingültige und allumfassende Information zur DS-GVO. Die Informationen müssen zielgruppenorientiert erstellt und – genauso wichtig – auch richtig adressiert sein.

Unschlagbare Argumente

Eine klassische Form der Datenschutzschulung ist die Präsenzveranstaltung mit einem Vortrag zum Datenschutz und der Gelegenheit Fragen zu stellen. Das Format ist bewährt und bringt den Datenschutzbeauftragten in einen direkten Kontakt mit seinen „Schützlingen“. Es stößt jedoch schnell an Grenzen, wenn viele Menschen in kurzer Zeit zu schulen sind oder diese auf mehrere Standorte verteilt sitzen. Die Fragen erlauben zwar ein individuelles Eingehen auf den Fragesteller. Gleichwohl bleibt der Vortrag meistens allgemein gehalten.

Mit dem digitalen Lernen steht eine alternative Form der Wissensvermittlung bereit. Das digitale Lernen erlaubt zeitsparend, kostengünstig und umweltschonend wichtige Wissensinhalte an die richtigen Stellen zu transferiert. Durch seine Modularität wird eine differenziertere Wissensvermittlung möglich.

Das 3-Phasen-Prinzip

Ein gutes E-Learning-Programm funktioniert nach einem ganz einfachen Prinzip: (für das Thema) sensibilisieren, (über das Thema) informieren und aktivieren und (das Gelernte) kontrollieren. In der ersten Phase wird die Aufmerksamkeit der Lerner gewonnen und mithilfe von Quizfragen ihr Vorwissen aktiviert. Haben sich die Lerner für das Thema geöffnet, werden die zentralen Themen des Lerngegenstandes interaktiv präsentiert – und das in einem abwechslungsreichen Medienmix. Es wird darauf geachtet, dass der Lerner nicht nur „berieselt“ wird und die Rolle des Zuschauers übernimmt, sondern im höchsten Maße in das E-Learning eingebunden wird und explorativ sowie aktiv die Lerninhalte entdeckt. Die richtige Wahl des Wordings und der Tonalität helfen dabei, dass der Lerner sich nicht auf einem „fremden Terrain“, sondern thematisch „zu Hause“ fühlt. Die Regel ist immer „die Sprache der Zielgruppen“ zu sprechen und die Inhalte diesen immer anzupassen. Ein weiterer Punkt ist die Nähe zur Praxis: Die Lerninhalte werden praxisnah an die Arbeitsrealität der Lerner ausgerichtet, wodurch eine hohe Motivation und

Identifizierung mit dem Thema stattfindet. In der dritten Phase folgt dann die Wissensabfrage mithilfe eines Abschlusstests, der sowohl den Lernern selbst als auch dem Unternehmen ein Feedback zum Wissensstand liefert. Ob und wie viel das E-Learning vom Lerner bearbeitet wurde, ist für das Unternehmen durch das Learning Management System mit einem Klick kontrollierbar. Und der Vorteil bei gesetzlichen Auflagen von Schulungsthemen: Die Lerner können ihre Zertifikate als Nachweise ausdrucken. ▸

GESELLSCHAFT

Wie entsteht eigentlich ein Datenschutz Lernprogramm?

In einem Kick-off-Meeting treffen der Datenschutzbeauftragte und die E-Learning-Experten zusammen. Dabei werden grundsätzliche Fragen zu den Inhalten, der didaktischen Konzeption und grafischen sowie technischen Umsetzung geklärt und Ideen ausgetauscht. Auf dieser Basis entsteht das Konzept für das Lernprogramm. In enger Zusammenarbeit mit dem DSB schreibt ein Autor erst ein Grobkonzept, dann ein Feinkonzept und schließlich ein detailliertes Drehbuch. Auf Grundlage des Drehbuchs bereiten die Programmierer und Grafiker die Inhalte multimedial auf, denn nur mit einem gut gelayouteten Lernprogramm werden die Inhalte lebendig und das Lernen fängt an Spaß zu machen. Danach wird das Lernprogramm von einem professionellen Sprecher vertont und auf die visuellen Inhalte (Bilder/Texte/Grafiken) abgestimmt. Nach bestandener Qualitätssicherung und Endabnahme durch den DSB erhält dieser das fertige Lernprogramm.

Der optimale Mix: Blended Learning

Doch E-Learning muss Präsenzlernen nicht komplett ersetzen, sondern kann als ergänzende Maßnahme genutzt werden. Die Kombination aus E-Learning und Präsenzlernen (Blended Learning) kann in einem Blended Learning Konzept zusammen mit dem Unternehmen erarbeitet werden. Wichtig ist hier wieder der zielgruppengerechte und didaktisch sinnvolle Aufbau der beiden Lernformate. Beispielsweise ob eine Schulung mit einem Präsenzseminar starten sollte, damit sich die Lerner und Dozenten kennenlernen und austauschen oder eher mit einem E-Learning-Programm, in dem die Lerner sich bereits mit der Theorie eines Themas selbstgesteuert beschäftigen können, sind Aspekte, die in einem Blended Learning Konzept analysiert werden.

Modularisierung der Inhalte

Umfassendere Themenbereiche können auch modularisiert werden, sodass die Lerner in kürzeren Lerneinheiten noch selbstgesteuerter lernen können. Dabei werden die Lerneinheiten (Module) systematisch aufeinander aufgebaut und individuell auf die Lerner angepasst.

