Ausgabe 01/2021

ISSN: 2194-1025

# BvD-NEWS

Das Fachmagazin für den Datenschutz

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

## LOTSE DURCH DIE BÜROKRATIE

DATENSCHUTZBEAUFTRAGTE UND DIE EVALUIERUNG DES BDSG


**DOKUMENTATION: EVALUIERUNG DES BDSG** – S. 8

**PRIVACY LITIGATION** – S. 16

**NEUE EDSA-EMPFEHLUNGEN UND SCC-ENTWÜRFE IM LICHTE VON „SCHREMS II“** – S. 34

**DAS GESCHÄFTSGEHEIMNISGESETZ** – S. 46


BvD e.V.

DATENSCHUTZ GESTALTEN

Anzeige

www.bvdnet.de

2021

# BvD-Verbandstage & Behördentag | 19.05. - 21.05.2021

LIVE AUS DEM ELLINGTON HOTEL BERLIN.

BvD e.V.
DATENSCHUTZ GESTALTEN

## Next Level Datenschutz.
Der Datenschutzbeauftragte als Lotse in der Digitalisierung

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

## AKTUELLE UND PRAXISNAHE VORTRÄGE UND DISKUSSIONEN ZU DEN FOKUS-THEMEN:

- Datenschutz-To-dos digital & virtuell
- Datenschutz in der Praxis
- Bußgelder – Schadensersatzforderungen
- Digitale Welten
- Next Level Datenschutzbeauftragter

» Im Anschluss an die BvD-Verbandstage findet der Behördentag statt. Hier informieren Vertreter aus Behörden und Kommunen über aktuelle Themen zum Datenschutz und der Digitalisierung in Verwaltung und Ämtern.

## TEILNAHMEGEBÜHREN:

**BvD-Verbandstage 19.05.-20.05.2021**
BvD-Mitglieder: 695,00 €
Nichtmitglieder: 895,00 €

**BvD-Verbandstage 2021 – Tages-Ticket**
BvD-Mitglieder: 450,00 €
Nichtmitglieder: 550,00 €

**Behördentag 21.05.2021**
BvD-Mitglieder und öffentliche Einrichtungen/Behörden: 295,00 €
Nichtmitglieder: 450,00 €

**BvD-Verbandstage & Behördentag 19.05.-21.05.2021**
BvD-Mitglieder, öffentliche Einrichtungen/Behörden: 895,00 €
Nichtmitglieder: 1.150,00 €

Alle Preise zzgl. gesetz. MwSt.

## JETZT ANMELDEN:

https://www.bvdnet.de/termin/save-the-date-bvd-verbandstag-2021/

BERUFSVERBAND DER DATENSCHUTZBEAUFTRAGTEN DEUTSCHLANDS (BVD) E.V. | BUDAPESTER STRASSE 31, 10787 BERLIN

# EDITORIAL

## Liebe Leserinnen und Leser,

diese Ausgabe der BvD-News soll mit einem großen Dankeschön beginnen, das sich an Frau Helga Block (LDI NRW) und Herrn Prof. Dr. Michael Ronellenfitsch (HBDI) richtet, die den BvD während ihrer Amtszeiten wohlwollend und partnerschaftlich begleitet haben. Für die vertrauensvolle Zusammenarbeit bedanken wir uns und wünschen beiden alles Gute für die neue Lebensphase, den Ruhestand. Frau Block ist offiziell bereits im Juli 2020 in den Ruhestand gegangen, aber noch ohne Nachfolge, und in Hessen wurde Prof. Dr. Ronellenfitsch am 25. Februar 2021 in den Ruhestand verabschiedet.

Am 25. Mai 2018 trat das neue Bundesdatenschutzgesetz in Kraft. Spätestens drei Jahre später – also in diesem Frühjahr – ist eine Evaluierung vorgesehen. Wie schon bei der Evaluierung der DSGVO im vergangenen Frühjahr, bringt sich der BvD natürlich auch in diesen vom Bundesministerium des Innern, für Bau und Heimat (BMI) koordinierten Prozess aktiv ein. Dabei ist es unser Ziel, mit unseren aus Praxiserfahrungen gespeisten Vorschlägen insbesondere zur Entlastung des Mittelstands beizutragen. Es geht aber auch darum, der in diesem Kontext immer wieder drohenden Täuschung vorzubeugen, der DSB sei quasi die Personifizierung der bestehenden datenschutzrechtlichen Pflichten und „weniger DSB" bedeute daher „weniger Datenschutzbürokratie". Das Gegenteil ist der Fall: Der DSB hilft, die unabhängig von ihm bestehende Bürokratie zu meistern; er ist der versierte „Lotse durch die Bürokratie", wie es der Titel unserer BvD-News so treffend formuliert. Und: Wenn die Politik die gesetzlichen Voraussetzungen dafür schaffen würde, könnte er diese Aufgabe sogar noch viel besser erfüllen, als es ihm aufgrund der geltenden Regelungen derzeit möglich ist. Was sich ändern müsste, das haben der BvD-Vorstand und unser Ausschuss Recht & Politik anhand ganz konkreter Vorschläge erarbeitet, die Sie in den Artikeln zu unserem Themenschwerpunkt nachlesen können.

Wer als DSB-„Lotse" Unternehmen dabei begleitet datenschutzrechtliche Klippen zu umschiffen, der muss über diese Klippen natürlich bestens Bescheid wissen. Eine davon, die gerade aufgrund aktueller Urteile an Bedeutung gewinnt, ist die Gefahr von Schadensersatzklagen nach Art. 82 DSGVO. Der Artikel von Tim Wybitul (s. Seite 22) bringt Sie hierzu auf den neuesten Stand. Schon lange in der Diskussion ist hingegen das Thema Drittlandtranfers, es scheint sich zu einem Dauerbrenner zu entwickeln, der uns Datenschutzbeauftragte noch eine ganze Weile beschäftigen wird. In der vorliegenden Ausgabe schreiben Dr. Tilman Dralle, Jonathan Schröer und Dipl.-Wi.-Ing. Dominik Smasal ab Seite 34 über die neuen Empfehlungen des Europäischen Datenschutzausschusses und die Standarddatenschutzklauseln im Zusammenhang mit "Schrems II". Zu den ESDA-Empfehlungen hat übrigens auch unser europäischer Dachverband EFDPO Stellung genommen, nachzulesen unter www.efdpo.eu. Mit welchen Problematiken man sich bei der Nutzung von Standarddatenschutzklauseln auseinandersetzen muss, erläutert Prof. Dr. Tobias Straub ab Seite 40.

Nicht nur mit diesen und den vielen weiteren Artikeln des vorliegenden Hefts können Sie als DSB Ihr Know-How auf den aktuellen Stand bringen, auch die BvD-Verbandstage mit dem anschließenden Behördentag warten wieder mit einer geballten Ladung an Fachwissen auf. Sie sind herzlich eingeladen sich den 19. bis 21. Mai frei zu halten. Aufgrund der derzeitigen Lage können wir leider noch immer nicht alle gemeinsam in Berlin zusammenkommen, daher bauen wir im Ellington Hotel professionelle Livestream-Studios auf, aus denen die Referenten zu Ihnen auf die heimischen Bildschirme kommen werden. Trotz der räumlichen Entfernung werden wir alle Hebel in Bewegung setzen, um bei Ihnen ein echtes Kongressfeeling aufkommen zu lassen – zum Beispiel dadurch, dass Sie dieses Jahr nicht auf die Gala zur Preisverleihung unseres Datenschutz Medienpreises DAME verzichten müssen. Welche Beiträge die Jury für den vierten Jahrgang nominiert hat, lesen Sie auf Seite 80.

Spätestens zur Herbstkonferenz wollen wir dann wieder ein „echtes Treffen" möglich machen. Damit dies selbst bei gegebenenfalls noch bestehenden Hygienevorschriften möglich ist, haben wir uns bereits eine ausreichend große Location in Nürnberg gesichert.

Bis dahin wünsche ich Ihnen gutes Durchhalten, Gesundheit und natürlich eine anregende Lektüre.

Ihr

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
www.bvdnet.de/feed/

**Redaktion:**
Christina Denz (chd)
V.i.S.d.P.: Thomas Spaeing
bvd-news@bvdnet.de

**Fotos:**
www.123rf.com

**Lektorat:**
Frank Spaeing, Regina Mühlich

**Anzeigen:**
Christina Denz
Kooperationen: Karsten Füllhaase
(bvd-gs@bvdnet.de)

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

ISSN: 2194-1025
Erscheinungsweise: 3 x jährlich, Druckauflage 4.000 Exemplare (Unsere Mediadaten erhalten Sie unter bvdnet.de/Publikationen oder von unserer Geschäftsstelle per E-Mail an 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

*Thomas Spaeing* 3

## LOTSE DURCH DIE BÜROKRATIE

Die Stellung und Tätigkeit des DSB in der politischen Diskussion. Drei Positionen des BvD – *Von den Mitgliedern des BvD-Ausschusses Recht & Politik* 5
Dokumentation: Evaluierung des BDSG. Eckpunkte aus der Stellungnahme des BvD 8

## DSGVO

Privacy Ligitation. Von Betroffenenrechten über Unterlassungsansprüche bis hin zum Schadensersatzanspruch nach DS-GVO – *Thomas Kahl* 16
DSGVO-Schadensersatzklagen nach dem Paukenschlag des Bundesverfassungsgerichts – *Tim Wybitul* 22
Die Strafbarkeit juristischer Personen nach Art. 83 DSGVO. Ein Stolperstein für die einheitliche Anwendung der DSGVO – *Dr. Matthias Schmidl* 26
§§ 30, 130 OWiG vor der Herausforderung einer europaweit harmonisierten Bebußung nach Art. 83 DS-GVO – *Maria Christina Rost* 30

## GESETZ UND RECHTSPRECHUNG

Neue EDSA-Empfehlungen und SCC-Entwürfe im Lichte von „Schrems II": Entwicklungen und Perspektiven – *Dr. Tilman Dralle, LL.M., Jonathan Schröer, LL.M. und Dipl.-Wi.-Ing. Dominik Smasal* 34
Privacy Shield – der Vorhang zu und alle Fragen offen? – *Prof. Dr. Tobias Straub* 40
Das Geschäftsgeheimnisgesetz. Von Compliance und konkreten Maßnahmen bis zur Durchsetzung von Ansprüchen – *Regina Mühlich, Dr. Jens Eckhardt* 46

## DATENSCHUTZPRAXIS

Umgang mit Datenschutzpannen – *Stefan Sander* 50
Consent Tools für Webseiten im Praxistest – *Dr.-Ing. Klaus Meffert* 56
Datenschutzbeauftragte im Gesundheitswesen – eine spezielle Herausforderung – *Bernd Schütze* 61
Mittelstand-Digital. Kompetenzzentren unterstützen den Mittelstand bei der Digitalisierung – *Christian Munk* 71

## AUFSICHTSBEHÖRDEN

100. Datenschutzkonferenz – Die wichtigsten Ergebnisse und Entscheidungen im Überblick – *Andreas Schurig* 74

## GESELLSCHAFT

Vertraulichkeit und Verschwiegenheit. Wie weit geht die gesetzliche Verschwiegenheitspflicht des Datenschutzbeauftragten? – *Regina Mühlich, Dr. Jens Eckhardt* 77

## AUS DEM VERBAND

Datenschutz Medienpreis 2020: Jury gibt drei Finalisten bekannt – *Karsten Füllhaase* 80
Wo DSgzS-Dozenten noch was lernen – Der Dozententag der BvD-Initiative „Datenschutz geht zur Schule" fand 2020 online statt – *David Heimburger* 82

## REZENSIONEN

Die datenschutzrechtliche Einwilligung – *Marlene Voigt* 84
Datenschutzbeauftragte - Einsteigerlektüre für Anfänger – *Stephan Hansen-Oest* 86
DSGVO im Praxistest - Ermittlungen Bußgelder Verfahren – *Niko Härting, Lasse Konrad* 88
Datenverarbeitung in Drittstaaten. Komplexe Regelungen einfach erklärt. – *Dr. Jens Eckhardt, Bernd Fuhlert* 90

## TERMINE UND KONTAKTE

Termine der Regionalgruppen und Arbeitskreise des BvD 91

# DIE STELLUNG UND TÄTIGKEIT DES DSB IN DER POLITISCHEN DISKUSSION

## Drei Positionen des BvD

Von den Mitgliedern des BvD-Ausschusses Recht & Politik

Die Stellung und Tätigkeit des Datenschutzbeauftragten (DSB) ist immer wieder Gegenstand (rechts-) politischer Diskussionen. Typischerweise geht es dabei darum seine Stellung oder seine Tätigkeit einzugrenzen. Entweder wird ihm vorgeworfen, dass der Datenschutzbeauftragte die mit der DSGVO verbundene Bürokratie verursacht oder – wenn er seine Aufgabe ausfüllt – dass er unerlaubte Rechtsberatung erbringt. Beides ist falsch, bietet aber den Vorteil einer einfachen Sicht auf die Dinge. Um diese oberflächlich einleuchtende Kritik zu entkräften, ist hingegen eine Bereitschaft zu einer tiefergehenden Betrachtung mit der Thematik erforderlich.

Der Ausschuss Recht & Politik des BvD hat als Antwort auf diese oberflächliche Sichtweise drei klare politische Positionen zum Selbstverständnis und zur Stellung des DSB formuliert:

### Die Datenschutzbeauftragten: Wir gestalten Datenschutz

Die DSGVO bietet dem deutschen Gesetzgeber die Möglichkeit die Rolle des Datenschutzbeauftragten stärker als proaktiven Gestalter für das Unternehmen, weniger als reaktiven Überwacher zu formulieren. Ein DSB unterstützt Unternehmen (und insbesondere KMU) bei der Gestaltung ihrer Verarbeitungsprozesse. DSB liefern den Unternehmen die dringend benötigten Informationen für eine den Vorgaben des Datenschutzes genügende und dabei zugleich den Geschäftsprozessen entsprechende Modellierung ihrer Prozesse. Der DSB ist Gestalter, kein Bedenkenträger.

Unsere Forderung an die Politik ist daher, die Rolle des Datenschutzbeauftragten im BDSG dementsprechend stärker als Unterstützer auszugestalten. Seine Einbindung in die Gestaltung der Verarbeitung personenbezogener Daten zu stärken und dem Datenschutzbeauftragten die Möglichkeit zu eröffnen einzelne Aufgaben des Unternehmens nach der DSGVO zu übernehmen. Denn vor allem dort, wo der DSB nicht beratend und begleitend von Anfang an eingebunden ist, muss er ggf. im Nachgang im Rahmen seiner Beratung auf die Versäumnisse hinweisen und Handlungsempfehlungen geben.

Eine nachträgliche Justierung und/oder gar umfassende Prozessmodulation ist kosten- und zeitintensiv und führt zu unnötigen Verzögerungen. Mit einer frühzeitigen Einbindung, z.B. bereits in der Konzeptionsphase, kann durch den DSB eine effektive Entlastung der Unternehmensleitung und eine Nutzung des Know-hows zur Gestaltung der Nutzung personenbezogener Daten erreicht werden.

### Die Erfüllung der durch Art. 39 DSGVO vorgegebenen Aufgabe verstößt nicht gegen das Rechtsdienstleistungsgesetz (RDG).

Dem DSB ist durch die DSGVO eindeutig die Aufgabe der Beratung zugewiesen. Das schließt nach dem Selbstverständnis der DSGVO zwingend die Beratung zu allen Aspekten des Datenschutzes ein, natürlich ggf. auch zu datenschutzrechtlichen Themen. Die in Deutschland geführte Diskussion, dass dies vermeintlich gegen das Rechtsdienstleistungsgesetz (RDG) verstößt, berücksichtigt nicht die klaren europarechtlichen Vorgaben. Eine Einschränkung der Tätigkeit des DSB bei der Beratung auch in datenschutzrechtlichen Fragen durch eine Vorschrift eines Mitgliedsstaates verstößt gegen die höherrangige Vorgabe zur Beratung durch eine europäische Verordnung. Zudem ist festzustellen, dass die DSGVO nicht zwischen externen und internen Datenschutzbeauftragten unterscheidet, für beide gelten dieselben europarechtlichen Regelungen.

Weiterhin sprechen Umfang und Inhalt der nicht als Rechtsdienstleistung zu qualifizierenden Aufgaben

sowie der enge sachliche Zusammenhang zwischen den rechtsberatenden und den nicht-rechtsberatenden in der DSGVO genannten Aufgaben dafür, dass die durch einen Datenschutzbeauftragten zu erbringenden Leistungen dem deutschen Begriff der Rechtsdienstleistung nicht entsprechen. Aber selbst nach deutschen Recht ist eine rechtsberatende Tätigkeit, welche "im Zusammenhang mit einer anderen Tätigkeit, wenn sie als Nebenleistung zum Berufs- oder Tätigkeitsbild" erfolgt, entsprechend §5 Abs. 1 RDG zulässig.

Diese von einer Minderheit geführte Diskussion bindet jedoch Ressourcen, führt gerade in kleinen und mittelständischen Unternehmen, denen eine eigene juristische Abteilung nicht die rechtlichen Vorgaben erklären kann, zu einer Unsicherheit und verhindert so die Nutzung der Potentiale beim frühzeitiger Einbeziehung eines Datenschutzbeauftragten: Die proaktiv unterstützende Funktion des DSB im Unternehmen wird durch diese unnötige Diskussion behindert, wenn nicht gar verhindert.

Der BvD fordert den Bundesgesetzgeber daher auf, anlässlich der Evaluierung des BDSG und der Überarbeitung des RDG klarzustellen, dass bei der Erfüllung ihrer gesetzlichen Aufgaben erfolgende Beratungsleistung auch für externe Datenschutzbeauftragte keine Kollisionen zum RDG entsteht.

## Eine Entlastung ist nur durch Entflechtung und Harmonisierung des Datenschutzrechts möglich.

Der BvD fordert den Gesetzgeber auf, auf eine fokussierte, anstatt bürokratisierte Dokumentationspflicht hinzuwirken.

Die Hauptbelastung für Unternehmen unter der DSGVO und dem BDSG ist nicht die Einhaltung der Zulässigkeit der Verarbeitung. Die als unnötige Bürokratie empfundenen Anforderungen der DSGVO und des BDSG liegen vielmehr in der Vielzahl unterschiedlicher Dokumentationspflichten, die sich inhaltlich auch noch überschneiden, aber eben nicht deckungsgleich sind. Um nur einen Ausschnitt zu nennen, treffen das Unternehmen Dokumentationspflichten nach Artt. 5 Abs. 2, 13, 14, 30, 32 DSGVO. Diese überschneiden sich, sind aber nicht deckungsgleich. Dennoch ist jede dieser Dokumentationspflichten für sich mit einem Bußgeld bewehrt. Die Unternehmensleitung ist damit im Rahmen des Datenschutzes mehr damit beschäftigt, Dokumentationen stets aktuell zu halten, als sich mit der eigentlichen Frage der Zulässigkeit der Verarbeitung zu befassen.

Der BvD erkennt und anerkennt den Zweck dieser Dokumentationspflichten als Absicherung der Einhaltung der DSGVO, fordert aber anstatt vieler undifferenzierter Regelungen eine Fokussierung durch das BDSG. Eine effiziente Zielerreichung und größere Akzeptanz sind besser durch eine fokussierte Vorgabe realisierbar.

Der BvD fordert den Gesetzgeber auf, von seinen Gestaltungsmöglichkeiten Gebrauch zu machen, um unnötige Bürokratie abzuschaffen, zugunsten von Hinweisen in klarer und einfacher Sprache.

**Die DSGVO ist von detailverliebter Bürokratie im Klein-Klein geprägt, da:**

- zu viele Informationen gegeben werden, die dann dazu führen, dass betroffene Personen die wesentlichen Informationen nicht mehr wahrnehmen (Information-Overkill),
- Selbstverständlichkeiten endlos wiederholt werden,
- rechtliche Formalia gegenüber den inhaltlich wesentlichen Aussagen dominieren,
- die Zeitpunkte und Situationen nicht dazu beitragen, dass Inhalte ernsthaft wahrgenommen werden können,
- Informationspflicht und Informationsrecht sich in einem Spannungsfeld befinden,
- die Rechenschaftspflicht zu einer der Einwilligung gleichenden Verfahrensweise mit immensem Aufwand führt,
- die hohen Aufwände von Unternehmen nur einen geringen Beitrag zur Verbesserung der Transparenz leisten.

Ein Musterbeispiel für unnötige Bürokratie ist die Pflicht zur proaktiven Mitteilung der Rechtsgrundlagen in jedem Hinweis an die betroffene Person. Für die durchschnittliche betroffene Person bedeutet die Angabe des Gesetzestextes „Art. 6 Abs. 1 S. 1 lit. f DSGVO", „Art. 6 Abs. 1 S. 1 lit. a DSGVO" oder „Art. 6 Abs. 1 S. 1 lit. b DSGVO" keinen Informationsmehrwert. Gerade diese Pflicht ist aus Sicht der KMU ein Paradebeispiel für die beklagte Bürokratisierung des Datenschutzes.

Der BvD fordert den Gesetzgeber auf, von seinen in der DSGVO enthaltenen Gestaltungsmöglichkeiten hinsichtlich der nationalen Bundes- und Landesgesetzgebung Gebrauch zu machen, um Bürokratie in der Breite durch eine Vielzahl sich überschneidender Regelungen einerseits und detailverliebte Einzelregelungen ohne Informationsmehrwert für den Betroffenen andererseits abzuschaffen. In dieser Hinsicht sollte das BDSG überarbeitet werden. Desgleichen sollten die deutschen Bundes- und Landesgesetze zum Datenschutz besser aufeinander abgestimmt werden. Durch wenige, klare Regelungen wird für die betroffenen Personen der Zweck der DSGVO erreicht, jedoch mit signifikant weniger Aufwand für Verantwortliche.

## Die BvD-Position auf den Punkt gebracht:

- Die Rolle des DSB ist stärker als proaktiver Gestalter für das Unternehmen und weniger als reaktiver Überwacher auszugestalten.
- Es ist klarzustellen, dass durch die Beratungsleistung (auch externer) Datenschutzbeauftragter bei der Wahrnehmung ihrer aus der DSGVO resultierenden gesetzlichen Aufgaben keine Kollisionen zum RDG entsteht.
- Bürokratie ist abzuschaffen – sowohl in der Breite (verursacht durch eine Vielzahl sich überschneidender Regelungen) als auch in der Tiefe (verursacht durch zu detaillierte Einzelregelungen).

Entsprechend dieser strategischen Ziele hat sich der BvD in der aktuellen Befragung des Bundesministeriums des Innern, für Bau und Heimat (BMI) zur Evaluation des BDSG in Bezug auf den DSB nichtöffentlicher Stellen eingebracht. Die Position dokumentieren wir in Auszügen nachfolgend. Insbesondere verweisen wir auf die Stellungnahme zur Einschätzung von § 38 BDSG auf Seite 11.

## Über die Autoren:

Der Ausschuss Recht & Politik im BvD begleitet die Evaluierungsprozesse von BDSG und DSGVO und bezieht darüber hinaus Stellung zu weiteren aktuellen Gesetzesvorhaben. Er unterstützt den Vorstand dabei, Positionspapiere und Kommentare zur Rolle der Datenschutzbeauftragten zu erstellen. Der Ausschuss wird von BvD-Justiziar Dr. Jens Eckhardt geleitet, weitere Mitglieder sind Regina Mühlich, Rudi Kramer, Bernd Schütze und Andrea Backer-Heuveldop.

Anzeige

**Datenschutz-Kontrolle** für die Websites Ihrer Kunden

decareto

Wir schützen Unternehmen vor Abmahnungen und Bußgeldern durch automatisierte Datenschutz-Prüfung ihrer Websites.

**Schwachstellen schnell entdecken**

Unsere Lösung entdeckt Cookies und Tracker, die ohne Einwilligung geladen werden, warnt bei Datenübermittlung in unsichere Drittstaaten, entdeckt Lücken in der Datenschutzerklärung, und vieles mehr. In Echtzeit und für beliebig viele Websites gleichzeitig.

**Sie sparen Zeit und verbessern Ihren Service**

Das decareto-Dashboard zeigt den Risiko-Score aller Ihrer Kunden auf einen Blick, mit detaillierten Reports in Ihrem eigenen Branding beschleunigen Sie die Erstellung von Audits und Schwachstellen-Bewertungen.

decareto GmbH Hochfeld 1b 22607 Hamburg info@decareto.de

# DOKUMENTATION: EVALUIERUNG DES BDSG

## Eckpunkte aus der Stellungnahme des BvD

*Für das am 25. Mai 2018 in Kraft getretene neue Bundesdatenschutzgesetz ist eine Evaluierung spätestens drei Jahre nach Inkrafttreten vorgesehen. Diese Evaluierung führt das Bundesministerium des Innern, für Bau und Heimat (BMI) durch und hat dazu in einem ersten Schritt im November 2020 einen Fragebogen versendet, den der BvD am 15.01.2021 beantwortet eingereicht hat. Ein Auszug der Antworten werden in diesem Artikel vorgestellt.*

### Teil 1
### I. Anwendungsbereich und Begriffsbestimmungen

*Frage des BMI im Rahmen der Evaluation:* „1. Ist der Anwendungsbereich in § 1 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

**Stellungnahme des BvD:** Nein. Es ist problematisch, dass durch das BDSG sowohl die Anpassungen an die DSGVO vorgenommen werden als auch die Umsetzung der JR-Richtlinie erfolgt. Dies führt zu einer unnötigen Verkomplizierung des Anwendungsbereichs des BDSG und zieht sich wie ein roter Faden durch die „Gemeinsamen Bestimmungen" und zwingt dann zu einer weiteren Festlegung des jeweiligen Anwendungsbereichs der Teile 2 und 3. Eine Ausgliederung der Umsetzung der JR-Richtlinie in ein eigenständiges Gesetz dient der Rechtsklarheit (siehe Definitionskatalog) und der Anwendungsklarheit (Entbehrlichkeit der Abgrenzung von Teil 2 und 3).

*Frage des BMI im Rahmen der Evaluation:* „2. Ist der Anwendungsbereich in § 45 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

**Stellungnahme des BvD:** In unserem Verband sind keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten, daher verzichten wir auf eine entsprechende Kommentierung.

*Frage des BMI im Rahmen der Evaluation:* „3. Sind die Begriffsbestimmungen in § 2 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

**Stellungnahme des BvD:** Die Begriffsbestimmungen in § 2 BDSG sind aus unserer Sicht – jedenfalls teilweise – nicht normenklar und damit auch nicht praktikabel. Es gibt öffentliche Stellen, die nur teilweise am Wettbewerb teilnehmen und bei denen sich die Frage stellt, ob sie als nichtöffentliche Stelle gelten. Eine Klarstellung könnte durch die Formulierung "ganz oder teilweise" in Absatz 5 Satz 1 erreicht werden.

### II. Rechtsgrundlagen für die Datenverarbeitung

*Frage des BMI im Rahmen der Evaluation:* „1. Sind die Rechtsgrundlagen für die Datenverarbeitung in den §§ 3, 4, 22, 23 und 24 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

**Stellungnahme des BvD:**

- Die Rechtsgrundlagen für die Datenverarbeitung in § 3 BDSG sind nur dann sachgerecht, praktikabel und normenklar geregelt, wenn die Aufgaben der öffentlichen Stellen in den jeweiligen Fachgesetzen so geregelt sind, dass die Aufgaben in den Fachgesetzen hinreichend genau beschrieben sind und somit die Erforderlichkeit beurteilbar ist.
- Mit Blick auf das Urteils des BVerwG vom 7. März 2019 (AZ. 6 C 2.18 ) ist klargestellt, dass § 4 BDSG im Anwendungsbereich der DSGVO nicht mehr angewendet werden darf. Dies muss gesetzlich durch die Streichung des § 4 BDSG im Teil „Gemeinsame Bestimmungen" klargestellt werden. Hier manifestiert sich die eingangs geäußerte Kritik an der gemeinsamen Anpassung an DSGVO und Umsetzung der JR-Richtlinie in einem Gesetz. Es sollte eine Anpassung an die DSGVO einerseits und Umsetzung der JR-Richtlinie in verschiedenen Gesetzen erfolgen und § 4 BDSG – wenn überhaupt – in dem Gesetz zur Umsetzung der JR-Richtlinie genannt werden.

**Die Rechtsgrundlagen für die Datenverarbeitung in § 22 BDSG sind nicht sachgerecht, praktikabel und normenklar geregelt.**

a. Die Vorgaben in § 22 Abs. 2 BDSG enthalten teilweise dieselben Anforderungen wie Art. 32 DSGVO:

- Pseudonymisierung
  - ▶ Art. 32 Abs. 1 Buchst. a DSGVO: Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - ▶ § 22 Abs. 2 Ziff. 6 BDSG: Pseudonymisierung personenbezogener Daten;
  - ▶ § 22 Abs. 2 Ziff. 7 BDSG: Verschlüsselung personenbezogener Daten
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
  - ▶ Art. 32 Abs. 1 Buchst. b, c DSGVO: die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
  - ▶ § 22 Abs. 2 Ziff. 8 BDSG: Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
  - ▶ Art. 32 Abs. 1 Buchst. d DSGVO: ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
  - ▶ § 22 Abs. 2 Ziff. 9 BDSG: zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Daher wird zur Erhöhung der Rechtssicherheit vorgeschlagen, auf die Wiederholung der Vorgaben der DSGVO zu verzichten, d.h. § 22 Abs. 2 Ziff. 6, 7, 8, 9 BDSG zu entfernen.

b. § 22 Abs. 2 Ziff. 1 beinhaltet die Vorgabe, die Verarbeitung besonderer Kategorien personenbezogener Daten so durchzuführen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt. Jede Verarbeitung personenbezogener Daten, welche nicht den Anforderungen der Verordnung (EU) 2016/679 genügt, erfolgt rechtswidrig. Eine Aufforderung, sich an europäisches Recht zu halten, erscheint nicht zielführend. Daher wird empfohlen, § 22 Abs. 2 Ziff. 1 BDSG zu entfernen

- Die Erfordernis, ob die Vorgaben in § 22 Abs. 2 BDSG verpflichtend bei der Verarbeitung besonderer Kategorien personenbezogener Daten zu beachten sind, wird unterschiedlich ausgelegt. Einerseits ist der Wortlaut „können dazu insbesondere gehören", was nahelegt, dass der Verantwortliche selbst entscheidet, ob er die Maßnahmen berücksichtigt. Andere Autoren leiten eine Pflicht zur Beachtung aus der Formulierung ab, d.h. der Verantwortliche muss ihrer Ansicht nach begründen, wenn er diese Vorgaben nicht berücksichtigt. Hier wäre vorteilhaft, den Wortlaut bzgl. der Berücksichtigung der Aufzählung an den Wortlaut der DSGVO anzugleichen, so dass hier die Kommentarliteratur zur DSGVO analog herangezogen werden kann.
- Die **Rechtsgrundlagen** für die Datenverarbeitung in **§ 23 BDSG sind nur zum Teil sachgerecht, praktikabel und normenklar geregelt.**

a. Die Regelung in Ziffer 5 ist nicht normenklar, da „schwerwiegenden Beeinträchtigung der Rechte einer anderen Person" unklar ist. Daher wird vorgeschlagen, hier stattdessen auf die Erforderlichkeit zum Schutz lebenswichtiger Interessen einer anderen natürlichen Person abzustellen.

b. In Ziffer 6 werden die Verarbeitungen „Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen" genannt, die jedoch alle zu den Aufgaben der öffentlichen Stelle gehören, deren Erlaubnistatbestand in § 3 BDSG geregelt ist. Dies gilt auch „für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen"; handelt es sich nicht um einen Ausbildungs- oder Schulungsbetrieb, erscheint eine Zweckänderung der Verarbeitung nicht angebracht, handelt es sich um einen Ausbildungs- oder Schulungsbetrieb, gehört die Verarbeitung zu den in § 3 BDSG geregelten Aufgaben der öffentlichen Stelle.

- Die **Rechtsgrundlagen für die Datenverarbeitung in § 24 BDSG** sind **nicht sachgerecht, praktikabel und normenklar geregelt.**

Eine Erforderlichkeit für die Regelung in § 24 Abs. 1 BDSG ist neben Art. 6 DSGVO nicht erkennbar. Ein Anwendungsbereich über die DSGVO hinaus kann sich im Regelungsgehalt des § 24 Abs. 2 BDSG ergeben, sodass die Regelung in § 24 BDSG in diesem Fall insgesamt hierauf beschränkt sein sollte.

*Frage des BMI im Rahmen der Evaluation:* „2. Sind die Rechtsgrundlagen für die Datenübermittlung in § 25 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

**Stellungnahme des BvD:** Die **Rechtsgrundlagen für die Datenübermittlung in § 25 BDSG sind** aus unserer Sicht **nicht sachgerecht, praktikabel und normenklar.**

a. Eine Übermittlung stellt lediglich eine Form der Verarbeitung dar. Laut § 3 BDSG ist die „Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe" erforderlich ist. Somit ist die Regelung von § 25 Abs. 1 BDSG bereits in § 3 BDSG enthalten. Die Regelung in Absatz 1 sollte daher entfernt werden.

b. Auch § 25 Abs. 2 Ziff. 1 BDSG wird durch § 3 BDSG bereits geregelt und sollte daher entfernt werden.

c. Die in § 25 Abs. 2 Ziff. 3 BDSG geregelte Übermittlung zur „Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche" der öffentlichen Stelle gegenüber einer nichtöffentlichen Stelle gehört ebenfalls regelhaft zu den Aufgaben einer öffentlichen Stelle und wird somit bereits durch § 3 BDSG adressiert. Auch § 25 Abs. 2 Ziff. 3 BDSG sollte daher entfernt werden.

*Frage des BMI im Rahmen der Evaluation:* „3. Sind die Regelungen in Bezug auf besondere Verarbeitungssituationen in den §§ 26 bis 31 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

**Stellungnahme des BvD:**

- Die **Regelungen** in Bezug auf besondere Verarbeitungssituationen **in § 26 BDSG** sind aus unserer Sicht normenklar, aber **nicht sachgerecht und praktikabel.**

§ 26 BDSG stellt lediglich die Fortschreibung der § 32 BDSG a.F. dar. Alle bereits zu § 32 BDSG a.F. als ungelöst kritisierten Fragen zum Beschäftigtendatenschutz wie beispielsweise die Grenzen des Fragerechts des Arbeitgebers, die Datenerhebung über Bewerber im Internet oder auch die Speicherdauer von Bewerberdaten bleiben weiterhin ungelöst. Neue Ansätze wie Predictive Analytics oder auch Big Data Szenarien können mit den vorhandenen Regelungen nicht rechtssicher begleitet werden.

Sofern nicht jedenfalls in der nächsten Legislaturperiode ein eigenes Beschäftigungsdatenschutzgesetz verabschiedet wird, sollten die beschriebenen Klarstellungen bereits im BDSG berücksichtigt werden.

- Die **Regelungen** in Bezug auf besondere Verarbeitungssituationen **in § 27 BDSG** sind aus unserer Sicht **nicht normenklar, sachgerecht und praktikabel.**

a. Die Öffnungsklausel in Art. 9 Abs. 4 DSGVO für nationale Gesetzgeber erfasst ausschließlich die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten, die Regelung in § 27 Abs. 1 BDSG betrifft aber alle in Art. 9 Abs. 1 DSGVO genannten besonderer Kategorien personenbezogener Daten und dürfte somit nicht europarechtskonform sein. Wir schlagen daher vor, zur Erhöhung der Rechtssicherheit für den Rechtsanwender den Erlaubnistatbestand auf die in Art. 9 Abs. 4 DSGVO genannten Datenkategorien zu beschränken.

b. Beschränkungen der Betroffenenrechte können nur entsprechend den in Art. 23 Abs. 1 DSGVO enthaltenen Vorgaben erfolgen, die Regelung in § 27 Abs. 2 BDSG erfüllt in der Allgemeinheit jedoch nicht die Anforderungen von Art. 23 Abs. 1 DSGVO. Zudem fehlt in § 27 Abs. 2 BDSG die Berücksichtigung von Art. 23 Abs. 2 DSGVO. Die Anwendung von § 27 Abs. 2 BDSG stellt daher eine Rechtsunsicherheit dar.

Eine Beschränkung wäre – unter Berücksichtigung, dass Art. 9. Abs. 4 DSGVO bzgl. § 27 Abs. 1 BDSG nur Regelungen hinsichtlich der Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten erlaubt – aus unserer Sicht nur unter Nutzung von Art. 23 Abs. 1 Buchst. e DSGVO im Sinne von „Forschungs- oder Statistikzwecke des allgemeinen öffentlichen Interesses Deutschlands" sowie von „Forschungs- oder Statistikzwecke im Bereich der öffentlichen Gesundheit" möglich, begleitet von Art. 23 Abs. 2 DSGVO adressierenden spezifischen Vorschriften.

c. Auch in § 27 Abs. 3 BDSG ist die Regelung auf die in Art. 9 Abs. 4 DSGVO genannten Datenkategorien anzupassen.

- Die **Rechtsgrundlagen** für die Datenübermittlung in **§ 28 BDSG** sind aus unserer Sicht **nicht sachgerecht, praktikabel und normenklar.**

Die Begründung ist analog dem Kommentar zu § 27 BDSG, dass der in Art. 9 Abs. 4 DSGVO enthaltene Erlaubnistatbestand für nationale Regelungen nicht alle in Art. 9 Abs. 1 DSGVO genannten Datenkategorien umfasst. Auch § 28 Abs. 1 BDSG muss daher angepasst werden.

- Die **Regelungen in § 29 Abs. 1 BDSG** sind aus unserer Sicht **nicht sachgerecht, praktikabel und normenklar.**

Eine Beschränkung der in Kapitel II DSGVO genannten Betroffenenrechte können nur entsprechend den in Art. 23 Abs. 1 DSGVO enthaltenen Vorgaben erfolgen, die Regelung in § 29 Abs. 1 BDSG der Einschränkung aufgrund der „überwiegenden berechtigten Interessen eines Dritten" genügt nicht den Anforderungen von Art. 23 Abs. 1 DSGVO. Aus unserer Sicht ist eine Einschränkung der Rechte für Dritte nur unter Nutzung von Art. 23 Abs. 1 Buchst. j DSGVO möglich.

Art. 34 DSGVO kennt keine Öffnungsklausel, sodass eine Einschränkung wohl nicht europarechtskonform erfolgen kann. Daher sollte auf diesen Abschnitt verzichtet werden.

- Die Regelung für die Datenübermittlung in **§ 30 Abs. 1 BDSG** sollte so formuliert sein, das deutlicher hervortritt, dass es sich hierbei nicht um eine Rechtsgrundlage für eine Datenverarbeitung handelt.

- Die Rechtsgrundlagen für die Datenübermittlung in **§ 31 BDSG** sind aus unserer Sicht sachgerecht, praktikabel und normenklar. Gleichwohl bestehen Zweifel daran, dass diese Regelung von einer Öffnungsklausel umfasst ist.

*Frage des BMI im Rahmen der Evaluation:* „4. Sind die Rechtsgrundlagen für die Datenverarbeitung in den §§ 48 bis 51 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

**Stellungnahme des BvD:** In unserem Berufsverband sind keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten, daher nehmen wir von Ausführungen Abstand.

## III. Datenschutzbeauftragte öffentlicher und nichtöffentlicher Stellen

*Frage des BMI im Rahmen der Evaluation:* „1. Sind die Regelungen zu Datenschutzbeauftragten öffentlicher Stellen in den §§ 5 bis 7 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

**Stellungnahme des BvD:** Ja.

*Frage des BMI im Rahmen der Evaluation:* „2. Sind die Regelungen zu Datenschutzbeauftragten nichtöffentlicher Stellen in § 38 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

**Stellungnahme des BvD:**

Die **Regelungen zu Datenschutzbeauftragten nichtöffentlicher Stellen in § 38 BDSG sind** aus unserer Sicht praktikabel und normenklar, aber **nicht sachgerecht.**

a. Die Gestaltung in §38 Abs. 1 Satz 1 BDSG erscheint aufgrund der geübten Praxis zu dieser Regelung tragfähig. Gleichwohl ist die Anhebung des Quorums von 10 auf 20 grundlegender Kritik ausgesetzt (siehe Antwort zu Frage III.3). Entscheidend hierfür ist neben der sachlichen Kritik auch, dass diese Anhebung untauglich war und ist, das damit verbundene Ziel der "Entbürokratisierung" zu erreichen.

Im Interesse der Normenklarheit wird angeregt, die Sätze 1 und 2 des Abs. 1 auf zwei Absätze zu verteilen.

b. Wenngleich die Anzahl der mit der Verarbeitung befassten Personen ein Indiz für die Erforderlichkeit eines DSB ist, darf dies kein Ausschlusskriterium für die Erforderlichkeit darstellen, weshalb auch Kriterien definiert und vorgesehen sein müssen, dass unterhalb dieses Quorums ein DSB verpflichtend zu bestellen ist.

Über die bereits in §38 Abs. 1 Satz 2 BDSG enthaltenen Aspekte hinaus sollte eine Erweiterung der Benennungspflicht vor allem unter folgenden Aspekten erfolgen:

- Die feste Zuordnung von mindestens 20 Personen für eine Benennungspflicht berücksichtigt nicht die Anzahl betroffener Personen und/oder verarbeiteter Datensätze. Gerade bei der digitalen Verarbeitung personenbezogener Daten kann z.B. ein Startup, welches nur 3 bis 5 Personen beschäftigt, eine sehr große Menge personenbezogener Daten von einer größeren Anzahl Personen verarbeiten,

wohingegen in einer Schreinerei vielleicht 20 Beschäftigte die Daten von deutlich weniger Kunden und/oder Datensätze als das Startup verarbeiten.

- Um der Zielsetzung des Art. 25 Abs. 1 DSGVO ("Privacy by design") effektiv Rechnung tragen zu können, erscheint es geboten, nicht nur die Verantwortlichen, sondern auch die durch Art. 25 DSGVO mittelbar adressierten Hersteller der Produkte, Dienste und Anwendungen (z.B. Videoüberwachung mit Gesichtserkennung, medizinische Informationssysteme) zur Benennung eines DSB zu verpflichten. Denn Art. 25 Abs. 1 DSGVO nimmt formal die Verantwortlichen in die Pflicht, obgleich deren Erfüllung auch die vorgenannten Hersteller adressiert. Diese Pflicht sollte jedenfalls dann bestehen, wenn die Produkte, Dienste und Anwendungen ihren bestimmungsgemäßen Einsatz nach einer Datenschutz-Folgenabschätzung unterliegen. Dies würde dazu führen, dass die datenschutzrechtlichen Pflichten bereits bei Herstellung und nicht erst später (evtl. ohne Änderungsmöglichkeiten) Berücksichtigung finden werden. Dies könnte insbesondere einen Beitrag zur bürokratischen Entlastung von KMU bei der Durchführung einer Datenschutz-Folgenabschätzung leisten.

c. Die aus dem Datenschutzrecht resultierenden Pflichten bestehen für Verantwortliche unabhängig von der Tatsache, ob ein Datenschutzbeauftragter benannt wurde oder nicht. Hingegen kennt ein Datenschutzbeauftragter die gesetzlichen Anforderungen und kann den Verantwortlichen bzgl. der Erfüllung der gesetzlichen Anforderungen beraten und unterstützen. Ehrlicherweise muss man davon ausgehen, dass eine hohe Anzahl von Unternehmen ohne benannten Datenschutzbeauftragten die gesetzlichen Anforderungen nicht kennen, folglich diese nicht umsetzten können und aus Unwissen gegen datenschutzrechtliche Bestimmungen verstoßen. Daher sollte auch aus dieser Sichtweise die Benennung eines Datenschutzbeauftragten auch an der Menge der von der Verarbeitung betroffenen Personen/Datensätze abhängig gemacht werden.