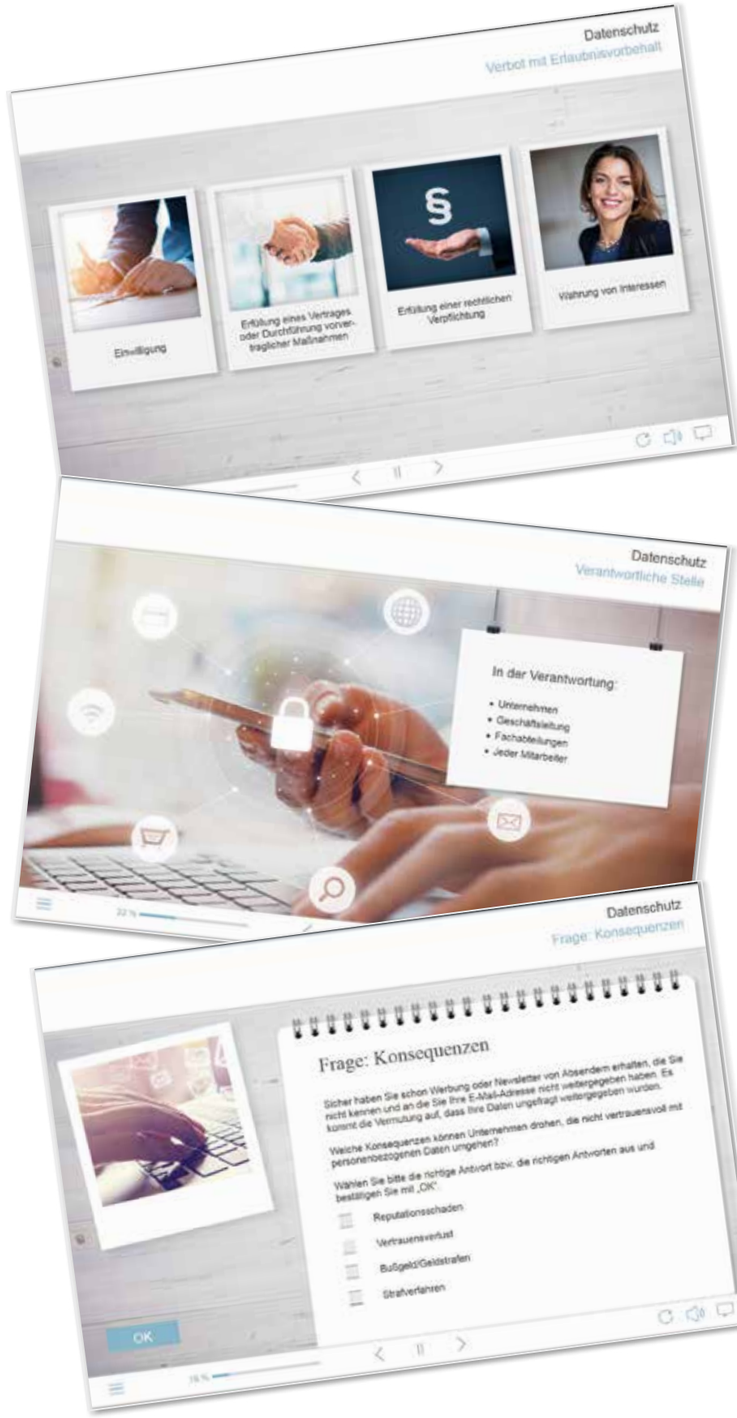
Einbindung in bestehende Prozesse und Systeme

Digitalen Lernens erfolgt technisch auf einer Lernplattform. Diese kann intern im Unternehmen oder im Rahmen einer Auftragsverarbeitung extern betrieben werden. Beiden Versionen gemeinsam ist, die Möglichkeit zur Integration in die betrieblichen Abläufe. Eine Kopplung mit einem Personalinformationssystem erlaubt bspw. die automatische Einladung neuer Mitarbeiter zum Kurs. Basierend auf der Position kann automatisch eine Zuweisung zu den relevanten Kursen erfolgen.

Der Teilnahmeerfolg kann automatisch hinterlegt werden. Einige Unternehmen koppeln zudem den Zugang zu IT-Geräten an das erfolgreiche Absolvierend des Kurses.

Die wichtigsten Vorteile von E-Learning im Überblick:

Unternehmen	Mitarbeiter	Lerninhalte	Datenschutzbeauftragte
können neues Wissen im Unternehmen zeitnah multiplizieren	erhalten attraktive Qualifizierungsmaßnahmen und Weiterbildungsmöglichkeiten	sind auf die Bedarfe und Bedürfnisse der Unternehmen individuell zugeschnitten	werden bei gleichzeitigem hohem Schulungsbedarf entlastet
erreichen die Zielgruppe direkt	sind räumlich und zeitlich flexibel und können orts- und zeitunabhängig lernen	sind immer aktuell und können schnell und regelmäßig aktualisiert werden	stellen die Schulungsteilnahme durch elektronische Verfahren sicher
integrieren innovative Schulungs- und Qualifikationsmöglichkeiten in den Arbeitsalltag	haben durch den anonymen Raum weniger Hemmnisse	sind immer für Lerner verfügbar	erhalten eine einfache Steuerung, welche Zielgruppe welche Inhalte erhält
agieren umweltfreundlich, da Reisekosten für Mitarbeiter entfallen	erhalten leichten Zugang zu Informationen	sind interaktiv	können schnell auf Änderungen im Datenschutzrecht reagieren
reduzieren Ausfallzeiten durch wegfallende Reisen zu Schulungsorten	können ihr Lerntempo selbst bestimmen und im eigenen Rhythmus lernen	bieten maßgeschneiderte Lernmethoden (Text, Ton, Video etc.)	sorgen durch die digitale Teilnahmedokumentation juristisch vor
können eine große Anzahl an Mitarbeitern / beliebig viele Nutzer gleichzeitig bzw. zu gleichen Themen schulen	können ihre Medienkompetenz steigern	können mit Präsenz-Lernangeboten verknüpft werden	können sich auf die identische Vermittlung von Lerninhalten an die Zielgruppen verlassen
können in verschiedenen Sprachen schulen	können Zertifikate erlangen	bieten eine Auswahl an unterschiedlicher medialer Aufbereitung	
können über integrierte Testsysteme statistische Auswertungen erstellen	können auch außerhalb von Bürozeiten auf Wissen zugreifen		
bieten ihren Mitarbeitern bedarfsgerechte Möglichkeiten an Qualifikationen	Kurs kann bei konkreten Fragen erneut durchlaufen werden („Nachschlagewerk“)		



Über die Autoren

Dr. Niels Lepperhoff

Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD e.V. und der GDD e.V.).

Dipl. Ing. Harald Mais

Gründungsmitglied und Mitglied der Geschäftsführung von Fischer, Knoblauch und Co. Medienproduktionsgesellschaft (FFM) mbH

▶ h.mais@fkc-online.com

AUS DEM VERBAND

BVD VERBANDSTAGE 2018 - EIN RÜCKBLICK

Datenschutzrechtliche Zeitenwende – Kopfzerbrechen inklusive

Die BvD-Verbandstage 2018 standen ganz im Zeichen der DS-GVO

Genau vier Wochen vor dem Start der Datenschutz-Grundverordnung (DS-GVO) waren in Berlin rund 200 Datenschutzbeauftragte zu den BvD-Verbandstagen 2018 zusammengekommen. In dem mittlerweile traditionellen BvD-Tagungshotel ELLINGTON drehte sich unter dem Motto „Wegweisend im Datenschutz“ alles um die „datenschutzrechtliche Zeitenwende“, wie BvD-Vorstand Thomas Spaeing zum Auftakt des wichtigen Branchentreffs sagte. Aber vier Wochen vor dem Start in die neue Datenschutz-Epoche waren eben noch viele Fragen ungeklärt. „Das bereitet uns auch Kopfzerbrechen“, sagte Spaeing, unter anderem, weil es für die vielen Einzelpunkte der DS-GVO „noch keinen Praxischeck gibt“.

Worüber sich die Fachleute und Experten einig waren: Unter dem Eindruck des Facebook-Datenskandals, bei dem ein Unternehmen massenweise Daten von Facebook-Nutzern missbrauchte, hatte sich der Wind gedreht. „Wir hören mittlerweile viel Zuspruch zur Grundverordnung“, sagte die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, in einem Grußwort. Der Vorfall zeige, wie notwendig und wichtig nachhaltiger Datenschutz sei.

Lebendiger Austausch für die DS-GVO

Dr. Nina Wunderlich, Leiterin Zentrales Rechtsreferat im Bundeswirtschaftsministerium, betonte, der Facebook-Datenskandal mache deutlich, welche Verantwortung Unternehmen für die Daten ihrer Kunden und Nutzer trügen. Sie wertete die DS-GVO als „große Errungenschaft“, die Wettbewerbsverzerrungen innerhalb der EU weitestgehend bereinigt habe. Das Regelwerk insgesamt bezeichnete sie als „angemessenen Ausgleich zwischen den Wirtschaftsinteressen einerseits und dem Recht von Verbrauchern andererseits“.

Vor allem vor dem Hintergrund neuer Entwicklungen wie „Smart home“ oder „Smart City“ und automatisiertem Fahren sei es wichtig, die Auskunftsrechte von Bürgern und das Recht auf Vergessen zu stärken, zugleich aber solche Entwicklungen zu ermöglichen.

Aber auch Wunderlich räumte ein: Die DS-GVO „stellt uns alle und die Unternehmen vor die Herausforderungen, ein effektives Datenschutzmanagement zu präsentieren“. Ihr Haus hatte gemeinsam mit dem Deutschen Industrie- und Handelskammertag (DIHK) und den örtlichen IHK im Vorfeld des 25. Mai eine Roadshow durch die Republik initiiert. Der Kontakt mit Unternehmern und Bürgern habe gezeigt, dass es über den 25. Mai hinaus einen „lebendigen Austausch“ mit den Aufsichtsbehörden, Verbänden und europäischen Partnern geben müsse. „Dann können sich die Chancen der DS-GVO voll entfalten“, sagte sie.

Von Löschkonzepten und Meldepflichten

In den weiteren Vorträgen und Workshops ging es um spezielle Aspekte der DS-GVO, etwa über die Frage, wie die IT-Sicherheit im Zuge der Umstellung gewährleistet sein muss. Über die derzeit noch bestehenden Diskrepanzen zwischen der geplanten ePrivacy-Verordnung und der DS-GVO sprach Ministerialrat Winfried Ulmen vom Bundeswirtschaftsministerium.

Maria Wilhelm, Referentin der Stabsstelle Europa beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, diskutierte mit den Fachleuten über die Informations- und Meldepflichten nach der DS-GVO. Ministerialrat Michael Will vom Bayerischen Innenministerium zeigte Änderungen der Landesdatenschutzgesetzte vor dem Hintergrund der DS-GVO auf. Weitere Themen waren die Einwilligung nach der DS-GVO, Datenschutz im Medizin-Sektor, Löschkonzepte nach der DS-GVO und Datenschutz-Compliance.

Informationen zu den BvD-Verbandstagen 2018 erhalten Sie unter:

https://www.bvdnet.de/bvd-verbandstag/

Interessierte können die Vorträge auf

https://www.bvdnet.de/termin/bvd-verbandstag-2018/ nachlesen.

Voßhoff bedankt sich für gute Zusammenarbeit

Die Bundesdatenschutzbeauftragte Andrea Voßhoff konnte nicht an den BvD-Verbandstagen 2018 teilnehmen, wurde aber per Video ins Plenum übertragen. Sie zeigte sich überzeugt, ▸

Datenschutz-Software-Forum

Renommierte Software-Unternehmen und Entwickler präsentierten im Rahmen der BvD-Verbandstage 2018 den Entwicklungsstand ihrer Systeme und erläuterten Handhabung und Nutzen in Fachvorträgen. Besucher erfuhren, welche aktuellen Produkte auf dem Markt angeboten werden und in wie weit die Datenschutz-Grundverordnung in die Entwicklung bereits berücksichtigt wurde.

Themen-Überblick waren:

- Lizenzmodelle
- Kostenstruktur
- Eignung für Beratungsunternehmen
- Einbindung in Konzernstrukturen
- Webversion für externen Zugriff
- Anwendung unter DS-GVO
- Umsetzung Risikofolgeabschätzung
- Anpassung der Übersicht der Verarbeitungen
- Umstellung Prüfkataloge Auftragsverarbeitung
- Nachweis der Rechtmäßigkeit der Datenverarbeitung
- Prüfkataloge für Privacy by Design/Default
- Berücksichtigung Normen/Gesetze
- Verfügbare Sprachversionen

▶ https://www.bvdnet.de/termin/datenschutz-software-forum-2/

dass die DS-GVO als „Anfangs-Werkzeugkasten" dem Datenschutz weltweit zu mehr Wirkung verhelfen werde.

Voßhoffs Amtszeit endet im Dezember 2018. Sie dankte dem BvD für die gute Zusammenarbeit und zeigte sich vor allem von der Bildungsarbeit des Verbands und der Initiative „Datenschutz geht zur Schule" begeistert.

Gemeinsam mit dem BvD und dem Verein „Deutschland sicher im Netz" (DsiN) lud sie am 3. Juli zur Dialogkonferenz „Datenschutz für Kinder" Fachleute und Bildungsexperten nach Berlin ein. Auch BvD-Vorstand Thomas Spaeing und der Sprecher des BvD-Arbeitskreises Schule, Rudi Kramer, waren mit dabei. (siehe Bericht S. 62).

Zum Abschluss war BvD-Vorstand Spaeing überzeugt, dass auch in den Wochen nach dem Start der DS-GVO „nichts Schlimmes passieren" werde. Die Aufsichtsbehörden seien kooperativ und selbst an Aufklärung interessiert. Allerdings mahnte Spaeing eine schnellere Bearbeitung noch offener Gesetzesfragen an. „Wir warten noch immer auf das Beschäftigtendatenschutz-Gesetz", sagte er, „auf die ePrivacy-Verordnung und eine Novelle des Telemediengesetzes". Diese dürften unter anderem Themen der BvD-Verbandstage 2019 sein, die vom 5. bis 6. Juni in Berlin stattfinden. Traditionell im ELLINGTON HOTEL BERLIN.

▶ https://www.bvdnet.de/bvd-verbandstag/

BvD-News Redaktion

ERFOLGS-MOTOR DAME

Wie der BvD Filme- und Videomacher mit dem Datenschutz-Medienpreis fördert

Kein Wunder, dass Monica Oliveira begeistert ist. Mit ihren Kolleginnen Natalia Rasstrigina und Leslie Iseli hat sie für den Clip „Social Engineering" den ersten Datenschutz-Medienpreis (DAME) 2017 gewonnen. Aber auch von der Intention des Preises schwärmt Oliveira. "Der Preis ist eine geniale Sache", sagt sie. Denn das Thema Datenschutz „ist brandaktuell und wird immer wichtiger" in der schnell voran schreitenden Digitalisierung. Menschen, die nicht täglich damit zu tun hätten, fehle Wissen und Information. Der Preis biete die Möglichkeit, Datenschutz einfach zu erklären, „so dass die Botschaft klar verständlich ankommt".

Aber noch aus einem anderen Grund ist Oliveira begeistert. Denn das Team hat durch den Preis eine Kooperation mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) geschlossen: Danach soll der kurze Clip, der ohne Worte auf die Gefahren des Geo-Trackings in den sozialen Netzwerken hinweist, in der Mediathek eines Schulportals zum Download angeboten werden. „Dadurch kommen wir an eine Zielgruppe, die für die Thematik sensibilisiert werden soll", sagt Oliveira. „Das war von Anfang an unsere Absicht."