*Frage des BMI im Rahmen der Evaluation:* „3. Mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG- EU) wurde in § 38 Absatz 1 Satz 1 BDSG die maßgebliche Zahl der Personen, ab der ein betrieblicher Datenschutzbeauftragter zu benennen ist, von 10 auf 20 angehoben. Angestrebt wurde damit vor allem eine Entlastung kleiner und mittlerer Unternehmen sowie ehrenamtlich tätiger Vereine.

*Frage des BMI im Rahmen der Evaluation:* „a) Welche Wirkungen hat die Änderung des § 38 Absatz 1 Satz 1 BDSG nach Ihrer Kenntnis erzielt?

**Stellungnahme des BvD:** Durch die Anhebung des Benennpflicht-Quorums ist für kleinere und mittlere Unternehmen im Ergebnis statt einer Entlastung ein zusätzliches Risiko für unternehmerische Fehlbewertung der Anforderungen entstanden, die gegebenenfalls erhebliche Nachteile mit sich bringt.

Durch den Wegfall des Datenschutzbeauftragten sind nicht die Aufwände für die Erfüllung der datenschutzrechtlichen Anforderungen durch den Verantwortlichen reduziert worden, hingegen fehlt jetzt die Kenntnis, wie man fachkundig und ressourcenschonend mit diesen Anforderungen umgeht. Die Anhebung des Quorums führt somit zu einer zusätzlichen Belastung der Unternehmensleitung.

*Frage des BMI im Rahmen der Evaluation:* „b) Hat die Änderung der Norm nach Ihrer Kenntnis zu einer Erleichterung für Unternehmen und Vereine geführt?

**Stellungnahme des BvD:** Nein. Es haben sich keine Bürokratieerleichterungen durch die Anhebung ergeben, da alle Erfordernisse aus der DSGVO weiterhin bestehen bleiben und beachtet werden müssen. Der DSB trägt aufgrund seiner Fachkompetenz zu einer Erleichterung in der Umsetzung bei.

## IV. Zusammenarbeit, Zuständigkeiten und Befugnisse der Aufsichtsbehörden

*Frage des BMI im Rahmen der Evaluation:* „1. Ist die Zusammenarbeit der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

**Stellungnahme des BvD: Die Zusammenarbeit der Aufsichtsbehörden** ist im BDSG aus unserer Sicht normenklar, aber **nicht sachgerecht und praktikabel geregelt.**

Dem Föderalismus folgend, ist die Zuständigkeitsverteilung zwischen Bundesländern und Bund geboten. Damit einher gehen auch – wenngleich nicht stets und zu jedem Aspekt - unterschiedliche Auslegungen der DSGVO und des BDSG durch die Aufsichtsbehörden der Länder und des Bundes. Dies kann für Verantwortliche und Auftragsverarbeiter

zur Folge haben, dass in einem Bundesland eine Verarbeitung nach Ansicht der dortigen Aufsichtsbehörde rechtskonform erfolgt, während sie in einem anderen Bundesland durch die dort zuständige Aufsichtsbehörde als rechtswidrig angesehen wird.

Vor allem für Auftragsverarbeiter, die für Verantwortliche in unterschiedlichen Bundesländern tätig sind und somit indirekt mit verschiedenen Aufsichtsbehörden zusammenarbeiten müssen, hat dies Auswirkungen. Wir fordern den Gesetzgeber auf, in Abstimmung mit den zuständigen Aufsichtsbehörden eine Gestaltung zu finden, welche diese Unsicherheit in der Rechtsanwendung ausschließt oder die Abweichung hinreichend transparent macht.

*Frage des BMI im Rahmen der Evaluation:* „2. Sind die Zuständigkeiten der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

**Stellungnahme des BvD: Die Zuständigkeiten der Aufsichtsbehörden** im BDSG **sind** aus unserer Sicht **nicht sachgerecht, praktikabel und normenklar geregelt.** Die Zuständigkeit der Aufsichtsbehörden ist bei bundeslandübergreifender Verarbeitung nicht geregelt. Eine Abstimmung zu einer einheitlichen Rechtsauslegung im konkreten Einzelfall für beteiligte Aufsichtsbehörden ist nicht vorgeschrieben. In § 17 BDSG wird zudem die Tatsache, dass der Bundesrat keinen Stellvertreter wählt, nicht berücksichtigt.

**Lösungsvorschlag:** Die Schaffung einer Regelung für eine federführende deutschen Aufsichtsbehörde ähnlich dem europäischen Recht für bundeslandübergreifende Verarbeitungen, damit Verantwortliche und Auftragsverarbeiter eine Aufsichtsbehörde als verbindlichen Ansprechpartner haben.

*Frage des BMI im Rahmen der Evaluation:* „3. Hat sich aus Ihrer Sicht die Regelung in § 40 Absatz 2 BDSG bewährt, wonach sich, wenn der Verantwortliche oder Auftragsverarbeiter mehrere inländische Niederlassungen hat, die zuständige Aufsichtsbehörde entsprechend Artikel 4 Nummer 16 DSGVO nach der Hauptniederlassung bestimmt?

**Stellungnahme des BvD:** Nein, siehe Antworten zu den Fragen IV.1 und IV.2

*Frage des BMI im Rahmen der Evaluation:* „Sind die Befugnisse der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

**Stellungnahme des BvD:** Nein, siehe Antworten zu den Fragen IV.1 und IV.2

*Frage des BMI im Rahmen der Evaluation:* „5. Gibt es aus Ihrer Sicht neben den in den Fragen 1 bis 3 angesprochenen Aspekten Änderungsbedarf bei der Regelung der Datenschutzaufsicht im BDSG und wenn ja, worin besteht er?

**Stellungnahme des BvD:** Die Kernanliegen wurden vorstehend adressiert.

## V. Betroffenenrechte

*Frage des BMI im Rahmen der Evaluation:* „1. Sind die Regelungen zu den Betroffenenrechten in den §§ 32 bis 37 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

**Stellungnahme des BvD: Die Regelungen** zu den Betroffenenrechten **in den §§ 32 bis 37 BDSG sind** aus unserer Sicht **nicht uneingeschränkt sachgerecht, praktikabel und normenklar.**

Beschränkungen der Betroffenenrechte können nur entsprechend den in Art. 23 Abs. 1 DSGVO festgelegten Grenzen unter Beachtung der Maßgaben des Art. 23 Abs. 2 DSGVO. Der BvD regt eine Ausrichtung der Ausnahmen an diesen Regelungen an, um ein Mehr an Rechtssicherheit zu erreichen.

*Frage des BMI im Rahmen der Evaluation:* „2. Sind die Regelungen zu den Betroffenenrechten in den §§ 55 bis 61 BDSG aus Ihrer Sicht normenklar? Sind sie aus Ihrer Sicht sachgerecht und praktikabel, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen?

**Stellungnahme des BvD:** In unserem Berufsverband sind keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten, daher nehmen wir von Ausführungen Abstand.

**HINWEIS** Auf Antworten zu den Fragenkomplexen VI. (Pflichten der Verantwortlichen und Auftragsverarbeiter) und VII. (Datenübermittlungen an Drittstaaten und an internationale Organisationen) hat der BvD mit der Begründung verzichtet, dass in unserem Berufsverband keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten sind.]

## VIII. Haftung und Sanktionen

*Frage des BMI im Rahmen der Evaluation:* „1. Sind die Regelungen zu Sanktionen in den §§ 41 bis 43 BDSG aus Ihrer Sicht sachgerecht und normenklar?

**Stellungnahme des BvD: Die Regelungen zu Sanktionen in den §§ 41 bis 43 BDSG sind** aus unserer Sicht **nicht uneingeschränkt sachgerecht und normenklar.**

Nach § 41 Abs. 1 BDSG sind die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß anzuwenden. Die Bezugnahme auf insbesondere §§ 30, 130 OWiG ergibt Friktionen zu dem Art. 83 DSGVO zugrunde liegenden Unternehmensbegriff. Der BvD regt im Interesse der Rechtsklarheit eine klarstellende Überprüfung an.

*Frage des BMI im Rahmen der Evaluation:* „2. In wie vielen Fällen haben nach Ihrer Kenntnis Landgerichte gemäß § 41 Absatz 1 Satz 3 BDSG über einen Einspruch gegen einen Bescheid über ein Bußgeld von mehr als 100.000 (einhunderttausend) Euro wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 DSGVO entschieden? (Bitte nach Jahren und Landgerichten aufschlüsseln)

**Stellungnahme des BvD:** Der BvD führt entsprechend seinen Verbandsaufgaben keine solche Aufstellung. Aufgrund der beruflichen Geheimhaltungspflichten sind die Mitglieder des BvD auch nicht ohne Weiteres berechtigt hierzu zu kommunizieren. Der BvD regt an, dass eine Veröffentlichung der verhängten Bußgelder und Entscheidungen eingerichtet wird. Zu berücksichtigen ist jedoch, wie auch die aktuelle Rechtsprechung zeigt, dass hierdurch kein „Pranger-Effekt" entsteht. Eine bundesweit gemeinsame, anonyme Veröffentlichung könnte diesen Effekt vermeiden, aber gleichwohl der erforderliche Erkenntnisgewinn aus den Entscheidungen zur Einheitlichkeit der Rechtsanwendung beitragen.

*Frage des BMI im Rahmen der Evaluation:* „3. Sind die Regelungen zu Haftung und Sanktionen in den §§ 83 und 84 BDSG aus Ihrer Sicht sachgerecht und normenklar?

**Stellungnahme des BvD:** In unserem Berufsverband sind nicht in signifikantem Umfang Verarbeiter im Sinne des Teils des BDSG vertreten, daher nehmen wir von Ausführungen Abstand.

## IX. Allgemein zu den Regelungen des BDSG

*Frage des BMI im Rahmen der Evaluation:* „1. Wie bewerten Sie das BDSG insgesamt in Bezug auf die Sachgerechtigkeit, Praktikabilität und Normenklarheit der Bestimmungen?

**Stellungnahme des BvD:** Die DSGVO wird aufgrund ihre Bürokratie-Aufwände und der damit verbundenen Kosten für die Verantwortlichen kritisiert. Diese Bürokratie und diese Kosten bestehen unabhängig von der Benennung eines DSB. Denn die umfassenden Dokumentations-, Informations- und Prüfungspflichten der DSGVO bestehen unabhängig von der Benennung eines DSB. Mit anderen Worten: Der Verzicht auf die Benennung eines DSB bringt für die Verantwortlichen keine Entbürokratisierung. Eine hierauf ausgerichtete Ausgestaltung der Tätigkeit des DSB entlastet hingegen die Unternehmensleitung in KMU:

Die DSGVO bietet dem BDSG anders als im alten Datenschutzrecht besser die Möglichkeit, die Rolle des Datenschutzbeauftragten stärker als proaktiven Gestalter für das Unternehmen, weniger als reaktiven Überwacher auszugestalten.

**Der BvD regt daher an, die Einbindung des Datenschutzbeauftragten in die Gestaltung der Verarbeitung personenbezogener Daten zu stärken und dem Datenschutzbeauftragten die Möglichkeit zu eröffnen, die Unternehmensleitung bei einzelnen Aufgaben nach der DSGVO zu entlasten.**

Davon würden vor allem kleine und mittlere Unternehmen profitieren und es würde eine effektive Nutzung des Know-hows zur Gestaltung der Nutzung personenbezogener Daten erreicht werden.

Konkrete Ansätze zur effektiveren Einbindung von Datenschutzbeauftragten sieht der BvD in folgenden Maßnahmen:

- Anpassung der Meldepflicht bei Datenpannen: Meldungen von (Verdacht auf) Datenpannen an die Aufsichtsbehörden erst bei einem hohen Risiko. Meldung aller Vorgänge an den DSB, der zudem ein Register aller Vorfälle führt und die Abhilfemaßnahmen überwacht.

- Anpassung der Zuständigkeit bei der Datenschutz-Folgenabschätzung (DSFA): Die Erstellung der DSFA und die Beurteilung der Risiken sollte in den Händen des DSB liegen. Das Ergebnis wird dann von der Unternehmensleitung verbindlich festgestellt und die vorgesehenen Maßnahmen werden umgesetzt.
- Führen des Verzeichnisses der Verarbeitungstätigkeiten durch den DSB anstatt der ansonsten hierfür verantwortlichen Leitung des Verantwortlichen.

**Der BvD fordert den Bundesgesetzgeber zudem auf, anlässlich der Evaluierung des BDSG klarzustellen, dass durch die Beratungsleistung externer Datenschutzbeauftragter bei der Wahrnehmung ihrer gesetzlichen Aufgaben gem. Art. 39 DSGVO im Rahmen ihrer Benennung keine Kollisionen zum RDG entsteht.** Dem DSB ist durch die DSGVO eindeutig die Aufgabe der Beratung zugewiesen. Das schließt nach dem Selbstverständnis der DSGVO zwangsweise die Beratung zu allen Aspekten des Datenschutzrechts ein, die datenschutzrechtliche Thematiken tangieren. Die in Deutschland geführte Diskussion, dass dies vermeintlich gegen das RDG verstößt, verhindert die proaktiv unterstützende Funktion des DSB im Unternehmen, obgleich diese in der DSGVO so vorgesehen ist. Eine Einschränkung der Tätigkeit des DSB bei der (datenschutz-)rechtlichen Beratung durch eine Vorschrift eines Mitgliedsstaates verstößt gegen die höherrangige Vorgabe zur Beratung durch eine europäische Verordnung.

**Schließlich fordert der BvD den Gesetzgeber auf, von seinen Gestaltungsmöglichkeiten, insbesondere nach Art. 23 DSGVO Gebrauch zu machen, auf eine fokussierte anstatt bürokratisierte Dokumentationspflicht hinzuwirken.** Die Hauptbelastung für die Unternehmen unter der DSGVO und BDSG ist nicht die Einhaltung der Zulässigkeit der Verarbeitung. Die als unnötige Bürokratie empfundenen Anforderungen der DSGVO und des BDSG liegen vielmehr in der Vielzahl unterschiedlicher Dokumentationspflichten, die sich inhaltlich auch noch überschneiden, aber nicht deckungsgleich sind. Dennoch ist jede dieser Dokumentationspflichten für sich mit einem Bußgeld bewehrt. Die Unternehmensleitung ist damit im Rahmen des Datenschutzes mehr damit beschäftigt, Dokumentationen stets aktuell zu halten, als sich mit der eigentlichen Frage der Zulässigkeit zu befassen.

*Frage des BMI im Rahmen der Evaluation:* „2. Bestehen in Ihrer datenschutzrechtlichen Praxis Schwierigkeiten mit der Auslegung und Anwendung des BDSG? Wenn ja, welche Schwierigkeiten sind das und auf welche Regelungen des BDSG beziehen sie sich?

**Stellungnahme des BvD:** Die Schwierigkeiten wurden in den Fragen I. bis VIII. dargestellt.

Auf Antworten zum Fragenkomplex X. (Schutz- und Dokumentationspflichten bei Unterbleiben einer Information der betroffenen Person) hat der BvD mit der Begründung verzichtet, dass uns hierzu als BvD keine Informationen im signifikanten Umfang vorliegen.

Der vollständige Fragebogen ist nachzulesen unter:
https://www.bvdnet.de/presse/fragebogen-des-bmi-zur-evaluation-des-bdsg/

Über den QR-Code kommen Sie direkt zum Fragebogen.

# PRIVACY LITIGATION

## Von Betroffenenrechten über Unterlassungsansprüche bis hin zum Schadensersatzanspruch nach DS-GVO

Thomas Kahl

Sorgten in den ersten Jahren mit der DS-GVO hohe Umsetzungsaufwände und -kosten sowie erhebliche Bußgeldandrohungen für Aufruhr, bereitet seit geraumer Zeit ein neues Phänomen einer wachsenden Gruppe an Unternehmen Kopfzerbrechen: Die vermehrte Durchsetzung von Betroffenenrechten wegen (vermeintlich) datenschutzrechtswidriger Verarbeitungshandlungen mit gerichtlicher Hilfe oder einfach „Privacy Litigation" – und das mit wachsendem Erfolg!

Klar ist: Der Umgang mit Betroffenenrechten wie Auskunfts- oder Löschungsansprüchen hat Unternehmen schon vor Inkrafttreten der DS-GVO vor große praktische Herausforderungen gestellt. Die neuere Entwicklung der verstärkten Durchsetzung von Betroffenenansprüchen mit gerichtlicher Hilfe, allen voran der in Art. 82 DS-GVO geregelten Schadensersatzansprüche, bringt Unternehmen in vielerlei Hinsicht in Bedrängnis.

Die Problematik erschließt sich nicht auf den ersten Blick: Mag das Handling und die Verteidigung gegen einen oder eine kleine Anzahl von Anspruchstellern noch mit vertretbarem Aufwand möglich sein, können die praktischen und finanziellen Belastungen bei einer Vielzahl geltend gemachter Betroffenenansprüche schnell unüberschaubar werden.

Datenschutzvorfälle, nicht funktionierende Prozesse für das Handling von Betroffenenanfragen oder datenschutzrechtswidrige Gestaltungen von Webseiten, Apps oder sonstigen Produkten oder Diensten können so schnell zur (zusätzlichen) Kostenfalle für Unternehmen werden.

Im folgenden Beitrag werfen wir einen Blick auf die wesentlichen Grundzüge der „Privacy Litigation", also der (gerichtlichen) Durchsetzung von Betroffenenansprüchen, den Stand der Rechtsprechung sowie die wesentlichen Take Aways für Unternehmen im Handling entsprechender Situationen.

### Betroffenenansprüche – ein Überblick

Die DS-GVO kennt verschiedene, ausdrücklich geregelte Betroffenenrechte, die dem Betroffenen im Hinblick auf die Verarbeitung personenbezogener Daten zustehen. Umfasst sind hiervon zum einen die „klassischen" Betroffenenrechte gem. Art. 12-22 DS-GVO, allen voran der Auskunftsanspruch gemäß Art. 15 DS-GVO oder das in Art. 21 DS-GVO enthaltene Recht auf Widerspruch. Neben dem Recht des Betroffenen gemäß Art. 77 DS-GVO, sich bei der zuständigen Aufsichtsbehörde zu beschweren, erlangt das Recht auf Schadensersatz in Art. 82 DS-GVO zunehmend an Bedeutung.

### (Gerichtliche) Durchsetzung von Betroffenenansprüchen

In Art. 12 DS-GVO finden sich verschiedene Grundsätze, die für die Auslegung der Reichweite von Betroffenenansprüche sowie deren Durchsetzung von Bedeutung sind. Zu nennen wären hier der Effektivitätsgrundsatz gem. Art. 12 Abs. S. 1 DS-GVO (Erleichterung der Ausübung der Betroffenenrechte) sowie der in Art. 12 Abs. 3 und 4 angelegte Beschleunigungsgrundsatz. Die weitere und insbesondere gerichtliche Durchsetzung von Betroffenenansprüchen selbst ist in der DS-GVO nur rudimentär geregelt (vgl. Art. 78-80 DS-GVO) und der weiteren Ausgestaltung durch das mitgliedstaatliche Recht überlassen.

Erfüllt der Verantwortliche entsprechende Anfragen des Betroffenen nicht ordnungsgemäß, steht diesem zum einen der Weg zur zuständigen Aufsichtsbehörde offen (Beschwerderecht gem. Art. 77 DS-GVO).

Entspricht die angerufene Behörde dem Begehr des Betroffenen nicht, besteht (je nach Maßnahme und rechtlicher Einordnung) ggf. die Möglichkeit eines gerichtlichen Vorgehens, zum Beispiel in einem verwaltungsgerichtlichen Verfahren. Besondere Rege-

lungen hierzu finden sich in § 20 BDSG, der der Umsetzung von Art. 78 Abs. 1 DS-GVO dient.

Alternativ besteht die Möglichkeit für den Betroffenen, seine Rechte im Klageweg vor den ordentlichen Gerichten durchzusetzen. Art. 79 Abs. 2 DS-GVO bestimmt, an die Gerichte welchen Mitgliedsstaates sich der Betroffenen wenden kann (internationale Zuständigkeit). Weitere Details, insbesondere welches nationale Gericht für die Geltendmachung der Ansprüche örtlich und sachlich zuständig ist, ergibt sich aus § 44 BDSG sowie dem jeweiligen nationalen (Prozess-)Recht, in Deutschland also den Regelungen der Zivilprozessordnung (ZPO, zur örtlichen Zuständigkeit) sowie des Gerichtsverfassungsgesetzes (GVG, zur sachlichen Zuständigkeit).

Örtlich zuständig sind danach die Gerichte des Ortes, an dem der Verantwortliche (oder Auftragsverarbeiter) eine Niederlassung unterhält oder an dem der Betroffene seinen gewöhnlichen Aufenthaltsort hat (vgl. § 44 Abs. 1 BDSG). Gemäß § 23 GVG liegt die Grundzuständigkeit im ersten Rechtszug bei den Amtsgerichten. Dies gilt für Rechtsstreitigkeiten mit einem Streitwert von nicht mehr als 5.000 Euro (streitwertabhängige Zuständigkeit) sowie weitere, themenspezifische Zuständigkeiten (streitgegenstandsunabhängige Zuständigkeit). Die Zuständigkeit des Landgerichts ist gem. § 71 Abs. 1 GVG für Streitigkeiten mit einem Streitwert über 5.000 Euro sowie streitwertunabhängig für weitere, im Gesetz spezifizierte Streitigkeiten gegeben. Besondere Vorgaben können u.a. bei Streitigkeiten aus dem Arbeits- oder Versicherungsverhältnis bestehen (vgl. § 2 ArbGG oder § 215 VVT).

Aus Sicht des Betroffenen dürfte der wesentliche Unterschied in der Anrufung von Amts- oder Landgerichten zum einen im sogenannten Anwaltszwang liegen, der erst vor dem Landgericht entsteht. Vor den Amtsgerichten kann sich der Betroffene somit „selbst" vertreten. Eines (kostspieligen) Rechtsbeistands bedarf es nicht. Zum anderen fallen vor den Landgerichten regelmäßig höhere Verfahrenskosten an, mit denen der Betroffene insbesondere im Fall des Unterliegens belastet wird.