Auch die Filme der beiden weiteren Nominierten, die zur spannenden Preisverleihung am 25. April nach Berlin eingeladen waren, wurden für das Schulportal angefragt. Danach können Lehrkräfte sowohl die fünfteilige Animations-Serie „Sicher surfen einfach erklärt" von Alexander Lehmann als auch den Aufklärungsfilm „Datenschutz - Fast wie Sex" von Tom Schildhauer für den Unterricht herunterladen. „Das finde ich sehr cool, auf diese Weise Schüler zu erreichen", sagt Schildhauer. „Das ist viel wert".

„Datenschutz ist unumgänglich"

Schildhauer nahm mittlerweile ein Studium für Entwicklung und Produktion von Computer-Spielen auf. Sein Know-how über Datenschutz hält er dabei für unerlässlich. „Ich bin einer der wenigen, die beim Thema Datenschutz Impulse bei der Entwicklung von Computerspielen setzen können", sagt er. Dabei müssten die Teilnehmenden an Online-Spielen viele persönliche Daten preisgeben. „Da ist das Thema Datenschutz unumgänglich."

Alexander Lehmann hat bereits den nächsten Film zum Thema Datenschutz fertiggestellt. Für die Initiative „Deine Daten, Deine Rechte“ produzierte er zehn Erklärvideos zur Datenschutz-Grundverordnung (DS-GVO), darunter den Animationsfilm „Update für Deine Freiheit“.

„Seit zehn Jahren beschäftige ich mich in Filmen mit Datenschutz“, sagt Lehmann, „da werden noch einige Beiträge folgen“. Lehmann hofft durch die Nominierung auf eine größere Bekanntheit, nicht nur für sich und sein Team, sondern auch für das Thema Datenschutz. Denn im Zug des Starts der DS-GVO am 25. Mai habe es zwar viel Aufklärung für Unternehmen und Selbständige gegeben, wie sie sich auf die neuen Regeln vorbereiten. „Aber der normale Bürger ist dabei zu kurz gekommen“, sagt er.

DAME – „Das hat viel ausgelöst“

Über eine Kooperation mit weiterer Perspektive freut sich auch der 18-jährige Kevin Lehmann vom Verein Juuuport, Er hatte den ersten „Sonderpreis Jugend“ für seinen Rap-Video „Daten unter Artenschutz“ erhalten. Jetzt sollen weitere Videos u.a. mit der Initiative „Datenschutz geht zur Schule“ des BvD im Rahmen der Förderung der DATEV-Stiftung Zukunft folgen. Kevin komponierte und textete bereits die nächsten Songs, die sich um die Themen Datenklau, Cybermobbing und Datenschutz drehen. Die Songs werden „ein bisschen anders“ sein, „damit es nicht langweilig wird“, verspricht er.

Kevin macht nächstes Jahr Abitur, aber für den Verein Juuuport, für den er als einer von rund 30 bundesweit tätigen Scouts Jugendliche bei Problemen mit dem Internet berät, will er treu bleiben.

Über Kevins Erfolg freut sich auch Lennart Sörnsen, Sprecher von Juuuport, einer bundesweiten Beratungsplattform für Jugendliche, die übers Internet Mobbing oder Abzocke erleben müssen. „Der Preis hat die Resonanz für unsere Arbeit erhöht“, sagt Sörnsen. „Das hat viel ausgelöst.“ Juuuport will sich noch mehr auf Videos konzentrieren, weil sie beispielsweise über die Video-Plattform YouTube ihre Zielgruppe erreichen.

Video als Informationsmedium

Das war auch einer der Gedanken, die BvD-Vorstand Thomas Spaeing sich für den Wettbewerb für Film- und Videobeiträge zum Thema Datenschutz begeistern ließ. „Videos sind heute ein wichtiges Informationsmedium, nicht nur für junge Leute“, sagt er. „Mit unserer DAME wollen wir Filmemacher und Video-Autoren ermutigen, Datenschutz-Themen auf Video-Kanälen zu verbreiten und damit zur Aufklärung über komplexe Datenschutz-Sachverhalte beizutragen.“

Von den 25 Einreichungen für die erste DAME-Runde war die Juy begeistert, der neben Spaeing noch Birgit Kimmel (pädagogische Leiterin der EU-Initiative klicksafe bei der Landeszentrale für Medien und Kommunikation Rheinland Pfalz), Klaus Müller (Vorstand Verbraucherzentrale Bundesverband), Frederick Richter (Vorstand Stiftung Datenschutz) und die Landesbeauftragte für den Datenschutz Niedersachsen, Barbara Thiel, angehörten. Sie sind auch in der zweiten Runde der DAME mit dabei.

Datenschutz lebendig und spannend

Die eingereichten Beiträge hätten gezeigt, dass Datenschutz nicht verstaubt und trocken sein muss, sagt Frederick Richter von der Stiftung Datenschutz. „Datenschutz kann lebendig und spannend erzählt werden.“ Neben Kino-Filmen und TV-Reportagen habe es auch viele „sehr emotionale oder witzige Stories“ gegeben, sagt Landesdatenschutzbeauftragte Thiel.

Spaeing hofft für die zweite DAME-Runde auf eine ähnliche Bandbreite. „Die Nominierten und die Preisträger können sich darauf verlassen, dass wir uns als Berufsverband der Datenschutzbeauftragten für ihre Filme und Clips einsetzen, auch über den Preis hinaus“.

Interessierte Filmschaffende, TV-Autoren oder Video-Nachwuchsfilmer können sich noch bis 01. November 2018 für die zweite Runde des mit 3.000 Euro dotierten Datenschutz-Medienpreises bewerben. Der „Sonderpreis Jugend“ ist mit 500 Euro dotiert. Die DAME 2018 wird auf den BvD-Verbandstagen vom 5. bis 6. Juni 2019 auf einer feierlichen Gala in Berlin überreicht. Drei Nominierte werden zu der Verleihung eingeladen, der oder die Gewinner dann am Abend bekannt gegeben.

Die Bewerbungsunterlagen erhalten Interessierte unter Datenschutz-Medienpreis auf der Internetseite

https://www.bvdnet.de/datenschutzmedienpreis/

BvD-News Redaktion

DAME 2018 BvD DATENSCHUTZ MEDIENPREIS

Jetzt für DAME 2018 bewerben:

Teilnahmebedingungen und Bewerbungsbogen

https://www.bvdnet.de/datenschutzmedienpreis/

And the Winner DAME 2017 is …

„Social Engineering“ von Monica Oliveira erzählt ohne Worte von den Gefahren, die Jugendlichen durch eine unbewusste Preisgabe von Daten in den Sozialen Netzen drohen. Der kurze Clip wurde für die Schweizerische Akademie der Wissenschaften (SADW) erstellt.

„Datenschutz unter Artenschutz“ Kevin Lehmann von der Beratungsplattform JUUUPORT.de. Der 18-jährige Schüler aus Oldenburg überzeugte die Jury mit seinem selbstgeschriebenen Rap „Daten unter Artenschutz“, den er zum Abschluss der Veranstaltung live performte.

„Datenschutz – Fast wie Sex“ von Tom Schildhauer. Der animierte Erklärfilm widmet sich mit Augenzwinkern und eingängigen Vergleichen der Frage, welche Daten Verbraucher täglich im Netz oft unwissend von sich preis geben.

„Sicher surfen einfach erklärt“ von Alexander Lehmann. Die 5-teilige Animations-Serie erklärt niedrigschwellig und leicht verständlich, wie jeder Einzelne seine Daten schützen kann. Die Reihe erschien für eine Ausstellung des Zentrums für Kunst und Medien (ZKM) Karlsruhe, auf „Spiegel Online“ und im ORF.

AUS DEM VERBAND

VORTAGSREIHE DATEN-DIENSTAG

Rückblick

Seit 2015 bietet der BvD zusammen mit dem Museum für Kommunikation in Nürnberg die Vortragreihe „Daten-Dienstag – Privatheit im Netz?“ an. In 2018 kam als Mitveranstalter noch das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hinzu.

Von Anfang an hatte die Reihe das Ziel, der gesellschaftlichen Diskussion um die Bewahrung der Werte im Internet und deren Schutz einen Raum zu geben. Entsprechend vielfältig waren Redner und Themen ausgewählt. Begann im Januar 2015 der damalige BITKOM-Präsident Prof. Dieter Kempf mit seinen Gedanken zu der Frage „sind Daten die Währung von morgen?“, so folgte darauf der Präsident des BayLDA Thomas Kranig mit Ausführungen darüber was man selbst mit eigene Bildern und denen anderer im Netz machen darf.

Betrachtet man die Diskussionen der letzten Monate: Ein immer noch aktuelles Thema. Wie sich Jugendliche im Social Web verhalten beleuchtete Niels Brüggen vom Institut für Medienpädagogik in München und Bernd Fuhlert schilderte die Möglichkeit, sich gegen Rufmord im Netz zu wehren.

Einen Ausflug ins Berliner Museum für Kommunikation machte die Reihe im Mai 2015 mit Sabine Leutheusser-Schnarrenberger mit ihren Erfahrungsberichten aus dem Beirat von Google zur Umsetzung des EuGH-Urteils zum „Recht auf Vergessen“.

Malte Spitz referierte zu seinen Erfahrungen und Recherchen mittels Selbstauskünften auch im Vergleich zu den USA, die er im gleichnamigen Buch veröffentlichte.

Das Thema „Europäische Kriminalitätsbekämpfung und Datenschutz“ des Bayerischen Landesdatenschutzbeauftragten Dr. Thomas Petri erhielt im September unerwartete Aktualität, als es Überlegungen gab internationale Dateien der Polizei für die Verwaltung der Flüchtlinge zu verwenden.

Im Herbst 2015 wurde die Reihe des Daten-Dienstags auch um das Symposium des BvD zum Datenschutzbeauftragten in der DS-GVO erweitert, bevor mit dem Vortrag von Prof. Dr. Matthias Brand zum Thema Cybermobbing das Vortragsjahr 2015 abgeschlossen wurde.

Für 2016 wurden weitere sechs Termine im Rahmen der Vortragsreihe angeboten, die durch Dr. Wulf Kamlah mit einer Darstellung der Schufa aus datenschutzrechtlicher Sicht eröffnet wurde.

Kevin Marschall informierte in seinem Beitrag „was die Versicherung nicht weiß…“ zu den datentechnischen Möglichkeiten, Versicherungsbetrug aufzuklären und der Leiter Konzerndatenschutz der BMW Group Werner Bednarsch stellte das Datenschutzmanagementsystem des Unternehmens dar.

Den Blickwinkel auf Straftaten im Netz, denen Jugendliche ausgesetzt sind, schärfte der Kriminologe Thomas Gabriel Rüdiger und die Unternehmerin und Autorin Yvonne Hofstetter reflektierte ihre Wahrnehmungen und Erkenntnisse zu künstlicher Intelligenz. Fallbeispiele aus der Wissenschaft zur Forensischen Informatik bei der Verbrecherjagd steuerte Prof. Dr. Felix Freiling bei.

Für den Zeitraum September 2017 bis Juni 2018 äußerten sich dann mit André Pallinger aus der Geschäftsleitung von Payback mit Unterstützung durch den DSB von Payback zu den Aspekten der Kundenbindung und Mag. Dr. Christoph Tschohl zu Menschenrechten in der digitalen Welt.

Wie man ein Geschäftsmodell zu Gesundheitsaktivitäten bei der Generali Versicherung gestaltet, erläutere Astrid Koida von der Vitality Deutschland. Über die Formen der Radikalisierung im Internet berichtet der Kriminalhauptkommissar Stefan Malek. Sehr anschaulich stellte Ernst Schulten die Trackingmöglichkeiten im Netz dar. Andreas Sachs vom BayLDA informierte über die Möglichkeiten des Datenschutzes im Netz. Wie Marktforschung funktioniert refererierte Dr. Roland Abold von der GfK Nürnberg. Den Abschluss bildete für das BayLDA Thomas Kranig mit einem Überblick, was sich im Europäischen Datenschutzrecht nun wirklich ändert.

Die Besucher des Daten-Dienstages hatten jeweils nach den Vorträge die Gelegenheit, Fragen zu stellen, aus denen sich oftmals lebhafte Diskussionen entwickelten. Viele der Themen erreichten die Mitte der Gesellschaft erst mit Einführung der DS-GVO mit der öffentlich geführten Diskussion um das Verhältnis von §§ 22, 23 Kunsturhebergesetz und DS-GVO oder die Frage nach der praxisnahen Umsetzung der Transparenzpflicht. Die Diskussion wird fortgeführt werden müssen, stehen wir doch erst am Anfang der Erkenntnisse, wie sich unsere Gesellschaft durch die technischen Möglichkeiten verändern kann und wird.

https://www.mfk-nuernberg.de/datendienstag/

Über den Autor

Rudi Kramer
Rechtsanwalt (Syndikusrechtsanwalt),
DATEV eG, und Sprecher AK Schule des BvD

BvD e.V.
DATENSCHUTZ GESTALTEN

DATENSCHUTZ 2018

Regina Mühlich, Boris Maskow, Sascha Kuhrau, Dr. Jan K. Köcher, Martin Agethen, LL.M., Katharina Schreiner, Peer Lambertz

Regina Mühlich, Boris Maskow, Sascha Kuhrau, Dr. Jan K. Köcher, Martin Agethen, LL.M., Katharina Schreiner, Peer Lambertz
»Datenschutz 2018«

FORUM VERLAG HERKERT GMBH

Auflage 2018
292 Seiten
ISBN-13: 978-3-96314-008-2
65,00 Euro

Das Autoren-/ Herausgeberteam setzt sich aus renommierten Praktikern zusammen, die als externe Datenschutzbeauftragte agieren bzw. in der Rechtsberatung auch zu Datenschutzfragen tätig sind. Das Werk bietet einen fundierten Einstieg und Überblick über die relevanten Fragestellungen. In insgesamt sechs Kapiteln wird das Thema umfassend dargestellt: Einführung und Neuerungen im Überblick, Beschäftigtendatenschutz, Datenschutzbeauftragter, IT-Sicherheit und Datenschutz, Umgang mit personenbezogenen Daten in der Praxis und am Schluss: Rechte der betroffenen Person – Rechts-, Haftungs-, und Zahlungsfolgen bei Verstößen. Die Ausführungen sind praktikerorientiert, klar struktiert und bringen dem Leser selbst komplexe Sacherhalte anschaulich nahe.