Die gerichtliche Durchsetzung von Betroffenenrechten aus der DS-GVO beginnt (vorbehaltlich etwaiger Besonderheiten in speziellen Gebieten) auf Grund der oftmals geringeren Streitwerte vor den Amtsgerichten, es sei denn, die Zuständigkeit der Landgerichte ist auf Grund des höheren Streitwertes eröffnet. Die Festsetzung des Streitwertes liegt im Ermessen des Gerichts (vgl. § 3 ZPO). Beispielhaft sei auf die gerichtliche Durchsetzung von Auskunftsansprüchen verwiesen, bei der deutsche Gerichte zuletzt eher geringere Streitwerte angenommen haben (LAG Baden-Württemberg, Beschluss vom 23.01.2020, Az. 5 Ta 123/19: 500 EUR; dagegen zuvor noch AG München, Teilurteil v. 04.09.2019, Az. 155 C 1510/18: 5.000 EUR). Anders verhält es sich naturgemäß mit der gerichtlichen Durchsetzung eines (immateriellen) Schadensersatzanspruchs mit einem (geforderten) Betrag von mehr als 5.000 EUR, der sodann vor den Landgerichten geltend zu machen wäre.

Betroffene machen entsprechende Ansprüche vermehrt zum Gegenstand arbeitsgerichtlicher Prozesse, beispielsweise als Annex in einem Kündigungsschutzprozess, wenn ein entsprechender Bezug zum Beschäftigungsverhältnis des Betroffenen besteht (vgl. hierzu zuletzt u.a. den Fall des Arbeitsgerichts Düsseldorf, Urt. v. 05.03.2020, Az. 9 Ca 6557/18).

Zuletzt besteht für den Betroffenen die Möglichkeit der Einschaltung von Einrichtungen, Organisationen oder Vereinigungen im Bereich des Datenschutzrechts, die die Rechte des Betroffenen in dessen Auftrag geltend machen bzw. in entsprechenden Verfahren vertreten können. Details zu solchen Verbandsklagen regelt Art. 80 DS-GVO. Dabei ist umstritten, inwieweit sich welche Verbände für eine Klagebefugnis auf mitgliedsstaatliche Normen, in Deutschland insbesondere das Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen, kurz UKlaG, berufen können. Details sind derzeit Gegenstand gerichtlicher Klärung vor dem EuGH (vgl. BGH, Vorlagebeschluss vom 28.05.2020, Az. I ZR 186/17). Dabei darf nicht verkannt werden, dass es bereits heute einzelnen Verbänden wie den Verbraucherzentralen möglich ist, entsprechende Fragestellungen gerichtlich klären zu lassen. Da hiervon durchaus rege Gebrauch gemacht wird, sind entsprechende Szenarien in die Risiko-Betrachtung stets mit einzustellen. Sollte der EuGH die Gruppe der berechtigten Gruppierungen weit(er) fassen – zu denken ist hier auch an

Gewerkschaften oder Betriebsräte – dürften auf Unternehmen unruhige Zeiten zukommen.

## Auskunftsansprüche im Lichte der aktuellen Rechtsprechung

Immer mehr Gerichte werden mit der Durchsetzung von Auskunftsansprüchen befasst. Die Reichweite von Art. 15 DS-GVO wird dabei unterschiedlich, aber zunehmend extensiv verstanden. Auffällig ist, dass die Gerichte Art. 15 DS-GVO deutlich umfassender als die Datenschutzaufsichtsbehörden interpretieren.

So folgt unter anderem das LG München I in einer aktuelleren Entscheidung (Urt. v. 06.04.2020, Az. 3 O 909/19) einer umfassenden Auslegung des Art. 15 Abs. 3 DS-GVO. Die Klägerin hatte die Aushändigung von Kopien aller personenbezogenen Daten, insbesondere in Form von Telefonnotizen, Aktenvermerken, Protokollen, E-Mails, Briefen und Zeichnungsunterlagen, begehrt. Das Gericht gab der Klage statt. Hauptargument: „Belanglose" Daten gebe es nicht mehr. Der Auskunftsanspruch sei weit zu verstehen. Ähnlich hatten zuvor bereits das LAG Baden-Württemberg (Urt. v. 20.12.2018 – 17 Sa 11/18) und das OLG Köln (Urt. v. 26.07.2019 – 20 U 75/18) geurteilt.

Auskunftsansprüche scheinen sich zudem derzeit in arbeitsrechtlichen Auseinandersetzungen zu einem „Standard-Prozedere" zu entwickeln, wohl nicht zuletzt, um den Druck auf den Arbeitgeber im Rahmen einer entsprechenden Streitigkeit zusätzlich zu erhöhen.

Nicht selten werden solche Ansprüche als Teil einer Einigung „wegverglichen" und treiben den Preis einer zu zahlenden Abfindung in die Höhe. Inwieweit die arbeitsgerichtliche Rechtsprechung diese Praxis zukünftig beschränken wird, bleibt abzuwarten. In jedem Fall gehört der Auskunftsanspruch mittlerweile zum „Standard-Repertoire" in arbeitsgerichtlichen Streitigkeiten und führt auf Grund der tendenziell extensiven Interpretation zu oftmals nur schwer auflösbaren Konflikten zwischen den Interessen des betroffenen Beschäftigen und denen des Arbeitsgebers und anderer betroffener Personen (zum Beispiel weiterer Mitarbeiter), unter anderem im Hinblick auf den Schutz der Vertraulichkeit (Stichwort Hinweisgebersysteme) sowie den allgemeinen Persönlichkeitsrechtschutz.

## Gerichtliche Durchsetzung von Unterlassungsansprüchen im Datenschutzrecht

Hochumstritten ist die Frage, ob Betroffenen neben den in der DS-GVO ausdrücklich vorgesehenen Betroffenenrechten ein genereller Unterlassungsanspruch gegen Verantwortliche oder Auftragsverarbeiter im Fall einer unrechtmäßigen Verarbeitung zusteht und woraus sich dieser Anspruch bejahendenfalls ergibt. Der Vorteil eines solchen Anspruchs für den Betroffenen liegt unter anderem in der Möglichkeit des Verbots (oder ggf. sogar der positiven Anordnung) einer konkreten Verarbeitungshandlung, die gegebenenfalls nicht unmittelbar mit der Geltendmachung der eigentlichen Betroffenenrechte der DS-GVO im Zusammenhang steht – soweit einschlägig auch im Wege des Eilrechtsschutzes.

Die DS-GVO sieht auf den ersten Blick keine Unterlassungsansprüche vor. Argument: Neben den ausdrücklich in Art. 12-22, 77 sowie 82 geregelten Betroffenenrechten finden sich keine weiteren „Ansprüche" zu Gunsten des Betroffenen.

Zudem: Art. 79 DS-GVO sieht neben der gerichtlichen Durchsetzung der dem Betroffenen nach der DS-GVO „zustehenden Rechte" (= Betroffenenrechte) keine zusätzlichen gerichtlichen Rechtsbehelfe vor.

Das VG Regensburg scheint dieser Sichtweise zumindest teilweise zu folgen und erkannte zuletzt in einer Entscheidung (Bescheid v. 06.08.2020, Az. RN 9 K 19.1061) dem Betroffenen lediglich einen individualrechtlichen Unterlassungsanspruch zu, erteilte einem „allgemeinen" Unterlassungsanspruch nach §§ 1004 Abs. 1, 823 Abs. 2 BGB im Bereich des Datenschutzes jedoch grundsätzlich eine Absage (Berufung zugelassen).

Weiter geht das LG München I in einem Urteil vom 07.11.2019 (Az. 34 O 13123/19) und erkennt überhaupt keinen Unterlassungsanspruch aus der DS-GVO an. Das Recht auf Unterlassung rechtswidriger Datenverarbeitung sei nicht als solches in der DS-GVO verankert. Zudem stelle die bloß verordnungswidrige Datenverarbeitung gerade (noch) keine Rechtsverletzung dar, deren Rechtsfolgen in der DS-GVO geregelt sei. Ein präventiver Schutz des Betroffenen vor einer Rechtsverletzung wegen einer verordnungswidrigen Datenverarbeitung sei dem Wortlaut der DS-GVO an keiner Stelle zu entnehmen.

Auch wenn neben der Systematik auch die Entstehungsgeschichte von Art. 79 DS-GVO (entsprechende Klarstellungen wurden seinerzeit verworfen) gegen die Annahme eines Unterlassungsanspruchs bei Datenschutzverletzungen spricht, dürfte die Frage auch im Hinblick auf Art. 8 Abs. 1 der europäischen Grundrechtecharta (EU-GRCh) und Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV, hier Recht auf Schutz personenbezogener Daten) weiterhin umstritten bleiben.

Mit der Zuerkennung von Unterlassungsansprüchen in Verfahren auf Gewährung einstweiligen Rechtschutzes (Eilrechtsschutz) scheinen deutsche Zivilgerichte bislang zurückhaltend.

So lehnt das bereits zuvor zitierte LG München I (Urteil vom 07.11.2019; Az. 34 O 13123/19) die Gewährung einstweiligen Rechtsschutzes nicht nur mangels Bestehens eines Unterlassungsanspruchs, sondern auch unter Verweis auf bestehende Alternativen ab, mit denen der Betroffene sich der Datenverarbeitung entziehen könne – eine Argumentation, die sich zwar auf den konkret zu entscheidenden Fall bezog, aber zukünftig unter anderem bei (vermeintlichen) Datenschutzverletzungen im Online-Bereich noch an Bedeutung gewinnen könnte.

Anders hatte dies noch das LG Würzburg, (Beschluss v. 13.09.2018, Az. 11 O 1741/18) gesehen, hier aber maßgeblich auf die gleichzeitige Verletzung wettbewerbsrechtlicher Vorschriften (und somit einen bereits daraus folgenden Unterlassungsanspruch) abgestellt.

Die spannende und weiterhin ungeklärte Frage der sogenannten Abmahnfähigkeit von Datenschutzverstößen durch Wettbewerber nach dem Gesetz gegen unlauteren Wettbewerb (UWG) soll hier nicht vertieft werden, wird Unternehmen aber je nach Ausgang der höchstrichterlichen Klärung durch den EuGH ebenso auf Trapp halten (vgl. zuletzt BGH, Vorlagebeschluss v. 28.05.2020, Az. I ZR 186/17; ablehnend u.a. LG Bochum, Urteil v. 07.08.2018, Az. 12 O 85/18 unter Hinweis auf den abschließenden Charakter der Art. 77 ff DS-GVO; zustimmend u.a. das Urteil des OLG München vom 07.02.2019, Az.: 6 U 2404/18).

## Schadensersatzansprüche wegen Datenschutzverletzungen - Das „neue“ Schreckgespenst

Im deutschen Recht werden Schadensersatzansprüche für immaterielle Schäden grundsätzlich nur unter besonders restriktiven Voraussetzungen anerkannt. Schäden im Fall von Datenschutzverletzungen weisen die Besonderheit auf, dass sie sich oft nicht materialisieren (z.B. in Vermögensschäden niederschlagen). In Art. 82 DS-GVO findet sich eine eigene Anspruchsgrundlage für Schadensersatzansprüche des Betroffenen, die ausdrücklich den Ersatz immaterieller Schäden umfasst. Der Schadensbegriff ist nach Erwägungsgrund 146 weit auszulegen.

Waren Gerichte in den vergangenen ein bis zwei Jahren noch zurückhaltend in der Zuerkennung solcher Ansprüche, scheint sich das Blatt zu wenden: Vermehrt finden sich Urteile, in denen Betroffenen wegen – auf den ersten Blick – untergeordneter Datenschutzverletzungen Schadensersatzforderungen in Teils erheblichem Umfang zugesprochen werden.

Die Entwicklung ruft Verbraucheranwälte und Prozessfinanzierer auf den Plan, die hierin ein interessantes Betätigungsfeld für sich entdecken - und vielen Unternehmen große Sorge bereiten: Denn bei einer Vielzahl Betroffener können Datenschutzvorfälle schon bei Zusprache geringer Schadensersatzbeträge zu erheblichen Belastungen führen – sei es, um entsprechende Forderungen zu begleichen oder sich „nur“ (oftmals unter Aufwendung erheblicher zusätzlicher Kosten) gegen eine Vielzahl von Ansprüchen gerichtlich zu verteidigen.

Die Anzahl der Gerichte, die Betroffenen bereits Schadensersatzansprüche unter der DS-GVO zugesprochen haben, scheint sich (noch) die Waage mit solchen zu halten, die solche Ansprüche abgelehnt haben.

Nach dem aktuellen Votum des Bundesverfassungsgerichts (vgl. BVerfG, Beschl. V. 14.01.2021, Az. 1 BvR 2853/19) ist jedoch mehr als unklar, wie mit sogenannten Bagatellschäden umzugehen ist. Nach der bisherigen Rechtsprechung waren Verletzungen des Persönlichkeitsrechts nur im Fall von spürbaren, schwerwiegenden Auswirkungen

beim Betroffenen ersatzfähig. Es musste eine gewisse „Erheblichkeitsschwelle" überschritten werden. Inwieweit das mit Art. 82 DS-GVO noch vereinbar ist, bleibt durch den EuGH zu klären.

## Schadensersatzansprüche - Gerichte scheinen uneins

So reicht für die einen die bloße Befürchtung eines Schadenseintritts (vgl. LG Karlsruhe, Urt. v. 02.08.2019 – 8 O 26/19) oder die bloße Möglichkeit, dass Daten von Dritten in Folge eines Datenschutzverstoßes unbefugt genutzt werden können, nicht aus (vgl. AG Frankfurt a.M., Urt. v. 10.07.2020, Az. 385 C 155/19; LG Frankfurt a.M., Urt. v. 18.09.2020). Maßgeblich blieben die Grundsätze des deutschen Schadensersatzrechts. Folge: keine weite Auslegung der einschlägigen Tatbestände (vgl. LG Köln, Urt. v. 07.10.2020, Az. 28 O 71/20). Und: Bagatellverstöße ohne ernsthafte Beeinträchtigungen vermögen keine Schadensersatzansprüche zu begründen (vgl. u.a. LG Landshut, Urt. v. 06.11.2020, Az. 51 O 513/20).

Andere folgen der extensiven Auslegung des Art. 82 DS-GVO und argumentierten mit der abschreckenden Wirkung und erzieherischen Effekten, die dem deutschen Schadensersatzrecht bislang eher fremd sind (vgl. zuletzt LAG Köln, Urt. v. 14.09.2020, Az. 2 Sa 358/20).

Folgt der EuGH der extensiven Auslegung, dürfte die Verteidigung gegen entsprechende Ansprüche erheblich erschwert werden.

Ob deutsche Gerichte die bislang ausgeurteilten Schadensersatzsummen von einigen hundert bis zu mehreren tausend Euro bis dahin weiter in die Höhe treiben, bleibt abzuwarten. „Spitzenreiter" bleibt zunächst das Arbeitsgericht Düsseldorf (Urt. v. 05.03.2020, Az. 9 Ca 6557/18) mit Zuerkennung von 5.000 Euro immateriellen Schadensersatzes für die unvollständige und verspätete Erfüllung eines Auskunftsersuchens.

## Take Aways für Unternehmen

Die gerichtliche Praxis zeigt: Bußgelder sind nicht mehr die einzige ernst zu nehmende Bedrohung unter der DS-GVO. Die gerichtliche Geltendmachung von Betroffenenansprüchen kann ähnlich verheerende Folgen für die Unternehmen nach sich ziehen. Auch auf den ersten Blick kleine Schadensersatzbeträge können zu enormen Folgekosten führen. Dabei dürfen neben möglicherweise zu leistenden Schadensersatzforderungen insbesondere praktische Aufwände (interne Ressourcen) sowie (Folge-)Kosten der Anspruchsverteidigung nicht unterschätzt werden.

Nach der aktuellen Rechtsprechung des BverfG könnten je nach Fortgang der gerichtlichen Klärung auch untergeordnete DS-GVO-Verstöße Schadensersatzforderungen begründen, was die Risiken für Unternehmen deutlich schwerer kalkulierbar machen dürfte.

## Was lernen wir daraus?

Anfragen Betroffener zur Geltendmachung von Betroffenenrechten müssen ernst genommen und mit Priorität behandelt werden. Wie gesehen, können nicht schnell genug, unvollständig oder gar nicht beantwortete Betroffenenanfragen schnell zu streitigen Auseinandersetzungen und bei entsprechend extensiver Auslegung durch die Gerichte zu erheblichen wirtschaftlichen Belastungen führen.

Effektive Prozesse für das Management von Betroffenenanfragen sind das „A und O". Insbesondere im Fall von arbeitsgerichtlichen Auseinandersetzungen dürften sich Arbeitgeber jeder Größenordnung darauf einstellen können, mit entsprechenden Forderungen zukünftig standardmäßig und insbesondere im Rahmen arbeitsgerichtlicher Auseinandersetzungen konfrontiert zu werden. Sie sollten ihre Prozesse darauf ausrichten und optimieren.

Selbst bei der zuletzt extensiven Auslegung der Betroffenenrechte durch deutsche Gerichte bleibt festzustellen: Viele Fragen sind weiterhin ungeklärt! Gerichte in anderen europäischen Mitgliedstaaten interpretieren die Vorgaben der DS-GVO scheinbar teils restriktiver. Das eröffnet auch weiterhin Ansatzpunkte für eine erfolgreiche Verteidigung, die jedoch sorgfältig vorbereitet und rechtlich begleitet werden muss.

Besonderes Augenmerk der Verteidigung dürfte bis zu einer gerichtlichen Klärung durch den EuGH auch weiterhin auf den „Grundpfeilern" des bisherigen deutschen Schadensersatzrechts liegen, unter anderem bei der Frage der Beweislastverteilung (Grundsätzlich muss der Anspruchsteller die Rechtsverletzung und einen Schaden – materiell oder immateriell – nachweisen!).

Unternehmen sind gut beraten, zukünftig auch aus diesem Grund genau darauf zu achten, welche Informationen zu Datenschutzvorfällen in einem aufsichtsbehördlichen Verfahren verakt-tet werden, um potenziell Geschädigten und Verbraucheranwälten nicht die Möglichkeit zu geben, sich für Prozesse im Wege der Geltendmachung von Einsichtsrechten und Behördenanfragen zu wappnen.

Besondere Vorsicht dürfte auf Grund der Vielzahl an ungeklärten rechtlichen Fragen im Fall von Abmahnungen, Aufforderung zur Abgabe von Unterlassungs- und Verpflichtungserklärungen sowie der Drohung mit Maßnahmen des einstweiligen Rechtschutzes geboten sein, in denen aus Unkenntnis und Angst vor (vermeintlichen) rechtlichen Konsequenzen oftmals vorschnell Fakten geschaffen werden, die später nur noch schwer aus der Welt zu räumen sind (beispielsweise voreilige Abgabe einer Unterlassungs- und Verpflichtungserklärung).

Last but not least: Alle Unternehmen sollten die sich im Moment rasant entwickelnde Rechtsprechung genauestens im Auge behalten, um die eigenen Prozesse schnell an neue Gegebenheiten anpassen zu können.


Über den Autor

**Thomas Kahl**
Fachanwalt für IT-Recht, Taylor Wessing
Der Autor ist Rechtsanwalt und Partner der internationalen Wirtschaftskanzlei Taylor Wessing am Standort Frankfurt. Er berät nationale wie internationale Unternehmen zu Fragen des Datenschutzes, der IT-Sicherheit und Compliance im Rahmen der Ausgestaltung von (konzernweiten) Datenverarbeitungsprozessen und aufsichtsbehördlichen Verfahren.

▶ www.taylorwessing.com

TaylorWessing



Anzeige

DATENSCHUTZ | DIGITAL PRODUCT SECURITY | INFORMATIONSSICHERHEIT | IT-SECURITY

## Einführung und Betrieb von Microsoft 365:
Was tun als Datenschutzbeauftragter?

> In jeder Phase, von der Einführung bis zum Betrieb, sind vielfältige Datenschutzaspekte zu betrachten. Wir zeigen Ihnen die relevanten Themen und bieten praxisorientierte Lösungen zu Architektur, Cloud-Strategie, Backup- und Berechtigungsregeln, Löschkonzepte.

> Wir analysieren Ihren aktuellen Projekt- und Umsetzungsstand aus der Sicht des Datenschutzes, der Informationssicherheit und der IT-Sicherheit und geben Ihnen konkrete Empfehlungen für die weitere Vorgehensweise.

> Gemeinsam mit Ihnen erstellen wir auf Basis unserer Vorlagen alle erforderlichen Dokumente (Richtlinien, Schulungsmaterial, Betriebsvereinbarungen...).

Ihr Ansprechpartner: Manfred Binder, Tel. 07321 37 7845, Manfred.Binder@ditis.de

ditis Systeme – Zweigniederlassung der JMV SE & Co. KG • ein Unternehmen des Voith Konzerns
Lise-Meitner-Straße 15 • 89081 Ulm • www.ditis.de

# DSGVO-SCHADENSERSATZKLAGEN NACH DEM PAUKENSCHLAG DES BUNDESVERFASSUNGSGERICHTS

## Wie geht es weiter?

Tim Wybitul

*Klagen auf immateriellen Schadensersatz nach Art. 82 DSGVO haben derzeit Konjunktur. Zwar haben deutsche Gerichte entsprechende Schadensersatzforderungen wegen tatsächlichen oder vermeintlichen Datenschutzverstößen häufig mit der Begründung abgewiesen, dass es sich um Bagatellschäden handele. Das Bundesverfassungsgericht (BVerfG) hat dem nun aber einen Riegel vorgeschoben. Es entschied, dass es sich bei einer möglichen Erheblichkeitsschwelle bei Schadensersatzansprüchen nach Art. 82 DSGVO um eine Frage des Europarechts handele, die der Europäische Gerichtshof (EuGH) entscheiden müsse. Die Entscheidung des BVerfG dürfte Wasser auf die Mühlen von Verbrauchern, Datenschutzaktivisten, Klägeranwälten und Prozessfinanzierern sein. Denn sie erschwert es deutschen Gerichten, DSGVO-Schadensersatzklagen abzuweisen. Der vorliegende Überblick zeigt die wesentlichen rechtlichen Rahmenbedingungen und die Folgen der Entscheidung des BVerfG. Zudem fasst er die wichtigsten Entscheidungen deutscher Gerichte zum DSGVO-Schadensersatz tabellarisch unter Nennung der zugesprochenen Schadenssummen und der wesentlichen Argumente zusammen.*

## A. Schadensersatzklagen nach Art. 82 DSGVO

### I. Rahmenbedingungen

Das deutsche Schadensersatzrecht ist grundsätzlich auf den Ersatz materieller Vermögensschäden ausgerichtet. Allerdings kann nach Art. 82 Abs. 1 DSGVO jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immateriellen Schaden entstanden ist, vom Verantwortlichen oder dem Auftragsverarbeiter Schadensersatz verlangen. Diese Vorschrift sieht also auch den Ersatz von immateriellen Schäden, also Nichtvermögensschäden, vor. Erfahrungsgemäß liegt bei möglichen Datenschutzverstößen der Schwerpunkt auf Verletzungen des Persönlichkeitsrechts und nicht unmittelbar auf Vermögensschäden. Daher häufen sich derzeit vor deutschen Gerichten Klagen auf immateriellen Schadensersatz wegen behaupteten Datenschutzverstößen. Derartige Verfahren können für Unternehmen in der Praxis erhebliche finanzielle Konsequenzen nach sich ziehen. Denn häufig betreffen Datenschutzvorfälle nicht nur einzelne Personen, sondern oft viele potenzielle Kläger. Zudem besteht die Möglichkeit, gleich eine Vielzahl von Verfahren mit sehr gleichförmigen oder sogar identischen Sachverhalten einzuleiten. Dies erleichtert es Klägern und ihren Anwälten massenhaft Ansprüche vor deutschen Gerichten geltend zu machen.

### II. Bisherige Position der deutschen Gerichte

Überwiegend haben deutsche Gerichte einen immateriellen Schaden erst dann angenommen, wenn ein Datenschutzverstoß im Einzelfall zu einer konkreten, nicht bloß unbedeutenden oder empfundenen Verletzung von Persönlichkeitsrechten führte. Dementsprechend waren deutsche Gerichte bisher mit dem Ersatz immaterieller Schäden nach Art. 82 DSGVO eher zurückhaltend. Dies könnte sich nun mit dem unter B. näher dargestellten Beschluss des BVerfG ändern.

### III. Weite Auslegung des Begriffs des immateriellen Schadens

In Gerichtsverfahren wegen Schadensersatz nach Art. 82 DSGVO ist regelmäßig entscheidend was genau unter einem immateriellen Schaden zu verstehen ist. Prozessvertreter betroffener Personen argumentieren in solchen Verfahren oft, dass allein der Verstoß gegen datenschutzrechtliche Vorschriften schon einen immateriellen Schaden darstelle. Eine solche weite Auslegung birgt allerdings ein nicht unerhebliches Missbrauchspotenzial und künftig gegebenenfalls erhebliche Risiken für Unternehmen. Denn je weiter Gerichte den immateriellen Schadensbegriff auslegen, desto eher können betroffene Personen nach Datenpannen und anderen (tatsächlichen oder vermeintlichen) DSGVO-Verstößen

entsprechende Ansprüche nach Art. 82 DSGVO geltend machen.

**IV. Neuere Rechtsprechung zu Art. 82 DSGVO und ihre Folgen**

Seit einigen Monaten zeichnet sich in der Rechtsprechung allerdings ein Trend zu höheren Schadensersatzsummen bei DSGVO-Verstößen ab. Dabei wird Art. 82 DSGVO auch zunehmend sehr weit ausgelegt. Einige Gerichte gehen sogar davon aus, dass der den Klägern zuzusprechende Schadensersatz eine abschreckende Wirkung haben bzw. abschreckende Höhe erreichen müsse. Diese Entwicklung kann erhebliche finanzielle und andere Konsequenzen für datenverarbeitende Unternehmen haben. Datenpannen und andere Verstöße gegen das Datenschutzrecht betreffen häufig nicht nur einzelne Personen. Gerade im Unternehmensbereich wirkt sich eine fehlerhafte Datenverarbeitung zumeist auf eine Vielzahl von Personen aus. Daher stehen Datenpannen großer Unternehmen auch bei Verbraucheranwälten und kommerziellen Prozessfinanzieren besonders im Fokus. Je mehr Personen potenziell von einem Datenschutzverstoß betroffen sind, desto größer ist auch der potenzielle Gewinn für Prozessfinanzierer und ähnliche Akteure. Gerade solche Vorfälle eignen sich besonders für Massenverfahren und führen zu einer Kommerzialisierung der Schadensersatzansprüche aus Art. 82 DSGVO.

## B. Beschluss des BVerfG zu Art. 82 DSGVO

Ein kürzlich veröffentlichter Beschluss des BVerfG vom 14.01.2021 (Aktenzeichen: 1 BvR 2853/19) erschwert es deutschen Gerichten künftig Schadensersatzklagen nach Art. 82 DSGVO mit der Begründung abzuweisen, der Kläger habe lediglich einen Bagatellschaden erlitten.

Über den folgenden Link können Sie den Beschluss des Bundesverfassungsgerichts abrufen:

https://www.bundesverfassungsgericht.de/e/rk20210114_1bvr285319.html

Oder scannen Sie den QR-Code:

In der Entscheidung hob das BVerfG ein Urteil des Amtsgerichts Goslar vom 27.09.2019 (Aktenzeichen: 28 C 7/19) auf. In dem Verfahren hatte ein Rechtsanwalt ein Unternehmen verklagt, weil dieses ihm unverlangt eine Werbe-E-Mail zugeschickt hatte. Der Kläger klagte unter anderem auf Unterlassung und Schadensersatz von mindestens 500 EUR. Das Amtsgericht gab ihm in Bezug auf den Unterlassungsanspruch statt. Es verurteilte das beklagte Unternehmen, dem Kläger keine weiteren Werbe-E-Mails zuzuschicken. Den geltend gemachten Anspruch auf immateriellen Schadensersatz nach Art. 82 DSGVO wies das Amtsgericht Goslar hingegen zurück. Es fehle an einer nennenswerten Beeinträchtigung des Klägers. Das Amtsgericht ließ eine Berufung zum Landgericht nicht zu. Wegen des geringen Streitwerts des Schadensersatzanspruchs handelte es in letzter Instanz.

Gegen diese Entscheidung erhob der Kläger Verfassungsbeschwerde. Er rügte, dass das Amtsgericht Goslar sein Recht auf den gesetzlichen Richter nach Art. 101 Abs. 1 S. 2 GG verletzt habe. Denn in dem Verfahren vor dem Amtsgericht sei die Auslegung von Art. 82 DSGVO, einer europarechtlichen Norm, entscheidungserheblich gewesen. Hierüber hätte nur der EuGH entscheiden dürfen. Das BVerfG gab der Verfassungsbeschwerde statt. Es hob die Entscheidung des Amtsgerichts Goslar auf. Bei der Frage nach einer möglichen Erheblichkeitsschwelle bei immateriellem Schadensersatz nach Art. 82 DSGVO handele es sich um eine bislang ungeklärte Rechtsfrage, deren Antwort auch nicht offensichtlich auf der Hand liege. Daher müsse ein deutsches Gericht diese Frage vor einer Entscheidung in letzter Instanz dem EuGH zur Vorabentscheidung vorlegen.

Der Beschlusses des BVerfG hat eine weitere, nicht zu unterschätzende Konsequenz zur Folge: Deutsche Gerichte dürfen nun Klagen auf immateriellen Schadensersatz nach Art. 82 DSGVO nicht mehr alleine mit der Begründung ablehnen, dass die vom Kläger erlittene Beeinträchtigung einen Bagatellschaden darstelle. Es bleibt abzuwarten, inwieweit Gerichte künftig bereit sein werden, entsprechende Klagen mit anderen Begründungen abzuweisen, etwa weil ein möglicher Verstoß gegen die DSGVO nicht hinreichend dargelegt wurde.

## C. DSGVO-Schadensersatztabelle

Die nachstehende Tabelle fasst Gerichtsentscheidungen, die Klägern immateriellen Schadensersatz wegen Datenschutzverstößen zusprechen, in übersichtlicher Form zusammen. Zudem führt sie auf, welche Verstöße zu welchen Schadenssummen führen. Darüber hinaus sind der DSGVO-Schadensersatztabelle auch weitere Entscheidungen, die wichtige Fragestellungen bei der Geltendmachung von DSGVO-Schadensersatz betreffen, zu entnehmen.

# Aktuelle Rechtsprechung zu Art. 82 DSGVO – Stand Februar 2021

## Teil 1: Beschluss des BVerfG vom 14. Januar 2021

| Entscheidung | Kernaussagen des Gerichts |
|---|---|
| **BVerfG**,<br>Beschl. v. 14.01.2021 (1 BvR 2853/19) | • Der Anspruch auf Geldentschädigung nach Art. 82 DSGVO ist in der Rechtsprechung des EuGH weder erschöpfend geklärt noch kann er in seinen einzelnen Voraussetzungen unmittelbar aus der DSGVO bestimmt werden. Details und genauer Umfang des Anspruchs sind noch unklar<br>• Auch in der bislang vorliegenden Literatur, die sich im Hinblick auf Erwägungsgrund 146 wohl für ein weites Verständnis des Schadensbegriffes ausspricht, sind die Details und der genaue Umfang des Anspruchs nach Art. 82 DSGVO noch unklar<br>• Von einer richtigen Anwendung des Unionsrechts, die derart offenkundig ist, dass für vernünftige Zweifel kein Raum bliebe (*acte clair*), ist daher nicht auszugehen<br>• Das Amtsgericht hätte nicht ohne Vorabentscheidungsersuchen an den EuGH entscheiden dürfen, dass sich kein Anspruch des Beschwerdeführers aus Art. 82 DSGVO ergebe, weil ein Schaden nicht eingetreten sei |

## Teil 2: Aktuelle Entscheidungen, in denen Gerichte Klägern Schadensersatz zugesprochen haben

| Entscheidung | Schadensersatz | DSGVO-Verstoß | Kernaussagen des Gerichts |
|---|---|---|---|
| **LAG Köln**,<br>Urt. v. 14.09.2020 (2 Sa 358/20)<br><br>BeckRS 2020, 31543<br><br>Vorgehend: ArbG Köln, Urt. v. 12.03.2020 (5 Ca 4860/19) | **300€** | Unbefugte Veröffentlichung einer PDF-Datei mit einem beruflichen Tätigkeitsprofil auf der Website der Beklagten nach Ende des Arbeitsverhältnisses der Klägerin | • Die Veröffentlichung von Daten kann einen immateriellen Schaden i.S.v. Art. 82 DSGVO darstellen<br>• Neben dem Verschuldensgrad und der Intensität der Rechtsverletzung, hängt die Höhe des Schmerzensgelds auch davon ab, ob die Datenschutzbehörde den Verstoß bereits gerügt hat<br>• Schadensersatz nach der DSGVO soll einen erzieherischen Effekt haben<br>• Die Revision wurde nicht zugelassen |
| **ArbG Dresden**,<br>Urt. v. 26.08.2020 (13 Ca 1046/20)<br><br>BeckRS 2020, 26940 | **1.500€** | Verstoß gegen Art. 9 DSGVO wegen unbefugter Veröffentlichung von Gesundheitsdaten | • Durch die DSGVO ist eine Verschärfung der Rechtslage bzgl. des immateriellen Schadensersatz eingetreten<br>• Der Begriff des Schadens muss so ausgelegt werden, dass er den Zielen der DSGVO in vollem Umfang entspricht<br>• Die Auslegung gebietet eine abschreckende Wirkung des Schadensersatzes<br>• Die Kriterien des Art. 83 Abs. 2 DSGVO können zur Bemessung des Schadensersatzes herangezogen werden<br>• Der Schaden liegt in der Rufschädigung und dem Kontrollverlust über personenbezogene Daten |
| **ArbG Neumünster**,<br>Urt. v. 11.08.2020 (1 Ca 247 c/20)<br><br>BeckRS 2020, 29998 | **1.500€**<br><br>(500€ pro Monat der verspäteten Auskunft) | Verstoß gegen Art. 15 Abs. 1 DSGVO wegen verspäteter Beantwortung eines Auskunftsanspruchs | • Schadensersatz soll eine abschreckende Wirkung haben<br>• Erwägungsgrund 146 DSGVO verlangt eine vollständige und effektive Entschädigung<br>• Bei der Bemessung der Höhe können sich Gerichte an den Kriterien des Art. 83 Abs. 2 DSGVO orientieren<br>• Der Schaden liegt in der Ungewissheit über die Verarbeitung der eigenen Daten |
| **LG Lüneburg,**<br>Urt. v. 14.07.2020 (9 O 145/19) | **1.000€** | Verstoß gegen Art. 6 Abs. 1 DSGVO sowie Art. 17 Abs. 1 lit. d) DSGVO durch unzulässige Meldung einer Person bei einer Wirtschaftsauskunftei | • Der Schaden liegt im Kontrollverlust über personenbezogene Daten<br>• Durch die unzulässige Offenlegung personenbezogener Daten droht eine öffentliche "Bloßstellung" / "Stigmatisierung" welche über den immateriellen Schadensersatzanspruch ausgeglichen werden muss<br>• Die beabsichtigte abschreckende Wirkung von Schadensersatzansprüchen wird nur durch "empfindliche" Schmerzensgelder erreicht; insbesondere, wenn es an einer Kommerzialisierung fehlt<br>• Kein genereller Ausschluss von Bagatellfällen |
| **ArbG Lübeck**,<br>Beschl. v. 20.06.2020 (1 Ca 538/19)<br><br>ZD 2020, 422 | **(Anspruch in Höhe von 1.000€ möglich)**<br><br>(Prozesskostenhilfebeschluss — das Gericht hielt einen Anspruch i.H.v. max. 1.000€ für hinreichend wahrscheinlich) | Verstoß gegen Art. 4 Nr. 2 und Art. 6 Abs. 1 lit. b) DSGVO wegen unbefugter Veröffentlichung eines Mitarbeiterfotos auf sozialem Netzwerk | • Die effektive Ahndung von Verstößen gegen die DSGVO und das BDSG gebieten eine abschreckende Wirkung<br>• Der Schaden liegt in der unbefugten Veröffentlichung eines Fotos in einem sozialen Netzwerk |
| **LG Darmstadt**,<br>Urt. v. 26.05.2020 (13 O 244/19)<br><br>ZD 2020, 642 | **1.000€** | Verstoß gegen Art. 6 Abs. 1 DSGVO wegen unbefugter Offenlegung von Bewerberdaten an einen Dritten und Verstoß gegen Mitteilungspflicht aus Art. 34 DSGVO | • Durch die Veröffentlichung an einen unbeteiligten Dritten ist eine „etwaige" Bagatellgrenze überschritten<br>• Der Schaden liegt im Kontrollverlust darüber, wer Kenntnis von personenbezogenen Daten hat |
| **AG Pforzheim**,<br>Urt. v. 25.03.2020 (13 C 160/19)<br><br>BeckRS 2020, 27380 | **4.000€** | Verstoß gegen Art. 9 Abs. 1 DSGVO wegen unbefugter Offenlegung von Gesundheitsdaten | • Schadensersatz muss eine abschreckende Wirkung bzw. Höhe haben<br>• Der Schadensersatz muss zudem auch eine Genugtuungsfunktion für die betroffene Person erfüllen<br>• Zu berücksichtigen ist die besonders hohe Sensibilität der personenbezogenen Daten (hier Gesundheitsdaten) |
| **ArbG Düsseldorf**,<br>Urt. v. 05.03.2020 (9 Ca 6557/18)<br><br>NZA-RR 2020, 409 | **5.000€** | Unvollständige und verspätete Auskunft nach Art. 15 Abs. 1 DSGVO und Verstoß gegen das Transparenzgebot nach Art. 12 Abs. 3 DSGVO | • Der Schaden liegt im Kontrollverlust über personenbezogene Daten<br>• Die effektive Sanktionierung von DSGVO-Verstößen ist nur durch eine „abschreckende Wirkung" des Schadensersatzes zu erreichen<br>• Die Höhe des Schadens hängt von der wirtschaftlichen Leistungsfähigkeit des Beklagten ab |

## Teil 3: Aktuelle Entscheidungen, in denen Gerichte Schadensersatzansprüche abgelehnt haben

| Entscheidung | Aussagen zum Schadensersatz | DSGVO-Verstoß | Kernaussagen des Gerichts |
|---|---|---|---|
| **LG Landshut**,<br>Urt. v. 06.11.2020 (51 O 513/20)<br><br>BeckRS 2020, 33148 | Das Gericht lehnte einen Schadensersatzanspruch mangels Schadens ab | Behaupteter Verstoß gegen Art. 6 DSGVO durch die nicht erfolgte Schwärzung von personenbezogenen Daten von Wohnungseigentümern | • Schmerzensgeld nach der DSGVO ist nicht für einen Bagatellverstoß ohne ernsthafte Beeinträchtigung zu gewähren<br>• Die Verletzungshandlung muss zu einer konkreten und nicht nur unbedeutenden oder empfundenen Verletzung von Persönlichkeitsrechten führen<br>• Es muss eine objektiv nachvollziehbare Beeinträchtigung mit gewissem Gewicht erfolgt sein |
| **LG Köln**,<br>Urt. v. 07.10.2020 (28 O 71/20)<br><br>ZD 2021, 47 | Das Gericht lehnte einen Schadensersatzanspruch mangels eines über einen Bagatellverstoß hinausgehenden Schadens ab | Behaupteter Verstoß gegen die DSGVO durch die unbefugte Zusendung eines Kontoauszugs an einen Dritten | • Schmerzensgeld bei Bagatellfällen entspricht nicht dem Sinn und Zweck des Art. 82 DSGVO<br>• Ansonsten besteht die Gefahr einer uferlosen Häufung von Ansprüchen nach Art. 82 DSGVO<br>• Für den immateriellen Schadensersatz gelten die i.R.v. § 253 BGB entwickelten Grundsätze und die Kriterien des Art. 83 Abs. 2 DSGVO |
| **LG Frankfurt a.M.**,<br>Urt. v. 18.09.2020 (2/27 O 100/20)<br><br>GRUR-RS 2020, 24557 | Das Gericht lehnte einen Schadensersatzanspruch mangels Kausalität zwischen DSGVO-Verstoß und Schaden ab | Behauptete Verletzung der Datensicherheit durch die Veröffentlichung von Kreditkartendaten und Verstoß gegen Art. 5 Abs. 1 lit. a) oder lit. f) DSGVO. Dieser Verstoß wurde mit Verweis auf die Darlegungs- und Beweislast abgelehnt | • Immaterieller Schaden kann in der Zugänglichmachung personenbezogener Daten an Dritte (Bloßstellung) liegen<br>• Der Kläger ist für den Verstoß gegen die DSGVO darlegungs- und beweispflichtig<br>• Die Verletzungshandlung muss zu einer konkreten Verletzung von Persönlichkeitsrechten geführt haben<br>• Eine weite Auslegung des Schadens widerspricht der deutschen zivilrechtlichen Systematik |
| **LG Hamburg**,<br>Urt. v. 04.09.2020 (324 S 9/19)<br><br>BeckRS 2020, 23277 | Das Gericht lehnte einen Schadensersatzanspruch mangels Schadens ab | Behaupteter Verstoß gegen Art. 5 Abs. 1 lit. a) DSGVO durch die Veröffentlichung privater Daten im Internet | • Voraussetzung für einen immateriellen Schadensersatz ist ein Verstoß gegen die DSGVO sowie ein kausaler Schaden<br>• Der immateriellen Ausgleichspflicht aus Art. 82 DSGVO muss eine benennbare und tatsächliche Persönlichkeitsverletzung gegenüberstehen (bspw. in Form einer Bloßstellung)<br>• Die Darlegungs- und Beweislast liegt beim Kläger |
| **LG Frankfurt a.M.**,<br>Urt. v. 03.09.2020 (2-03 O 48/19)<br><br>GRUR-RS 2020, 25111 | Das Gericht lehnte einen Schadensersatzanspruch mangels Schadens ab | Behaupteter Verstoß gegen Art. 6 Abs. 1 lit. b) DSGVO durch die Löschung eines Posts auf sozialem Netzwerk | • Der Kläger hat sowohl den DSGVO-Verstoß als auch den dadurch entstandenen Schaden substantiiert darzulegen |