Zu den rechtlichen Darstellungen finden sich oftmals Beispiele, die durch Praxistipps angereicht werden. Zusammen mit Kontrollfragen, die sich an einzelne Ausführungen anschließen, helfen Checklisten die Umsetzung der gewonnenen Kenntnisse in der Praxis sicherzustellen.

Natürlich können durch Umfang und Zielrichtung des Werkes nicht alle Fragenstellungen in aller Tiefe erörtert werden. Sie werden aber angesprochen und Lösungsmöglichkeiten angeboten. Positiv hervorzuheben ist zudem, dass sich auch immer wieder Hinweise und Ausführungen zu den Besonderheiten des kirchlichen Datenschutzes finden.

Nicht nur deshalb erweist es sich als umfassendes Kompendium, das über den Einstieg hinausgeht.

Am Ende werden im Anhang die Kontaktdaten der deutschen Aufsichtsbehörden inkl. der kirchlichen Datenschutzaufsichtsbehörden veröffentlicht. Über eine Zip-Datei können zudem von den Seiten des Verlages die erforderlichen Rechtsgrundlagen heruntergeladen werden. Das Werk ist auch als eBook und in einer Print-/Digital-Kombination erhältlich.

Es empfiehlt sich für den Einsteiger wie auch erfahrenen Praktiker und eignet sich sowohl für den Einstieg wie auch für erfahreneren Experten.

BETRIEBLICHER DATENSCHUTZ SCHRITT FÜR SCHRITT - GEMÄSS EU-DATENSCHUTZ-GRUNDVERORDNUNG: LÖSUNGEN ZUR PRAKTISCHEN UMSETZUNG TEXTBEISPIELE, MUSTERFORMULARE, CHECKLISTEN

Grit Reimann

Die Autorin ist nicht nur durch die Erstauflage bekannt, sondern durch die Publizierung systematischer Aufbereitungen zu zahlreichen DIN-Normen und Anforderungskatalogen wie Qualitätsmanagement (DIN ISO 9001), Energiemanagement (DIN ISO 50001), Arbeits- und Gesundheitsschutz (DIN ISO 18001, Umweltmanagement (DIN ISO 14001), Gesundheitsmanagement (DIN ISO 45001). Dem Aufbau des Werkes kommt die Erfahrung der promovierten Didaktikerin zugute.

Grit Reimann
»Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung: Lösungen zur praktischen Umsetzung Textbeispiele, Musterformulare, Checklisten«
Hrsg.: DIN e.V.

Verlag Beuth, Berlin

vollständig überarbeitete und erweiterte 2. Auflage 2018
202 Seiten
ISBN-13: 978-341027981
68,00 Euro
Das Werk ist auch als eBook erhältlich.

In 15 Kapiteln werden die Einleitung, der Aufbau der DS-GVO, die Darstellung personenbezogener Daten und ausgewählte Inhalte, Ausführungen zum Datenschutzbeauftragten, technische und organisatorische Maßnahmen, Datenschutz-Folgenabschätzung inkl. Risikobewertung und Schutzstufenkonzept, betriebliche Regelungen, Auftragsverarbeitung, Drittstaatenthematik, Datenschutz im Personalwesen, vertragliche Regelungen mit Dienstleistern, Schulungen und Unterweisungen, Datenschutzkonzepte, Mindestregelungen und Sanktionen behandelt.

Mit Beispielen und Checklisten werden die einzelnen Themen anschaulich behandelt. Positiv hervorzuheben sind beispielsweise die Empfehlungen zur Gestaltung von Regelwerken zum Datenschutz.

Dass Zuordnungen des Dritten Teil des BDSG (2018) zur Umsetzung der DS-GVO erfolgen, könnte in einer späteren Auflage korrigierend behandelt werden, im Ergebnis ist es inhaltlich noch vertretbar, z.B. Verpflichtungen nach §§ 53 oder 47 BDSG (2018) zum Datengeheimnis und zu den Allgemeinen Grundsätzen für die Verarbeitung personenbezogener Daten auch für die Umsetzung der DS-GVO darzustellen, obwohl diese Paragrafen sich ausschließlich auf die Umsetzung der RL 680/2016 beziehen und die DS-GVO hier keine Öffnungsklauseln vorsieht. Bei manchen Empfehlungen könnte ein Hinweis helfen, dass eine andere Gestaltungsmöglichkeit in der herrschenden Meinung diskutiert wird, wie über Einwilligungen der Beschäftigten zur Übermittlung der erforderlichen Beschäftigtendaten an Reisedienstleister für die Buchung von Dienstreisen.

Insgesamt liegt ein didaktisch gelungenes Werk vor, das die essentiellen Aufgaben im Datenschutz anspricht und durch Checklisten direkte Hinweise zur Umsetzung an die Hand gibt. Dadurch eignet es sich sehr gut, Lehrbücher, Monographien und Kommentare zur DS-GVO sinnvoll zu ergänzen. Es empfiehlt sich für den Einsteiger, aber auch für Praktiker zur Heranziehung zu Einzel- und konkreten Umsetzungsfragen.

Über einen Webzugang erhält der Leser über einen im Buch hinterlegten Zugangscode noch weiteres Zusatzmaterial.

SOZIALRECHTSHANDBUCH (SRH)

Ruland / Becker / Axer (Hrsg.)

Das Werk umfasst alle Aspekte des Sozialrechts. Es ist untergliedert in 5 Teile: Grundlagen, Sozialleistungsträger – Sozialleistungen – Verfahren, Sozialversicherung, die sonstigen Bereiche des Sozialrechts und internationales, supranationales und zwischenstaatliches Sozialrecht. Der Sozialdatenschutz wird in § 10 des zweiten Teils auf 80 Seiten abgebildet und durch die Autoren Wolfgang Binne und Carsten Kremer erörtert. Die Darstellung des Sozialdatenschutzes untergliedert sich in insgesamt 25 Abschnitte. Erfreulich ist, dass bereits die Änderungen, die sich durch die Umsetzung der DS-GVO ergeben, weitestmöglich berücksichtigt werden, wobei die Ausführungen primär die Rechtslage vom Stand August 2017 wiedergeben. Wo es möglich ist, wird aber auf die Änderungen in den SGB, die zum 25.05.2018 wirksam wurden, eingegangen.