**Teil 3: Aktuelle Entscheidungen, in denen Gerichte Schadensersatzansprüche abgelehnt haben**

| Entscheidung | Aussagen zum Schadensersatz | DSGVO-Verstoß | Kernaussagen des Gerichts |
|---|---|---|---|
| **AG Frankfurt a.M.**, Urt. v. 10.07.2020 (385 C 155/19 (70))<br><br>BeckRS 2020, 22861 | Das Gericht lehnte einen Schadensersatzanspruch mangels Schadens ab | Behaupteter Verstoß gegen Mitteilungspflicht nach Art. 34 DSGVO und Auskunftspflicht nach Art. 15 DSGVO. Zuerkannt wurde ein Verstoß gegen die Integrität und Vertraulichkeit personenbezogener Daten nach Art. 5 Abs. 1 lit. f) DSGVO | Notwendig ist eine objektiv nachvollziehbare und feststellbare Beeinträchtigung (ein Gefühl des Unbehagens ist nicht ausreichend)<br>• Beweiserleichterung beim Nachweis der Kausalität zwischen Verletzung des Datenschutzes und Schaden nach Art. 5, 24 DSGVO<br>• Notwendig ist ein kausaler Schaden<br>• Die Beachtung des unionsrechtlichen Effektivitätsgrundsatzes verlangt eine Abschreckungswirkung |
| **AG Hannover**, Urt. v. 09.03.2020 (531 C 10952/29) | Das Gericht lehnte einen Schadensersatzanspruch mangels Schadens und Kausalität ab | Speicherung von Kundendaten durch Reisebüro | • Kein Schmerzensgeld für einen Bagatellverstoß ohne ernsthafte Beeinträchtigung oder für bloß individuell empfundene Unannehmlichkeiten<br>• Der Kläger hat die Kausalität zwischen dem Verstoß der DSGVO und dem dadurch eingetretenen Schaden zu beweisen |
| **OLG Dresden**, Hinweisbeschl. v. 11.12.2019 (4 U 1680/19)<br><br>BeckRS 2019, 36042 | Das Gericht lehnte einen Schadensersatzanspruch mangels DSGVO-Verstoßes und Schadens ab | Behaupteter Verstoß gegen Art. 4 Nr. 2 i.V.m. Art. 6 Abs. 1 lit. a) DSGVO wegen der Löschung eines Posts und der Sperrung eines Internetkontos | • Die bloße Sperrung eines Posts (also von Daten) und Datenverlust stellt noch keinen Schaden i.S.d. DSGVO dar<br>• Beeinträchtigungen mit „Bagatellcharakter" rechtfertigen keinen immateriellen Schadensersatz |
| **LG Karlsruhe**, Urt. v. 02.08.2019 (8 O 26/19)<br><br>BeckRS 2019, 17459 | Das Gericht lehnte einen Schadensersatzanspruch mangels DSGVO-Verstoßes ab | Behaupteter Verstoß gegen Art. 16 DSGVO durch unterlassene Korrektur eines Kreditwürdigkeits-Scorewerts | • Beim Anspruch aus Art. 82 DSGVO bleibt es bei den allgemeinen Regeln zivilrechtlicher Beweislastverteilung<br>• Der Kläger ist für den Verstoß und den Schaden darlegungs- und beweispflichtig<br>• Das Verschulden wird nach Art. 82 Abs. 3 DSGVO widerleglich vermutet; insoweit gilt eine Beweislastumkehr<br>• Ein Verstoß gegen die DSGVO allein führt nicht aus generalpräventiven Gründen zu einer Ausgleichspflicht |
| **OLG Dresden**, Beschl. v. 11.06.2019 (4 U 760/19)<br><br>ZD 2019, 567 | Das Gericht lehnte einen Schadensersatzanspruch mangels Schadens ab | Behaupteter Verstoß gegen Art. 6 Abs. 1 lit. a) DSGVO wegen der Löschung bzw. Sperrung eines Social Media Profils | • Die Auslegung von Art. 82 DSGVO ergibt, dass nicht jede individuell empfundene Unannehmlichkeit oder Bagatellverstöße einen immateriellen Schaden begründen<br>• Der Erwägungsgrund 146 DSGVO kann nicht im Sinne einer weiten Auslegung verstanden werden |
| **AG Diez**, Urt. v. 07.11.2018 (8 C 130/18)<br><br>BeckRS 2018, 28667 | Das Gericht lehnte einen Schadensersatzanspruch mangels Schadens ab | Behaupteter Verstoß gegen Art. 6 Abs. 1 lit. a) DSGVO wegen „einer als unzulässig monierten Email" | • Der bloße Verstoß gegen die DSGVO führt nicht zu einem Schadensersatz<br>• Dem Betroffenen muss ein spürbarer Nachteil entstanden sein<br>• Ein Bagatellverstoß ist nicht ausreichend |

**Teil 4: Sonstige Entscheidungen mit Bezug zu Art. 82 DSGVO**

| Entscheidung | Kontext der Entscheidung | Relevante Aussage des Gerichts mit Bezug zu Art. 82 DSGVO |
|---|---|---|
| **LG Rostock**, Urt. v. 11.08.2020 (3 O 762/19)<br><br>GRUR-RS 2020, 32027 | Wirksamkeit der Einwilligung in die Nutzung von Drittanbieter-Cookies | Den beklagten Verantwortlichen trifft nach Art. 24 Abs. 2 und Art. 5 Abs. 1 DSGVO die Darlegungs- und Beweislast dafür, dass er sich datenschutzrechtskonform verhalten hat |

LATHAM&WATKINS LLP

Der Abdruck der Tabelle erfolgt mit freundlicher Genehmigung der Latham & Watkins LLP.

Die Tabelle können Sie über den folgenden Link herunterladen:

https://de.lw.com/thoughtLeadership/Latham-DSGVO-Schadensersatztabelle

Oder scannen Sie den QR-Code:

## D. Fazit und Ausblick

Die bisherige Rechtsprechung deutscher Gerichte zu Art. 82 DSGVO ist ausgesprochen uneinheitlich. Bis zu einer Entscheidung des EuGH über das Erfordernis einer gewissen Erheblichkeitsschwelle bei immateriellem Schadensersatz wird noch einige Zeit vergehen. Eine Entscheidung vor 2022 erscheint eher unwahrscheinlich.

Bis dahin können Gerichte laufende Verfahren etwa mit der Begründung entscheiden, dass es auf eine mögliche Erheblichkeitsschwelle nicht ankomme. Dies ist etwa dann der Fall, wenn ein möglicher Verstoß nicht hinreichend dargelegt worden ist. Vor diesem Hintergrund wird es für Unternehmen zunehmend wichtiger, ihre internen Prozesse und sonstigen Maßnahmen zur Umsetzung der DSGVO auf eine Art und Weise zu dokumentieren, die es ihnen ermöglicht, spätere Gerichtsverfahren erfolgreich zu bestreiten.


### Über den Autor

**Tim Wybitul**
ist Partner im Frankfurter Büro von Latham & Watkins und ein führender Datenschutzanwalt. Er berät deutsche und globale Unternehmen in komplexen Datenschutzfragen, vertritt Mandanten in Datenschutzstreitigkeiten vor Gericht und mit Behörden, bei internen Untersuchungen und in anderen datenschutzrechtlichen Auseinandersetzungen. Tim Wybitul ist Certified Information Privacy Professional (CIPP-EU/GDPR) sowie Fachanwalt für Arbeitsrecht. Der Deutsche Bundestag bestellte ihn wiederholt zum Sachverständigen für Anhörungen zu Datenschutzfragen.

# DIE STRAFBARKEIT JURISTISCHER PERSONEN NACH ART. 83 DSGVO

## Ein Stolperstein für die einheitliche Anwendung der DSGVO

Dr. Matthias Schmidl

Art. 83 DSGVO normiert hohe Geldbußen für Verantwortliche und Auftragsverarbeiter bei Verstößen gegen die DSGVO. Anhand rezenter Judikatur verschiedener Gerichte soll in diesem Beitrag aufgezeigt werden, dass Art. 83 DSGVO uneinheitlich ausgelegt wird und dies einen massiven Stolperstein für die einheitliche Anwendung der DSGVO darstellt.

### Die rechtliche Einordnung von Geldbußen nach Art. 83 DSGVO

Bei Geldbußen handelt es sich um Verwaltungsstrafen, die von Datenschutz-Aufsichtsbehörden verhängt werden, und nicht um Strafen, die von Gerichten für gerichtlich strafbare Handlungen verhängt werden.

Dies ergibt sich einerseits aus einem Vergleich der unterschiedlichen Sprachfassungen von Art. 83 DSGVO: So spricht die englische Sprachfassung von „administrative fines" und die französische von „amendes administratives".

Andererseits ergibt sich dies aus einem Vergleich zwischen Art. 83 und Art. 84 DSGVO i.V.m. den Erwägungsgründen 150 und 152: So sprich Erwägungsgrund 150 in Bezug auf Art. 83 klar von „verwaltungsrechtlichen Sanktionen", die von den Aufsichtsbehörden verhängt werden sollten. Erwägungsgrund 152, der sich auf

Art. 84 bezieht, nimmt hingegen auf „schwere Verstöße“ gegen die DSGVO Bezug und überlässt es den Mitgliedstaaten, ob die dagegen verhängten Sanktionen „strafrechtlicher oder verwaltungsrechtlicher Art“ sein sollen. Eine Ausnahme gibt es gemäß Art. 83 Abs. 9 i.V.m. Erwägungsgrund 151 nur für Estland und Dänemark, wo Geldbußen nach Art. 83 auf Antrag der Aufsichtsbehörde von einem Gericht zu verhängen sind.

Somit handelt es sich bei Geldbußen um eine verwaltungsrechtliche Sanktion, deren Verhängung sich nach den einschlägigen Verwaltungsverfahrensvorschriften der Mitgliedstaaten richtet, in Österreich somit nach dem Verwaltungsstrafgesetz 1991 (VStG).

Da es sich bei Geldbußen dennoch um Strafen im Sinne des Art. 6 EMRK handelt, müssen die Verfahrensvorschriften entsprechende Kautelen vorsehen, um die Rechte von Beschuldigten (vor allem das Selbstbezichtigungsverbot, nemo tenetur) und Zeugen (vor allem Gründe eine wahrheitsgemäße Aussage zu verweigern) zu wahren.

Zusätzlich zu den nationalen Verfahrensvorschriften enthält Art. 83 Abs. 2 und 3 DSGVO unmittelbar anwendbare Verfahrensvorschriften, die im Kollisionsfall entgegenstehendes nationales Recht verdrängen. Jedenfalls lässt sich Art. 83 Abs. 2 lit. b DSGVO entnehmen, dass nur schuldhaftes Verhalten zur einer Geldbuße führen kann. Die DSGVO normiert somit keine verschuldensunabhängige Haftung.

Eine Analyse von Art. 83 DSGVO erhellt, dass dieser wettbewerbsrechtlichen Geldbußen nachgebildet ist. Dies ergibt sich insbesondere aus einem Vergleich mit Art. 23 der Verordnung (EG) 1/2003. Daraus folgt, dass die zu Art. 23 der Verordnung (EG) 1/2003 ergangene Rechtsprechung[1] des EuGH von Relevanz ist.

## Die unmittelbare Strafbarkeit juristischer Personen

Die Sanktionsdrohungen des Art. 83 DSGVO richtet sich gegen Verantwortliche (Art. 4 Z 7) und Auftragsverarbeiter (Art. 4 Z 8) und damit auch gegen „juristische Personen“.

Der Begriff der juristischen Person wird vom EuGH in seiner Rechtsprechung weit ausgelegt und umfasst demnach nicht nur Körperschaften, die aufgrund ihrer Form selbständig Träger von Rechten und Pflichten sein können (wie eine GmbH oder eine AG), sondern auch Personengesellschaften, die – zumindest nach österreichischem Recht – nicht immer rechtsfähige Konstrukte sind, sodass sie nur durch ihre Gesellschafter im Rechtsverkehr auftreten können (etwa eine Gesellschaft nach bürgerlichem Recht, GesbR). Wesentliches Abgrenzungskriterium zu natürlichen Personen ist jedenfalls, dass eine juristische Person ein eigenes Rechtssubjekt ist und somit unmittelbarer Adressat von behördlichen oder gerichtlichen Entscheidungen sein kann und sich somit „schützend“ vor die für sie agierenden natürlichen Personen stellt.

Da es sich bei juristischen Personen aber um Rechtskonstrukte handelt, die nur durch natürliche Personen als deren Vertreter handeln können, stellt sich die Frage, ob juristische Personen überhaupt schuldfähig – im Sinne einer Einsichtsfähigkeit in das Unrecht der Tat – sind. Schuldhaftes Handeln ist aber Voraussetzungen für die Verhängung einer Geldbuße nach Art. 83 DSGVO.

Der österreichische Verfassungsgerichtshof hat in einer Entscheidung zum Ausdruck gebracht, dass juristische Personen nur dann für einen Regelverstoß verantwortlich gemacht werden können, wenn ihnen das Verhalten einer für sie handelnden natürlichen Person zugerechnet werden kann.[2] Es ist daher ein hinreichender Konnex zwischen einer juristischen Person und der für sie handelnden natürlichen Person(en) erforderlich. Im Umkehrschluss bedeutet dies, dass eine juristische Person sich das Handeln von Außenstehenden nicht zurechnen lassen und dafür auch keine Verantwortung übernehmen muss. Dies ist unstrittig.

Strittig ist jedoch, wie exakt die Zurechnung zu erfolgen hat.

## Denkschulen

Hinsichtlich der Frage der oben beschriebenen Zurechnung können zwei Denkschulen unterschieden werden, die zu völlig unterschiedlichen Ergebnissen führen. Gemäß „Denkschule 1“ muss sich eine juristische Person jedwedes Handeln/Unterlassen einer für sie tätigen Person

[1] Urteil vom 09.11.2010, C-92/09 und C-93/09.
[2] Siehe dazu das Erkenntnis vom 2.12.2016, G497/2015 u.a., abrufbar unter https://www.ris.bka.gv.at/Vfgh/.

zurechnen lassen und die Behörde muss nicht genau prüfen, welche konkrete natürliche Person für die juristische Person gehandelt hat/etwas unterlassen hat.

Gemäß „Denkschule 2" muss sich eine juristische Person nur das Handeln/Unterlassen bestimmter für sie tätiger Personen zurechnen lassen und die Behörde muss diese Person(en) ermitteln und ihnen ein Fehlverhalten nachweisen.

Letztere Denkschule ist vor allem in Deutschland und Österreich stark verbreitet, weil die Bestimmung des § 30 des österreichischen Datenschutzgesetzes (DSG)[3] beziehungsweise die ganz ähnliche Bestimmung des § 30 OWiG nur auf bestimmte vertretungsbefugte natürliche Personen abstellen.

## Entscheidungen

In der Rechtsprechung wird „Denkschule 1" vom EuGH bei der Verhängung wettbewerbsrechtlicher Geldbußen vertreten und kommt insbesondere im Urteil vom 18.09.2003, C-338/00 P, zum Ausdruck, wo es in Rz 98 heißt:

> *Demnach hat das Gericht entgegen den Ausführungen der Rechtsmittelführerin keinen Rechtsfehler begangen, als es die vorsätzliche Begehung der Zuwiderhandlung für feststehend erachtet hat, ohne die Benennung der Personen zu verlangen, die innerhalb des Unternehmens schuldhaft gehandelt hatten oder für die möglicherweise fehlerhafte Organisation der Rechtsmittelführerin hätten verantwortlich gemacht werden müssen.*

In diesem Zusammenhang ist auch von Relevanz, dass der EuGH die Schuldfähigkeit einer juristischen Person bejaht.

Dies kommt insbesondere im Urteil vom 23.01.2014, T-391/09, zum Ausdruck, wo es in Rz 37 und 38 heißt:

> *Auch das Argument, das die Klägerinnen aus dem „Schuldprinzip" oder dem Verschuldenserfordernis (vgl. oben, Rn. 26) ableiten wollen, ist nicht stichhaltig. In den Schlussanträgen der Generalanwältin Kokott in der Rechtssache ETI u. a. (oben in Rn. 26 angeführt), auf die sich die Klägerinnen berufen, wird nämlich auf die Schlussanträge des Generalanwalts Ruiz-Jarabo Colomer in der Rechtssache Aalborg Portland u. a./Kommission (C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P und C-219/00 P, Urteil vom 7. Januar 2004, Slg. 2004, I-123, I-133, Nrn. 63 bis 65) verwiesen.*

> *Wie es dort aber in Nr. 65 heißt, muss die Anwendung des „Schuldprinzips" bei juristischen Personen abgeändert werden. Bei den kollektiven Einheiten findet sich das volitive Element im strengen Sinne nicht, doch eine Rechtsfiktion erlaubt, ihnen Zuwiderhandlungen zuzurechnen, die die Folge der von ihnen an den Tag gelegten Verhaltensweisen sind. Vom Willen getragene Handlungen gibt es bei juristischen Personen nicht, wohl aber die Fähigkeit, gegen Rechtsnormen zu verstoßen, die für sie gelten, was zur Folge hat, dass einer juristischen Person ein Verstoß, den sie nicht begangen hat, nicht zugerechnet werden darf.*

> *Aus diesen Erwägungen ergibt sich ferner, dass das Verschulden, das nach Art. 23 Abs. 2 der Verordnung Nr. 1/2003 Tatbestandsmerkmal einer Zuwiderhandlung gegen die Wettbewerbsregeln ist, letztlich nur einer oder mehreren natürlichen Personen zugerechnet werden kann, obwohl die Kommission diese in ihrer Entscheidung, mit der sie eine solche Zuwiderhandlung im Hinblick auf eine oder mehrere juristische Personen feststellt, nicht benennen muss.*

Da, wie bereits ausgeführt, Art. 83 DSGVO starke Parallelen zu Art. 23 der Verordnung (EG) 1/2003 aufweist, scheint diese Rechtsprechung des EuGH übertragbar zu sein.

Auf Ebene der Mitgliedstaaten haben sich – soweit ersichtlich – bis dato der französische Conseil d'Etat[4], das Landgericht Bonn[5] sowie der österreichische Verwaltungsgerichtshof[6] zu dieser Frage geäußert.

Während der Conseil d'Etat implizit die Rechtsauffassung des EuGH vertritt, wird dies im Urteil des LG Bonn deutlich hervorgehoben: Das LG Bonn geht sogar so weit, § 30 OWiG nicht anzuwenden, weil Art. 83 DSGVO ein Verbandsverantwortlichkeitsmodell sui generis darstelle und insoweit nicht auf das rechtswidrige und schuldhafte Handeln vertretungsbefugter natürlicher Personen abzustellen sei.[7]

Die gegenteilige Rechtsauffassung wird vom österreichischen Verwaltungsgerichtshof vertreten, der § 30 DSG nicht von Art. 83 DSGVO verdrängt sieht, das Argument der Parallelität zwischen Art. 83 DSGVO und Art. 23 der Verordnung (EG) 1/2003 ausdrücklich verworfen hat und daher verlangt, dass die Aufsichtsbehörde jene vertretungsbefugten natürlichen Personen zu ermitteln und in Straferkenntnis zu benennen hat, die im Namen der juristischen Person rechtswidrig und schuldhaft gehandelt haben.

[3] Abrufbar unter https://www.ris.bka.gv.at/Bundesrecht/.
[4] Entscheidung vom 12.06.2020, Nr. 430810, Société Google LLC (Bestätigung einer von der CNIL verhängten Geldbuße); abrufbar in französisch unter https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil.
[5] Urteil vom 11.11.2020, 29 OWi 1/20, abrufbar unter http://www.justiz.nrw.de/nrwe/lgs/bonn/lg_bonn/j2020/29_OWi_1_20_Urteil_20201111.html.
[6] Erkenntnis vom 12.05.2020, Ro 2019/04/0229, abrufbar unter https://www.ris.bka.gv.at/Vwgh/.
[7] Vgl. dazu ausführlich Zaczek, Das Verbandsverantwortlichkeitsmodell des Art. 83 DSGVO, in: Jahnel (Hrsg.), Datenschutzrecht. Jahrbuch 20 (2021), S 257 ff.

Diese unterschiedliche Rechtsprechung hat Auswirkungen auf das Verwaltungsstrafverfahren: Es macht aus Sicht der Aufsichtsbehörde nämlich einen großen Unterschied, ob die strafbare Handlung nur der juristischen Person vorgeworfen wird oder ob zusätzlich die Handlung auch allen – zum Tatzeitpunkt – vertretungsbefugten natürlichen Personen vorgeworfen und ihnen die Stellung als Beschuldigter eingeräumt werden muss.

## Zusammenfassung

Der vorliegende Beitrag zeigt, dass die Auslegung von Art. 83 DSGVO im Hinblick auf die Strafbarkeit juristischer Personen in den Mitgliedstaaten unterschiedlich ausgelegt wird. Insbesondere die Rechtsprechung des französischen Conseil d'Etat und des LG Bonn auf der einen und jene des österreichischen Verwaltungsgerichtshofes auf der anderen Seite stehen in diametralem Gegensatz zueinander.

Der EuGH wurde bis dato noch nicht im Wege einer Vorabentscheidung befasst, obwohl es – zumindest in Österreich – einige Anlassfälle dafür gegeben hätte.

Es bleibt daher zu hoffen, dass diese unterschiedliche Rechtsprechung, die enorme Auswirkungen auf die Verhängung von Geldbußen gegen juristische Personen hat, in näherer Zukunft durch den EuGH einer Klärung zugeführt wird.

## Über den Autor

**Dr. iur. Matthias Schmidl**
studierte Rechtswissenschaften in Wien und Groningen (NL). Er ist seit 2014 stellvertretender Leiter der Österreichischen Datenschutzbehörde. Zuvor war er beim österreichischen Verwaltungsgerichtshof, im Verfassungsdienst des österreichischen Bundeskanzleramtes und in der Geschäftsstelle der ehemaligen österreichischen Datenschutzkommission tätig. Zahlreiche Publikationen zu datenschutzrechtlichen Themen, Mitherausgeber eines Kommentars zur DSGVO und zum DSG; Vortragstätigkeiten im In- und Ausland.

▶ https://www.dsb.gv.at/

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

# §§ 30, 130 OWIG VOR DER HERAUSFORDERUNG EINER EUROPAWEIT HARMONISIERTEN BEBUßUNG NACH ART. 83 DS-GVO

Maria Christina Rost

Die Diskussionen um die Bebußung von Datenschutzverstößen nach der DS-GVO fahren sich immer wieder an einem Punkt fest, an § 41 BDSG und der Frage, ob § 41 BDSG europarechtswidrig ist, weil er die entsprechende Anwendung von §§ 30 und 130 OWiG vorsieht. Die Frage ist berechtigt und die „Többens-Trias" der §§ 9, 30, 130 OWiG komplex. Letztlich brauchen wir jedoch eine Lösung, die europäisch zur harmonisierten Bebußung führt.

Die Diskussion, die jetzt im Zusammenhang mit dem europäischen Bußgeldverfahren wegen Datenschutzverstößen geführt wird, ist nicht neu. Vom Unterschied zwischen Verbandsgeldbuße und Unternehmensgeldbuße wurde schon früher gesprochen.