So widmen sich bei allen relevanten Punkten eigene Abschnitte den Änderungen durch die DS-GVO wie bei der Darlegung der Begriffsbestimmungen, der Zulässigkeit des Erhebens von Sozialdaten, der allgemeinen Vorgaben für die Verarbeitung, der Zulässigkeit der Übermittlung und der Rechte der Betroffenen. Auch bei der Auftragsverarbeitung schließen sich Ausführungen an, die die Änderungen des § 80 SGB X und die Zusammenhänge zur DS-GVO erläutern. Es werden zudem auch die sich aus der Ausgestaltung der Einschränkung der Betroffenenrechte durch die Änderungen im SGB X ergebenden Fragen kritisch angesprochen.

Ruland / Becker / Axer (Hrsg.)
»Sozialrechtshandbuch (SRH)«

Nomos Verlagsgesellschaft, Baden-Baden

6. Auflage 2018
1.725 Seiten
ISBN-13: 978-3-8487-2792-6
180,00 Euro

Es ist davon auszugehen, dass mit der Umsetzung der DS-GVO im Sozialdatenschutzrecht oftmals erst neue Fragestellungen entstehen, die einer rechtssicheren Beratung entgegenstehen. Hier bietet das Werk eine solide Basis, um Lösungsansätze zu erarbeiten.

Das Sozialrechtshandbuch ist all denen zu empfehlen, die einen umfassenden Überblick zum Sozialrecht suchen, aber auch denjenigen, die eine qualifizierte Darstellung der Aspekte des Sozialdatenschutzes erwarten. Durch die Einbettung in das umfassende Gesamtwerk wird gewährleistet, dass alle Fragen rund um das Sozialrecht behandelt werden.

Rezensionen von

Rudi Kramer
Rechtsanwalt (Syndikusrechtsanwalt),
DATEV eG, und Sprecher AK Schule des BvD

BvD e.V.
DATENSCHUTZ GESTALTEN

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE DES BVD

Die wichtigsten Daten der BvD-Gremien

Die Arbeitskreise und Regionalgruppen sind wichtige Gremien innerhalb des BvD. Detaillierte Informationen zu den Treffen und den Terminen finden Sie unter:

▶ www.bvdnet.de/regionalgruppen **bzw.**
▶ www.bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

04.09.2018	RG Ost	**08.10.2018**	RG Karlsruhe
06.09.2018	RG West	**18.10.2018**	RG Mitte
12.09.2018	AK Soziale	**19.10.2018**	RG Ulm
17.-18.09.2018	AK Medizin	**26.10.2018**	RG München
20.09.2018	RG Gütersloh	**26.10.2018**	RG Nürnberg
20.09.2018	AK EVU	**27.11.2018**	RG Ost
21.-22.09.2018	AK Externe	**29.11.2018**	RG Gütersloh

Sie möchten zu einem Thema aktiv mitmachen oder in Erfahrungsaustausch mit Kollegen treten?

Termine und Anmeldung finden Sie auf unserer Webseite:
▶ www.bvdnet.de

VERNETZEN SIE SICH MIT UNS:

▶ www.bvdnet.de

XING: https://www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

TWITTER: www.twitter.com/bvd_datenschutz

BLOG: www.bvdnet.de/themen/bvd-blog/

RSS-Feed: https://www.bvdnet.de/feed/

BVD-STELLENBÖRSE

Sie suchen ausgewiesenes Datenschutz-Knowhow für Ihr Unternehmen? Mit einer Anzeige in der BvD-Stellenbörse finden

Sie zertifizierte Datenschutzbeauftragte für eine Festanstellung oder als externe Berater. Zur Stellenbörse:
▶ https://www.bvdnet.de/bvd-stellenboerse/

Anzeige

Überblick

Seminare – 2. Halbjahr 2018

Termin	Seminar/ Workshop	Ort
07.09.2018	**Marketing & Werbung nach DS-GVO**	NH Collection Berlin Mitte Referent: Dr. Jens Schulze zur Wiesche
25.09.2018	**Beschäftigtendatenschutz**	NH Hotel Frankfurt Niederrad Referentin: Katja Horlbeck
26.09.2018	**DS-GVO konforme Gestaltung der Webseite**	NH Collection Berlin Friedrichstraße Referent: Heiko Schöning
08.10.2018	**Betroffenenrechte & Auskunftspflichten**	Novotel Frankfurt City Referent: Thomas Kahl
08.11.2018	**Die ePrivacy Verordnung – Seminar**	NH Collection Frankfurt City Referentin: Kristin Benedikt
09.11.2018	**Die ePrivacy Verordnung – Workshop**	NH Collection Frankfurt City Referentin: Kristin Benedikt
22.11.2018	**Datenschutz-Compliance nach DS-GVO – Workshop**	Le Meridien Grand Hotel Nürnberg Referenten: Markus Gierschmann, Andreas Sachs

* nur für BvD Mitglieder

Information und Anmeldung unter www.bvdnet.de

WICHTIGE KONTAKTE

An dieser Stelle informiert Sie der BVD e. V. über aktuelle Kontakte zu Personen, Institutionen und Anbietern sowie wichtigen Partnern. Gerne können Sie sich hier mit Ihrem Angebot, Ihren Dienstleistungen und Ihrem Portfolio präsentieren.

Erfahren Sie mehr darüber und fordern Sie Informationen in der Geschäftsstelle unter bvd-gs@bvdnet.de an.

Software

Es gibt Dinge, die gehen niemanden etwas an.

FOLDERFLEX GERMAN STANDARD

Mehr Sicherheit für Ihre vertraulichen Daten.

www.folderflex.de

Marketing

FÜR DEN BESTEN EINDRUCK

www.tpdigitaldruck.de

Trend Point Marketing GmbH
Breitenbachstraße 24-29 | 13509 Berlin

Datenschutz

Die Seminare der udis: Alles, was man zum Thema Datenschutz wissen muss.

Jetzt informieren unter www.udis.de

udis zert 12345678

Datenschutz geht zur Schule BvD e.V. DATENSCHUTZ GESTALTEN

Datenschutz geht zur Schule – DSgzS
Eine Initiative des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Budapester Straße 31 · 10787 Berlin
Telefon (030) 26 36 77 62 · Telefax (030) 26 36 77 63
dsgzs@bvdnet.de · www.bvdnet.de/dsgzs

Hier könnte Ihre Anzeige stehen!
Jetzt Infos anfordern unter:
bvd-gs@bvdnet.de

Datenschutz

ALLE PFLICHTEN.
ALLES ERKLÄRT.
ALLES NACH PLAN.

Die ca. 50 Pflichten des EU-Datenschutzes sind machbar. Nutzen Sie hierfür unseren Praxisleitfaden!