Ausweislich eines Gutachtens des Bundeskartellamtes aus Anlass der Tagung des Arbeitskreises Kartellrecht am 4. Oktober 2012 wurde ein Hintergrundpapier erarbeitet (Titel: Kartellbußgeldverfahren zwischen deutschem Systemdenken und europäischer Konvergenz). In diesem wurde bereits bei der Europäisierung des Kartellrechts über die den Datenschutz beschäftigenden Fragestellungen diskutiert.

Der europäische Unternehmensbegriff wurde mit dem 9. GWB-ÄndG-E ins deutsche Kartellrecht übernommen. Bereits da bedurfte es

der Auseinandersetzung mit dem Wandel vom deutschen Rechtsträgerprinzip auf das europäische Funktionsträgerprinzip.

Das WP 253 des Europäischen Datenschutzausschusses hat bereits erste Indizien für die Auslegung des Art. 83 DS-GVO festgelegt. Die DSK hat in einer Entschließung vom 3. April 2019 bereits darauf hingewiesen, dass die nationalen Haftungsregeln bisher nicht europarechtkonform der neuen Rechtslage angepasst wurden. Der § 41 Abs. 1 BDSG verweise unzutreffend auf die zurechnungseinschränkenden Regeln im OWiG. Das Landgericht Bonn hat nun in seiner Entscheidung v. 11.11.2020 Az.: 29 OWi 1/20 festgestellt, dass § 30 Abs. 1 OWiG und das deutsche Rechtsträgerprinzip keine Anwendung finden. Die fruchtlose Forderung der DSK aus der Entschließung vom 3. April 2019 an den nationalen Gesetzgeber, diese Frage in die Beratungen zum Zweiten Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) aufzunehmen, lebt damit erneut auf.

Adressaten der datenschutzrechtlichen Normen sind die verantwortliche Stelle und der Auftragsverarbeiter. Im Falle eines Unternehmens richtet sich die Norm an das Unternehmen. Faktisch gehandelt wird durch Personen. Im Verwaltungsverfahren ergeben sich daraus keine wesentlichen Schwierigkeiten. Dort gelten für Unternehmen und natürliche Personen im Verfahren keine unterschiedlichen Anforderungen. Das Handeln von Mitarbeitern wird dem Unternehmen zugerechnet und in der Praxis geht es nur um das Verhalten des Unternehmens.

Im Bußgeldverfahren ist die Lage jedoch sehr viel komplexer. Nach nationalem Recht steht im Zentrum des Handelns das Handeln natürlicher Personen. Hier kommt das dem deutschen Ordnungswidrigkeitenverfahren zugrundeliegende Rechtsträgerprinzip zum Tragen. Nach bisherigem Rechtsverständnis ist nicht das Verhalten aller Mitarbeiter des Unternehmens sanktionierbar.

Vielmehr ist es das Verhalten ganz bestimmter Personen in Führungs- und Aufsichtspositionen. Diesen rechnet das Gesetz in § 9 OWiG die Eigenschaft eines „Unternehmens" zu. Und nur für deren Verhalten kann nach § 30 OWiG das Unternehmen mit einer Geldbuße belegt werden.

Daher sind nach dem Rechtsträgerprinzip, in jedem Einzelfall und für jedes beteiligte Unternehmen die Verantwortlichkeiten aufzuklären, wenn auch § 30 Abs. 4 OWiG diesbezüglich mit Blick auf europäische Entwicklungen schon gelockert wurde. § 30 Abs. 4 OWiG eröffnet die Abkoppelung der Verbandsgeldbuße von der Ahndung der Anknüpfungstat im selbstständigen Verfahren und schafft so die rechtliche Möglichkeit, die Geldbuße gegen den Verband auch dann zu verhängen, wenn der Täter der konkreten Anknüpfungstat nicht ermittelt ist. Das bedeutet, es kann nur jemand aus dem Täterkreis gehandelt haben oder es steht der Vorwurf der fahrlässigen Aufsichtspflichtverletzung durch eine mangelhafte Betriebsorganisation im Raume.

Auf weitere Rechtsträger des Gesamtunternehmens – etwa weitere juristische Personen eines Konzerns – erstreckt sich die Bußgeldhaftung nach deutschem Recht nicht (LG Bonn v. 11.11.2020 Az. 29 OWi/20 Rz. 49).

Das Rechtsträgerprinzip lässt eine solche Konstruktion nicht zu. Im deutschen Recht ist funktional ein der Konzernhaftung vergleichbares Instrument die Bebußung von Aufsichtspflichten im Konzern nach § 130 OWiG, bei der die Konzernmutter für die Verletzung einer Aufsichtspflicht über die Tochter haftet. Für den Umfang der Aufsichtspflicht im Sinne des § 130 OWiG sind die tatsächlichen Verhältnisse im Konzern maßgeblich, weshalb auf die tatsächliche Einflussnahme der Konzernmutter auf die Tochtergesellschaft abzustellen ist. Allerdings ist die Frage, ob das geltende Recht es zulässt, eine unzureichende Aufsicht der lenkenden Obergesellschaft über mit ihr verbundene Untergesellschaften, also vor allem Muttergesellschaft im Konzern über die Tochtergesellschaft, aus der heraus die Anlass-Zuwiderhandlung begangen wurde, nach § 130 OWiG zu ahnden, stark umstritten.

Dies kollidiert mit dem europäischen Funktionsträgerprinzip. Die DS-GVO lehnt an das europäische Kartellrecht an. Daraus kann man entnehmen, dass das Verfahren für die Kartellverfolgung, Abstellung und Ahndung auf einem einheitlichen Verfahren verwaltungsrechtlicher Prägung basiert. Adressaten sind die Unternehmen und die Handlungen von Personen werden im Rahmen eines Organ- oder Beschäftigungsverhältnis zugerechnet. Die Vorgaben für die haftungsbegründende Zurechnung sind weniger eng als in dem zuvor beschrieben deutschen Ordnungswidrigkeitenverfahren. In dem Verfahren wird der funktionale Unternehmensbegriff zugrunde gelegt. Das supranationale europäische Kartellrecht geht von einer unmittelbaren Verantwortlichkeit des Unternehmens aus. Nach dem Funktionsträgerprinzip haftet das Unternehmen als funktionale Einheit (LG Bonn v. 11.11.2020 Az. 29 OWi/20 Rz. 50). Hat ein Unternehmen mehrere Rechtsträger – wird danach ein einheitliches Unternehmen von mehreren juristischen Personen getragen – kann gegen sämtliche Rechtsträger die Geldbuße verhängt werden. Die einzelnen Rechtsträger des Unternehmens sind nach der Entscheidung des LG Bonn nur als formale Adressaten der Sanktionsent-

scheidung, als Verfahrensbetroffene und als Adressaten der Vollstreckung relevant. Für die Gesamtgeldbuße haften sie als Gesamtschuldner. Hieraus wird deutlich, dass in diesem Fall der gesamte Konzern haftet, sofern die Voraussetzungen einer wirtschaftlichen Einheit vorliegen.

Während nunmehr das LG Bonn zumindest den Weg zu einem europäischeren Ansatz geöffnet hat, geht das Bundesverwaltungsgericht der Republik Österreich in seiner Entscheidung v. 19.08.2019, Az. W211 2208885-1, welches über eine mit § 30 OWiG vergleichbare Norm zu entscheiden hatte, gerade nicht von einem Normenvorrang des Art. 83 Abs. 4 bis 6 DS-GVO aus. Das Straferkenntnis (dort handelt es sich um eine sog. Verwaltungsstrafe) wurde aufgehoben, weil die Geldbuße nicht an das Verhalten einer natürlichen Person angeknüpft war.

Allein durch diese beiden Entscheidungen kommt es zu einer Verzerrung der Harmonierung der Anwendung der DS-GVO. Die Entscheidung des Conseil d´Etat hilft hier nicht weiter. Entscheidungen aus weiteren Mitgliedstaaten sind noch abzuwarten. Sinnvoll wäre es letztlich, einen europäischen Vergleich der Verfahrensnormen für die Bußgeldverfahren nach DS-GVO vorzunehmen. Letztlich wird die Streitfrage vielleicht durch den EuGH entschieden werden müssen.

Die Vertreter der engen Auslegung werden sich entgegenhalten lassen müssen, dass die Anknüpfung an Art. 83 Abs. 4 bis 6 DS-GVO und das Funktionsträgerprinzip eine deutliche zielführende Ahndung versprechen und das Rechtsträgerprinzip als Hemmschuh für eine effektive Ahndung von Verstößen gegen die DS-GVO zu sehen ist.

Die Frage des Normenvorrang von Art. 83 Abs. 4 bis 6 DS-GVO kann europaweit nur einheitlich betrachtet werden.

Die naheliegende Gefahr, dass es europaweit zu einer unterschiedlichen Sanktionierungspraxis käme, widerspräche dem Ziel einer einheitlichen sowie effektiven Sanktionierung von Datenschutzverstößen von Unternehmen und damit einem der Grundanliegen der DS-GVO, wie sich aus den Erwägungsgründen 9, 10, 11, 13, 129 und schließlich auch 148 entnehmen lässt. Auch wenn den Erwägungsgründen keine Rechtsnormqualität zukommt, so haben sie doch zumindest „wegweisende“ Funktion.

Zudem steht ein Verstoß gegen den Effektivitätsgrundsatz unzweifelhaft im Raume. Wenn auch der europäische Gesetzgeber in Art. 83 Abs. 8 DS-GVO für die Gewährleistung angemessener Verfahrensgarantien „einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren“ auch auf das Recht der Mitgliedstaaten verweist. Der Inhalt dieser Vorschrift, insbesondere als nationale Regelungsbefugnis, ist im Lichte des europäischen Effektivitätsgebots („effet utils“ st. Rspr. EuGH vgl. Rechtsache C 6/90, NJW, 165, Rn. 32 m.w.N. ) auszulegen.

Das LG Bonn führt hierzu aus, dass in Ermangelung eines europäischen Bußgeldverfahrensrechts auf das nationale Verfahrensrecht nur insoweit zurückgegriffen werden darf, als damit die effektive Durchsetzung und praktische Wirksamkeit der DS-GVO gewährleistet bleiben. Die Nationalen Regelungskompetenzen nach Art. 83 Abs. 8 DS-GVO beziehen sich auf das Bußgeldverfahren. Laut dem LG Bonn können in Grenzbereichen zwischen Verfahrensrecht und materiellem Recht daher nur, wenn überhaupt, allenfalls einzelne materielle-rechtliche Vorschriften aus dem nationalen Recht angewendet werden, sofern das nationale Verfahrensrecht die Anwendung fordert. Diese materiell-rechtlichen Vorschriften können aber nur solche sein, die einer effektiven bußgeldrechtlichen Ahndung nicht entgegenstehen. Eine Einschränkung und Schwächung des unionsrechtlichen Haftungsmodells durch die Vorschriften wie in § 30 Abs. 1 OWiG ist nach dem LG Bonn von Art. 83 Abs. 8 DS-GVO nicht gedeckt.

Es dürfte ein Auftrag an den nationalen Gesetzgeber sein, seine im nationalen Recht getroffenen Entscheidungen im Zusammenhang mit Art. 83 Abs. 4 bis 6 DS-GVO auf den Prüfstand zu stellen. Es ist in der Praxis deutlich geworden, dass § 30 und 130 OWiG und das dahinterstehende Rechtsträgerprinzip im Lichte des europäischen Funktionsträgerprinzip keinen Beitrag zur Harmonisierung der Bußgelder nach DS-GVO leisten, sondern eher diese behindern. Nicht nur § 30 Abs. 1 DS-GVO sollte aus § 41 BDSG genommen werden. Auch der Verbleib des § 130 OWiG sollte nachdrücklich überdacht werden. Denn mit dem europäischen Funktionsträgerprinzip wären beide Normen umfasst.

Über die Autorin

**Maria Christina Rost**
ist Ministerialrätin beim Hessischen Beauftragen für Datenschutz und Informationsfreiheit (HBDI).

▶ https://datenschutz.hessen.de/

Anzeige

# 25% Rabatt auf den Jahrespreis für BvD Mitglieder

- seit über 40 Jahren
- monatlich
- topaktuell informiert über die wichtigsten Neuigkeiten, Risiken und die aktuelle Rechtsprechung
- mit konkreten Handlungsempfehlungen, Arbeitsmitteln und Checklisten für die tägliche Praxis

**https://www.datenschutz-berater.de**

- Seit über 40 Jahren ist der monatlich erscheinende **DATENSCHUTZ-BERATER** der verlässliche Ratgeber für Datenschutz und Datensicherheit. Mit den täglich wachsenden Möglichkeiten der Datenerhebung, -verarbeitung und -nutzung wird Datenschutz immer wichtiger. Technische und rechtliche Neuerungen, Risiken und die aktuelle Rechtsprechung fordern von den Verantwortlichen, sich fortlaufend zu informieren. Der Fachleser profitiert von konkreten Handlungsempfehlungen, Arbeitsmitteln und Checklisten für die tägliche Praxis. Literaturtipps und Terminhinweise für Aus- und Weiterbildung runden das Angebot ab.
- Zielgruppe sind Fach- und Führungskräfte der Datenschutzabteilung, Personalabteilung, interne und externe Datenschutzbeauftragte, Datenschutzabteilungen, Geschäftsführer, IT-Sicherheitsexperten und Revisoren.
- Die **R&W-Online Datenbank** online.ruw.de – mit allen Inhalten der R&W-Zeitschriften und des R&W-Buchportfolios – bietet eine publikationsübergreifende, schnelle und zuverlässige Recherchemöglichkeit. Highlights sind die Übersichtlichkeit, Bedienerfreundlichkeit und besonders die pdf-Darstellung gemäß des Original-Seitenlayouts.

## Per Faxantwort an 069/7595-1150

Name: _____

Firma: _____

Abteilung: _____

Straße: _____

PLZ | Ort: _____

Telefon: _____

E-Mail: _____

Datum | Unterschrift: _____

**Sichern Sie sich Ihr individuelles Vorteilsangebot und bestellen Sie jetzt den DSB – Datenschutz-Berater**

☐ **Testabo:** 3 Monate kostenlos lesen + 1 Zugang zur Online-Datenbank

Sie erhalten die nächsten 3 Ausgaben der Fachzeitschrift „Datenschutz-Berater" kostenlos. Falls Ihnen der „Datenschutz-Berater" gefällt, brauchen Sie nichts weiter zu unternehmen. Wenn Sie nicht innerhalb der Testzeit abbestellen, beginnt im Anschluss ein Jahresabo. Zunächst für ein Jahr (11 Ausgaben) zum Vorzugspreis von derzeit 339,- € inkl. aller Gebühren und MwSt. in Deutschland und anschließend bis auf Widerruf zum jeweils gültigen Jahrespreis. Das Abonnement kann bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus nach Erhalt der Rechnung zahlbar.

☐ **Jahresabo:** 11 Ausgaben + 1 Zugang zur Online-Datenbank

Sie erhalten die nächsten 11 Ausgaben der Fachzeitschrift „Datenschutz-Berater", sowie den Zugang zur Online-Datenbank. Der Abonnementvertrag wird für mindestens ein Jahr abgeschlossen. Das Abonnement kann jederzeit bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus nach Erhalt der Rechnung zahlbar und betragen 339,- € inkl. aller Gebühren und MwSt. in Deutschland.

**DATENSCHUTZ-BERATER**
kundenservice@ruw.de

dfv Mediengruppe

# NEUE EDSA-EMPFEHLUNGEN UND SCC-ENTWÜRFE IM LICHTE VON „SCHREMS II“: ENTWICKLUNGEN UND PERSPEKTIVEN

Dr. Tilman Dralle, LL.M., Jonathan Schröer, LL.M. und Dipl.-Wi.-Ing. Dominik Smasal[1]

## Einleitung

Das Schrems-II-Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020[2] löste erdrutschartige Folgen für das in der Datenschutz-Grundverordnung (DSGVO) angelegte Regime der Übermittlung personenbezogener Daten in Staaten außerhalb der Europäischen Union (EU) aus. Der bisherige, ziellandunabhängige „one-size-fits-all“-Ansatz bei der Nutzung der Datenübermittlungsmechanismen in Kapitel V der DSGVO ist einem grundlegend neuen Paradigma gewichen: Bei jedem Drittstaatentransfer muss der Datenexporteur nun einzelfallbezogen prüfen, ob der gewählte Transfermechanismus aus Art. 46 DSGVO im Hinblick auf die Rechtsordnung und gelebte Rechtspraxis des jeweiligen Ziellands für die angestrebte Datenübermittlung tatsächlich ein Schutzniveau sicherstellt, das dem in der EU garantierten Niveau „der Sache nach gleichwertig“ ist (*essentially equivalent*). Egal ob Standardvertragsklauseln (SCC)[3], Binding Corporate Rules (BCR), Codes of Conduct, Zertifizierungen oder ad-hoc-Vertragsklauseln: Die geeigneten Garantien gemäß Art. 46 DSGVO sind zwar *notwendig*, aber nicht in jedem Fall *hinreichend*. Werden Schutzlücken identifiziert, z.B. weil (Sicherheits-) Behörden im Zielland unverhältnismäßig weitreichenden Zugriff auf Daten haben, müssen zusätzliche, technisch-organisatorische Maßnahmen (sog. *supplementary measures*) ergriffen werden.[4] Welche zusätzlichen Schutzmaßnahmen letztlich erforderlich sind, um für den jeweiligen Transfer ein angemessenes Schutzniveau zu gewährleisten, wird die bestimmende Frage der kommenden Datenschutz-Dekade sein.

Am 11. November 2020, rund vier Monate nach der historischen Entscheidung des EuGH, hat der Europäische Datenschutzausschuss (EDSA) Handlungsempfehlungen zur Durchführung der einzelfallbasierten Prüfung durch den Datenexporteur sowie zur Ausgestaltung der ggf. erforderlichen zusätzlichen Schutzmaßnahmen vorgelegt (*Recommendations 01/2020*).[5] Diese werden ergänzt durch ein weiteres Papier des EDSA zu wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen (*Recommendations 02/2020*).[6] Beide Dokumente werden von den im EDSA vertretenen Aufsichtsbehörden im Rahmen ihrer Tätigkeit bereits angewendet.[7] Im November 2020 veröffentlichte darüber hinaus die Europäische Kommission einen Vorschlag zur Neufassung der Standardvertragsklauseln. Letztere greifen mit der Pflicht zur Durchführung eines sog. Transfer Impact Assessments (TIA, in der Praxis teilw. ebenfalls bezeichnet als „Data Transfer Risk Assessment“ oder „Schrems-II-Risikoanalyse“) die vom EDSA aufgestellten Anforderungen an eine Würdigung der Drittlandsrechtsordnung auf und schaffen hierfür einen formalen regulatorischen Rahmen.

Sowohl die aktuellen Empfehlungen des EDSA sowie der SCC-Entwurf der Europäischen Kommission werden in diesem Beitrag überblicksartig vorgestellt und hinsichtlich ihrer Praxisauswirkungen analysiert.

## EDSA-Empfehlungen zu zusätzlichen Schutzmaßnahmen

### Die sechsstufige Prüfung

Die EDSA-*Recommendations 01/2020* beschreiben ausführlich, wie ein als Datenexporteur han-

[1] Dieser Beitrag gibt ausschließlich die persönliche Meinung der Autoren wieder und stimmt nicht notwendigerweise mit den Ansichten des jeweiligen Arbeitgebers überein.

[2] Rechtssache C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems.

[3] Richtigerweise wäre hier der gesetzliche Terminus „Standarddatenschutzklauseln“ (i.S.v. Art. 46 DSGVO) zu verwenden, aus Gründen der Einfachheit wird allerdings im Folgenden an der in der Praxis geläufigen Begrifflichkeit festgehalten.

[4] EuGH, Rs. C-311/18, Rn. 130-133.

[5] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[6] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

[7] Siehe bspw. BayLDA, https://www.lda.bayern.de/de/thema_supplementary_measures.html.

delnder Verantwortlicher bzw. Auftragsverarbeiter vorgehen muss, um festzustellen, ob zur rechtmäßigen Übermittlung personenbezogener Daten in ein Land außerhalb der EU zusätzliche Maßnahmen ergriffen werden müssen, und wenn ja, welche zusätzlichen Maßnahmen angemessen sind. Die vom EDSA vorgegebene Prüfung ist sechsstufig.

**Schritt 1: Datenübermittlungen kennen**

Unternehmen müssen sich einen Überblick über ihre Datenübermittlungen in Drittländer verschaffen („Karte der Bestimmungsdrittländer").[8] Zu diesem Zweck kann bspw. auf ein gepflegtes Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO zurückgegriffen werden. In jedem Fall impliziert die „Know your Transfers"-Anforderung aus Schritt 1 keine über Art. 30 DSGVO hinausgehenden Dokumentationsanforderungen.

**Schritt 2: Auswahl eingesetzter Übermittlungsinstrumente**

Im nächsten Schritt muss der Datenexporteur prüfen, welches in Kapitel V der DSGVO aufgeführte Übermittlungsinstrument für den Drittstaatentransfer als Rechtsgrundlage zum Einsatz kommen soll. Diese Prüfung ist deswegen relevant, weil Übermittlungen auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission (Art. 45 DSGVO) oder eines Ausnahmetatbestandes (Art. 49 DSGVO) auch in Zukunft ohne zusätzliche Schutzmaßnahmen erfolgen können.[9]

Hierbei sollten Unternehmen allerdings beachten, dass der EDSA Art. 49 DSGVO als Ausnahmeregelung restriktiv auslegt und im Grunde nur für gelegentlich erfolgende bzw. sich nicht wiederholende Transfers akzeptiert.

Soll ein Übermittlungsinstrument gem. Art. 46 DSGVO genutzt werden (d.h. insbesondere SCC, BCR oder ad-hoc-Vertragsklauseln), greift die Pflicht, für ein „im Wesentlichen gleichwertiges Schutzniveau" sorgen zu müssen.