PRIVAZYPLAN®

www.privazyplan.eu

Auditierung

DSZ
EIN UNTERNEHMEN VON GDD UND BVD

DATENSCHUTZ
Zertifizierungsgesellschaft mbH

Datenschutz Zertifizierung:
unabhängig – transparent – standard-basiert

www.dsz-audit.de

BvD Beitrittserklärung

Bitte in Druckschrift ausfüllen, unterschreiben und per Fax an 030 / 2636 7763, E-Mail: bvd-gs@bvdnet.de oder Post an:

BvD e.V. DATENSCHUTZ GESTALTEN

Berufsverband der
Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Str. 31
10787 Berlin

Wie sind Sie auf uns aufmerksam geworden?*

- ☐ Xing
- ☐ Twitter
- ☐ BvD-News
- ☐ Veranstaltung
- ☐ Internet
- ☐ andere _____
- ☐ persönl. Empfehlung

Anrede:	Vorname:	Name:
Firma:		
Straße:		
Postleitzahl:	Ort:	
Telefon*:	E-Mail*:	

***Freiwillige Angaben. Bitte beachten Sie, dass die Verbandskommunikation überwiegend via E-Mail und Telefon verläuft.**

Ich beantrage eine:

	Einzelmitgliedschaft	Mitgliedsbeitrag/ Jahr
☐	interner/behördlicher Datenschutzbeauftragter	150,00 €
☐	Student (bis 27 Jahre – Nachweis erforderlich)	50,00 €
☐	Rentner / Pensionäre	75,00 €

	Mitgliedschaft Unternehmen	Mitgliedsbeitrag/ Jahr	Anzahl DSB	Anzahl Mitarbeiter gesamt
☐	Externer Datenschutzberater (bis 2 Berater)	250,00 €	1-2	
☐	Unternehmen ab 3 externen Beratern im Datenschutz	125,00 €/ je Berater		
☐	Unternehmen mit internen DSB ab 3 Mitarbeiter	**Beitrag abhängig von Anzahl Mitarbeiter		
☐	AöR, Kliniken, Hochschulen, Universitäten, etc.	250,00 €		

(**Der Jahresbeitrag kann vorab angefragt werden und wird Ihnen schriftlich mitgeteilt)

Bei einer Firmenmitgliedschaft wird das Stimmrecht ausgeübt durch: ……

☐ Informationen per E-Mail an die o. g. E-Mail-Adresse durch den BvD über Veranstaltungen, welche der BvD (mit-) organisiert oder an denen der BvD sonst (bspw. durch Referenten oder Vorträge) beteiligt ist und/oder für welche die Mitglieder Vergünstigungen erhalten, erwünscht. Eine Verpflichtung des BvD zur Information hierüber an die Mitglieder wird dadurch nicht begründet.

☐ Ich möchte die Zeitschrift DuD - Datenschutz & Datensicherheit abonnieren und stimme der Weiterleitung der Daten an den Verlag zum Bezug der Zeitschrift DuD - Datenschutz & Datensicherheit zu. Sofern ein Abonnement abgeschlossen wird, ist dieses direkt und allein mit dem Verlag geschlossen. Vorzugspreis für BvD-Mitglieder: 139,25 € netto zzgl. Versandkosten 16,82 € netto.

☐ Ich zahle via Rechnung

☐ Ich zahle via Lastschriftverfahren
(Bitte füllen Sie das Formular zur Erteilung einer Einzugsermächtigung und eines SEPA-Lastschrift-Mandats aus und fügen es der Beitrittserklärung bei)

Ich bin (freiwillige Angaben):

☐ interner DSB

☐ externer DSB

Anzahl betreuter Unternehmen: ☐
Anzahl Mitarbeiter der betreuten Unternehmen gesamt: ☐

Ich erkenne die Satzung (www.bvdnet.de) und die in der Satzung genannten Ziele des Vereins an.
Meinen Mitgliedsbeitrag überweise ich nach Erhalt meiner Beitrittsbestätigung auf das dort angegebene Konto.

Ort _____ Datum _____ Unterschrift _____

Anzeige

Verfügbar als App für iOS und Android oder online im Web-Browser:

Die wichtigsten Tipps und Meinungen zur Datenschutz-Grundverordnung. In der Sonderausgabe der SERVICETODAY.

Exklusiv in der SERVICETODAY App und online: Direkt herunterladen und informieren.

- » Exklusives Interview mit EU-Verhandlungsführer Jan Philipp Albrecht
- » Sabrina Brameshuber von Bitkom Consult zu Custom Audiences
- » Die DSGVO im Service bei SAP-Anwendern
- » Datenschützer Jürgen Hartz im Porträt
- » Datenschutz im Personalbereich: Darauf müssen Recruiter achten
- » Experten von Eversheds Sutherland zur Datenschutzgrundverordnung im Arbeitsverhältnis
- » Serview-Experte Torsten Schneider zum Bundesdatenschutzgesetz
- » Dr. Jens Eckhardt über Bußgelder
- » und vieles mehr

Jetzt im App Store von iOS und Android, bei Amazon und online unter **www.kvd.de**

KVD DER SERVICE-VERBAND

Pliesterbecker Straße 165 | 46284 Dorsten | Tel: 02362 . 9873 - 0 | Fax: 02362 . 9873 - 98 | E-Mail: gs@kvd.de | Internet: www.kvd.de

Anzeige

Datenschutz im Fokus.

ZD – Zeitschrift für Datenschutz
8. Jahrgang 2018. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.
Jahresabonnement € 245,–
Vorzugspreis für BvD-Mitglieder,
für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 185,–.
Vorzugspreis für Studenten und Referendare € 119,–
Abbestellung bis 6 Wochen vor Jahresende.
Preise jeweils inkl. MwSt. zzgl. Vertriebs-/Direktbeorderungsgebühren Inland (€ 13,80/€ 5,–) € 18,80 jährlich.

Mehr Informationen:
www.beck-shop.de/go/ZD

Die große Zeitschrift zum Datenschutz

Die ZD informiert umfassend über die relevanten datenschutzrechtlichen Aspekte aus allen Rechtsgebieten und begleitet die nationale sowie internationale Gesetzgebung und Diskussion um den Datenschutz. Im Mittelpunkt stehen Themen aus der **Unternehmenspraxis** wie z. B.
■ Datenschutz-Grundverordnung ■ Konzerndatenschutz ■ Beschäftigtendatenschutz ■ **Datenschutz-Folgenabschätzung** ■ Compliance ■ Kundendatenschutz ■ Telekommunikation ■ Soziale Netzwerke ■ Datentransfer in Drittstaaten ■ Vorratsdatenspeicherung ■ Informationsfreiheit ■ **Profiling und Scoring** ■ Tracking.

Geschaffen für die Unternehmenspraxis

Jedes Heft enthält ein Editorial, Aufsätze mit Lösungsvorschlägen, Angaben zur Lesedauer, Abstracts in Deutsch und Englisch, Schlagwortketten, Entscheidungen mit Anmerkungen und aktuelle Meldungen.

Alles inklusive:

- Online-Modul ZDDirekt – vollständiges Online-Archiv ab ZD 1/2011
- 14-täglicher Newsdienst ZD-Aktuell
- Homepage **www.zd-beck.de**
- Fundstellen-Recherche in beckonline.

3 Hefte gratis

Bestellen Sie das kostenlose Schnupperabo unter www.beck-shop.de/go/ZD.

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 158812

C.H.BECK