**Schritt 3: Beurteilung der Wirksamkeit des Übermittlungsinstruments**

Da die genannten Transferwerkzeuge vor allem vertragliche Garantien enthalten, muss der Datenexporteur nun prüfen, ob die Wirksamkeit des gewählten Instruments aus Art. 46 DSGVO im Kontext der vorgesehenen Übermittlung durch Rechtsvorschriften oder die Rechtspraxis des Drittlands beeinträchtigt wird. Dieser Schritt bildet mit Schritt 4 das „Herzstück" der vom EDSA skizzierten Prüfungsstruktur.

Eine Prüfung der gesamten ausländischen Rechtsordnung ist nicht zielführend. Vielmehr sind zunächst die für die jeweilige Drittlandsübermittlung einschlägigen Rechtsvorschriften korrekt zu ermitteln. In jedem Fall geprüft werden müssen diejenigen Normen der ausländischen Rechtsordnung, in denen die Voraussetzungen für eine Offenlegung personenbezogener Daten gegenüber staatlichen Stellen (z.B. für Zwecke der Strafverfolgung, zur Ausübung von Aufsichtsrechten oder für Zwecke der nationalen Sicherheit) geregelt sind. Sind keine derartigen Rechtsvorschriften vorhanden oder öffentlich zugänglich, müssen andere „relevante und objektive Umstände" berücksichtigt werden.

Ein angemessenes Schutzniveau im Sinne der DSGVO ist stets nur dann gewährleistet, wenn die einschlägigen Rechtsvorschriften im Drittland nicht über das hinausgehen, was in einer „demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt" (Prüfmaßstab).[10] Darüber hinaus muss Betroffenen ein wirksamer Rechtsbehelf im Drittland zur Verfügung stehen.

**Schritt 4: Zusätzliche Maßnahmen identifizieren**

Kommt der Datenexporteur zu dem Schluss, dass kein ausreichendes Schutzniveau besteht, müssen im vierten Schritt zusätzliche Maßnahmen identifiziert werden, um den Datentransfer dennoch rechtfertigen zu können.[11] Hierbei kommen grundsätzlich technische, organisatorische oder vertragliche Maßnahmen in Betracht, auch in Kombination miteinander. Allerdings sind vertragliche und organisatorische Maßnahmen laut EDSA „im Allgemeinen" nicht ausreichend, um unverhältnismäßige Zugriffsrechte staatlicher Stellen auf personenbezogene Daten im Drittland wirksam einzuschränken. In solchen Situationen muss folglich auf technische Schutzvorkehrungen zurückgegriffen werden.[12]

[8] EDPB Recommendations 01/2020, Rn. 8ff.
[9] EDPB Recommendations 01/2020, Rn. 14ff.
[10] Siehe auch Art. 23 DSGVO.
[11] EDPB Recommendations 01/2020, Rn. 45ff.
[12] EDPB Recommendations 01/2020, Rn. 48.

Bei der Bewertung der Wirksamkeit möglicher *supplementary measures* soll der Datenexporteur u.a. das Format der zu übermittelnden Daten, die Art der Daten, die Dauer und Komplexität der Datenverarbeitung sowie die Anzahl der beteiligten Akteure berücksichtigen. Gefordert ist folglich eine einzelfallbasierte Würdigung der Effektivität von zusätzlichen Maßnahmen im Lichte der konkreten Übermittlungskonstellation sowie der im dritten Schritt ermittelten Rechtsvorschriften des Ziellands.

### Schritt 5: Zusätzliche Maßnahmen umsetzen

Abhängig vom gewählten Übermittlungsinstrument (SCC, BCR, ad-hoc-Vertragsklauseln) sind im fünften Schritt weitere Punkte zu beachten. Bei der Verwendung von SCC darf nicht vergessen werden, dass die zusätzlich vereinbarten Maßnahmen weder direkt, noch indirekt die in den Musterverträgen niedergelegten Rechte und Verpflichtungen beschneiden.[13] Wie die Umsetzung für BCR und individuell vereinbarten Vertragsklauseln zu erfolgen hat, ist hingegen noch unklar.

### Schritt 6: Regelmäßige Neubewertung

Abschließend statuiert der EDSA eine Verpflichtung zur fortlaufenden Neubewertung der Lage im Drittland. Bei einer negativen Re-Evaluierung (zusätzliche Maßnahmen sind bspw. nicht mehr wirksam) müssen Datentransfers ggf. ausgesetzt oder beendet werden.

### Beispiele für zusätzliche Maßnahmen

In mehreren Beispielen („Use Cases")[14] geht der EDSA auf mögliche effektive Maßnahmen ein. Bei den vom EDSA präferierten technischen Maßnahmen steht die Verschlüsselung im Fokus, sowohl für data in transit als auch für *data at rest*. In diesem Zusammenhang macht der EDSA deutlich, dass für eine wirksame Verschlüsselung in jedem Fall der Verschlüsselungsalgorithmus und seine Parametrisierung dem Stand der Technik entsprechen, die Verschlüsselungsstärke an den Zeitraum der Speicherung angepasst und die zuverlässig verwalteten Schlüssel im Europäischen Wirtschaftsraum oder einem Drittland mit angemessenem Datenschutzniveau gespeichert werden müssen. Als ein Beispiel ohne wirksame Maßnahmen wird die Übermittlung an einen Cloud-Service-Anbieter genannt, der Zugang zu den unverschlüsselten personenbezogenen Daten benötigt, um die vertraglich vereinbarte Verarbeitungsleistung zu erbringen. Selbst eine Inhaltsverschlüsselung der Daten durch den Cloud-Service-Anbieter hält der EDSA für unzureichend, sofern der Cloud-Anbieter im Besitz der kryptographischen Schlüssel ist.

### Bewertung

Die EDSA-Handlungsempfehlungen sind ein wichtiger Schritt in die richtige Richtung. Denn sie geben Datenexporteuren in EU-weit abgestimmter Form eine erste Orientierung, wie die Imperative aus dem Schrems-II-Urteil in der Praxis umzusetzen sind. Klar ist bereits jetzt, dass der EDSA insgesamt eine strikte Position vertritt und dass damit in der Konsequenz viele EU-Unternehmen ihre Drittlandsübermittlungen anpassen oder einstellen müssen. Auch führende US-Technologiekonzerne haben den Ernst der Lage erkannt.

So kündigte Microsoft Ende 2020 als Reaktion auf das Schrems-II-Urteil sowie die EDSA-Empfehlungen an, Nutzer-Rechte über eine Ergänzung der Vertragsklauseln zu stärken. Auch wenn die Microsoft-Initiative von deutschen Datenschutzaufsichtsbehörden öffentlichkeitswirksam gelobt wurde, machten diese gleichzeitig deutlich, dass „die Transferproblematik in die USA nicht generell gelöst" und die vertraglichen Zusicherungen insofern nicht hinreichend seien.[15]

Für europäische Datenexporteure ergibt sich aus der EDSA-Position ein hoher Ressourcenaufwand. Das ausländische Rechtssystem muss in detail bewertet werden; dafür erforderlich sind Zugang zu Gesetzen, behördlicher Praxis und Rechtsprechung im Drittland sowie die Übersetzung von entsprechenden Dokumenten ins Deutsche oder Englische. EU-Exporteure müssen außerdem, wie vom EDSA vielfach betont, alle Abwägungen und Entscheidungen im Rahmen der sechsstufigen Prüfung gründlich dokumentieren, um ihrer Rechenschaftspflicht nachzukommen.

## EDSA-Empfehlungen zu wesentlichen europäischen Garantien hinsichtlich Überwachungsmaßnahmen

Die Empfehlungen des EDSA zu den wesentlichen

[13] EDPB Recommendations 01/2020, Rn. 56ff; siehe auch EG 109 DSGVO.

[14] EDPB Recommendations 01/2020, Rn. 69ff.

[15] BayLDA, https://www.lda.bayern.de/media/pm/pm2020_9.pdf.

europäischen Garantien in Bezug auf Überwachungsmaßnahmen (kurz „die Garantien") stellen eine Ergänzung der Empfehlungen zu zusätzlichen Schutzmaßnahmen dar. Ziel ist es, Datenexporteure bei der Beurteilung zu unterstützen, ob die in der Rechtsordnung eines Drittstaates verankerten Zugriffs- und Abhörrechte von nationalen Sicherheits- oder Strafverfolgungsbehörden einen zulässigen Eingriff in die Grundrechte auf Schutz der Privatsphäre und Schutz personenbezogener Daten darstellen oder ob europäische Standards nicht erfüllt werden können. Rechtsdogmatisch sind die identifizierten Garantien auf Stufe drei der vom EDSA aufgestellten Prüfstruktur (siehe oben) relevant. Sie ergeben sich aus einer Synthese von Rechtsprechung des EuGH[16] sowie des Europäischen Gerichtshofs für Menschenrechte[17].

Europäische Datenexporteure müssen prüfen:

- ob es eine transparente, öffentlich zugängliche gesetzliche Grundlage gibt, die Tragweite und Anwendung der betreffenden Überwachungsmaßnahmen hinreichend detailliert beschreibt, z.B. Definition der Personengruppen, die überwacht werden können, oder Angaben zur zeitlichen Begrenzung von Maßnahmen (Garantie A)
- ob die Überwachungsmaßnahmen verhältnismäßig sind, d.h. ob die Schwere des Eingriffs angemessen ist angesichts der Bedeutung des allgemeinen öffentlichen Interesses, das mit der Einschränkung verfolgt wird (Garantie B)
- ob ein unabhängiges Aufsichts- und Kontrollgremium existiert, das mit entsprechenden Machtbefugnissen, Kompetenzen und Ressourcen ausgestattet ist (Garantie C)
- ob betroffene Personen die Möglichkeit haben, vor einem unabhängigen Gericht oder einem gleichwertigen Organ ihre Rechte z.B. auf Zugang, Berichtigung oder Löschung durchzusetzen (Garantie D)

Der Rechtsrahmen im Drittland, der den Zugriff von Behörden auf Daten für Überwachungszwecke regelt, muss gegen diese vier Garantien im Rahmen einer Gesamtschau ausführlich geprüft werden. Aufgrund der vom EDSA selbst anerkannten Auslegungsbedürftigkeit der Garantien[18] ist der diesbezügliche Entscheidungsprozess eine wahre Mammutaufgabe.

## Entwürfe neuer Standardvertragsklauseln

### Ausgangslage

Als Folge des Schrems-II-Urteil wurden die SCC-alt, als am häufigsten verwendetes Instrument für internationale Datentransfers,[19] zwar nicht für ungültig erklärt,[20] allerdings wurde die Praxistauglichkeit der Musterverträge vehement in Frage gestellt. Doch bereits bevor der EuGH das Schicksal der SCC besiegelte, waren diese für den praktischen Rechtsanwender mit Vorsicht zu genießen.

Zum einen lag das schlicht am Alter der derzeit noch validen Kommissionsentscheidungen, welche gestützt auf die Datenschutzrichtlinie 95/46/EG erlassen wurden und demnach den Regelungsgehalt der DSGVO (v.a. von Art. 28 Abs. 3 DSGVO) nicht in Gänze abbilden.[21] Zum anderen resultieren erhebliche formale Probleme aus fehlenden SCC für komplexere Verarbeitungsketten, was sich derzeit nur mittels juristischer Kunstgriffe realisieren lässt.[22]

Am 12.11.2020 eröffnete die Kommission ein langersehntes Konsultationsverfahren, in welchem sowohl neue SCC für den Drittlandstransfer (gem. Art. 46 Abs. 2 lit. c DSGVO)[23] als auch für den innereuropäischen Datentransfer (gem. Art. 28 Abs. 7 DSGVO)[24] zur Bewertung bereitgestellt wurden. Die Rückmeldefrist endete zum 10.12.2020. EDSA und der Europäische Datenschutzbeauftragte (EDSB) wurden um Abgabe einer gemeinsamen Stellungnahme (joint opinion) gebeten, welche bzgl. beider Entwürfen zum 14.01.2021 publiziert wurde.[25]

### Methodik der SCC-neu

Waren die SCC-alt jeweils als Einzelverträge vorgesehen (ausgerichtet an der Verarbeitungssituation), wurde bzgl. der neuen SCC ein modularer Aufbau gewählt. Im Sinne einer „Werkzeugkiste" wurden alle denkbaren Verarbeitungskonstellationen in einem Vertragswerk zusammengefasst, welches hierbei je nach Anwendungsfall einen spezifischen

[16] Artikel 7, 8, 47 und 52 der Charta der Grundrechte der Europäischen Union.
[17] Artikel 8 der Europäischen Menschenrechtskonvention.
[18] EDPB Recommendations 02/2020, Rn. 49.
[19] Pressemitteilung der EU-Kommission vom 13.11.2020, https://ec.europa.eu/germany/news/20201113-datentransfers_de.
[20] Hierzu bereits Littger/Splittgerber/Schonhofen, BvD-News 3/2020, S. 24-27.
[21] Teilw. bereits unter BDSG-alt problematisch, siehe hierzu bspw. Düsseldorfer Kreis/DSK, Orientierungshilfe – Cloud Computing, Version 2 – Stand 09.10.2014, S. 16.
[22] Hierzu Düsseldorfer Kreis/DSK, Fallgruppen zur internationalen Auftragsdatenverarbeitung, 19.04.2007, S. 4,
[23] Ref. Ares(2020)6654686 - 12/11/2020.
[24] Ref. Ares(2020)6654429 - 12/11/2020.
[25] EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors & EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries.

Pflichtenkatalog in einzelnen Klauseln vorsieht.

Folgende Drittlandstransferszenarien lassen sich durch die SCC-neu nunmehr erfreulicherweise gem. Art 46 Abs. 2 lit. c DSGVO abbilden:

- **Modul 1:** Verantwortlicher <> Verantwortlicher
- **Modul 2:** Verantwortlicher <> Auftragsverarbeiter
- **Modul 3:** Auftragsverarbeiter <> Unterauftragsverarbeiter
- **Modul 4:** Auftragsverarbeiter <> Verantwortlicher

Eine Modernisierung der SCC ist insofern gelungen. Fortan können komplexe Verarbeitungsrealitäten formal besser abgedeckt werden.

### Inhaltliche Reaktion auf „Schrems II"

Um die seitens EuGH thematisierten Problemstellungen des Drittlandstransfers aufzugreifen, integrierte die Kommission in Abschnitt II zwei modulunabhängige Klauseln, die zukünftig von zentraler Bedeutung sein werden. In Klausel 2 findet sich eine Normierung des sog. „Transfer Impact Assessments" (TIA). Zudem reguliert Klausel 3 den Umgang mit behördlichen Auskunftsersuchen, die an den Datenimporteur adressiert werden. Wer hingegen gehofft hatte, die neuen SCC würden eine Übermittlung ohne zusätzliche Garantien (*supplementary measures*) ermöglichen, der wird leider enttäuscht. Sowohl Kommission[26] als auch EDSA und EDSB[27] verweisen explizit darauf, dass die SCC-neu weiterhin zusammen mit den EDSA-Empfehlungen (siehe oben) anzuwenden sind.

### Transfer Impact Assessment

Kern der als TIA bezeichneten Analyse stellt eine Bewertung des Risikos der jeweiligen Drittlandsrechtsordnung für den Vollzug der SCC dar. Hierbei zeigt sich jedoch in der Formulierung der Überschrift von Klausel 2 („*local laws affecting compliance with the clauses*") eine erste praktische Hürde bzgl. des Betrachtungshorizonts. Die Kommission schränkt im Entwurf die Pflicht zur Durchführung einer Risikobewertung explizit auf kodifizierte Gesetze ein. Darüber hinaus finden sich in der Entwurfsfassung keine ergänzenden Anforderungen für den praxisrelevanten Fall, dass in einem Drittland keine Gesetze über behördliche Datenzugriffsbefugnisse existieren oder einsehbar sind. Diese Unschärfe kritisieren EDSA/EDSB.[28] Eine Beschränkung des TIA auf „Gesetze" reduziert nach Rechtsauffassung der europ. Datenschützer nur unzureichend etwaige Gefahren für das Schutzniveau personenbezogener Daten. Für die Datenschutzpraxis erhärtet sich dadurch die antizipierte Befürchtung, sich intensiv mit dem Datenschutzniveau eines Drittlands in sämtlichen praktischen Ausprägungen auseinandersetzen zu müssen.

Der Kriterienkatalog zur Bewertung des konkreten Risikoniveaus findet sich in Klausel 2(b). Dem aktuellen SCC-Entwurfsstand zufolge sollten sich Verantwortliche mit folgenden Erwägungen der Risikosituation im Drittstaat nähern:

- Umstände der Drittlandsübermittlung,
- Gesetze des Drittlands,
- Etwaige zusätzliche Garantien.

Ein Unterschied in den Bewertungsansätzen von Kommission und EDSA/EDSB zeigt sich allerdings im Punkt der Analyse von Umständen der Datenübermittlung. Die Kommission möchte einschlägige praktische Erfahrungen oder bisherige behördliche Auskunftsersuchen zu Lasten des Datenimporteurs als subjektive Faktoren in die Risikoanalyse einfließen lassen. Dahingegen legen EDSA/EDSB, mit Verweis auf die Erwägungen des EuGH in „Schrems II", der Risikoanalyse ausschließlich objektive Faktoren zugrunde. Die bloße Tatsache, dass Daten in den Anwendungsbereich einer Drittlandsgesetzgebung ohne wesentliche Garantien fallen, führe bereits zu einer schlechteren Bewertung des Datenschutzniveaus. Auf die Wahrscheinlichkeit eines tatsächlichen Zugriffs kommt es also nicht mehr an.

Diesbezüglich empfehlen EDSA/EDSBA Konsistenz mit ihren Recommendations 01/2020 herzustellen.[29] Der finale Katalog bleibt abzuwarten. Via Klausel 2(d) müssen sich die SCC-Parteien letztlich dazu verpflichten, eine Dokumentation der vorgenommenen Bewertung vorzuhalten und diese auf Anforderung der zuständigen Datenschutzaufsichtsbehörde vorzulegen. Diese Pflicht geht EDSA/EDSB indes noch nicht weit genug. Basierend auf der Vermutung, dass die SCC-Parteien lediglich vereinbaren, ein TIA zu dokumentieren, ohne dies in der Praxis zu vollziehen, wurde der Kommission empfohlen[30] einen verpflichtenden Annex hierzu hinzuzufügen. Mithin sollen die Parteien vor Unterzeichnung der SCC-neu ein TIA dokumentieren und gleichermaßen als Vertragsbestandteil vorsehen.

### Bewertung

Die Formalisierung des Datenschutzes und der

[26] Ref. Ares(2020)6654686 - 12/11/2020, COMMISSION IMPLEMENTING DECISION, EG. 20.

[27] EDPB-EDPS Joint Opinion 2/2021, Rn. 21.

[28] EDPB-EDPS Joint Opinion 2/2021, Rn. 81.

[29] EDPB-EDPS Joint Opinion 2/2021, Rn. 86.

[30] EDPB-EDPS Joint Opinion 2/2021, Rn. 89.

Datenschutzpraxis in Unternehmen nimmt weiterhin signifikant zu. Allerdings dürften ernstzunehmende Risikoanalysen sowie die daraus abgeleiteten Bewertungsergebnisse ebenfalls das Potenzial haben, Entscheider dazu zu animieren, sich nach europäischen Alternativlösungen (falls verfügbar) umzuschauen.

Eine Komponente dürfen Unternehmen hinsichtlich ihrer Transferpraxis in keinem Fall aus den Augen verlieren. Die neuen SCC sind dazu gedacht bestehende Vorgängerversionen außer Kraft zu setzen, sodass die SCC-alt zeitnah ihre Gültigkeit verlieren. Diesbezüglich sieht die Kommission gnädigerweise eine Übergangsfrist von einem Jahr nach Inkrafttreten der SCC-neu vor. Danach sind ausschließlich letztere als valides Transferinstrument anzusehen.[31]

## Ausblick

In Anbetracht der jüngsten bzw. bevorstehenden regulatorischen Novellierungen im Zusammenhang mit Datentransfers in Länder ohne Angemessenheitsbeschluss (Art. 45 DSGVO) wird sich die Herangehensweise an eine Aufnahme von Vertragsbeziehungen mit Drittlandsunternehmen grundlegend ändern. De facto hat jeder Datenexporteur eigenverantwortlich, mittels des Instrumentes TIA, einen fallbezogenen „Angemessenheitsbeschluss-light" für sein konkretes Transferszenario zu schaffen. Diesen bisweilen ressourcenintensiven Dokumentationsprozessen dürften eher Großunternehmen als KMUs oder Mittelstand routiniert nachkommen können. Bleibt nur zu hoffen, dass letztere sich von Formalitäten nicht abschrecken lassen und nach wie vor internationale Wirtschaftsbeziehungen eingehen. In jedem Fall aber dürften die Kosten für Drittlandstransfers merklich zunehmen.

Zum einen wird hierfür die Implementierung von *supplementary measures*, v.a. von technischen Schutzmaßnahmen wie bspw. Verschlüsselungsmechanismen, ursächlich sein. Zum anderen bedingt eine Erstellung von Risikoanalysen und die Untersuchung von Drittlandsrechtsordnungen eine erhebliche Bindung personeller Ressourcen; falls dafür nicht sogar externes Experten-Know-How eingekauft werden muss. Sollte dieser formale Kraftakt dennoch gelingen, haftet dem Drittlandsdatentransfer trotz allem ein gewisses Maß an Rechtsunsicherheit an. Sowohl *supplementary measures* als auch die Bewertung der Drittlandsrechtsordnung sind das Ergebnis einer subjektiven Würdigung und Neuland für viele Marktteilnehmer. Ein Funke Hoffnung könnte der Arbeit von Wirtschafts-/Interessenverbänden entspringen, welche bspw. Einschätzungen zu Drittstaaten oder zumindest Orientierungshilfen zur Verfügung stellen könnten. Hingegen sollte nicht darauf gewartet werden, dass Datenschutzaufsichtsbehörden ergänzende Hilfestellungen bereitstellen, ganz im Gegenteil, Mitte Februar kursierte bereits Berichterstattung bzgl. behördlicher Kontrolle in Sachen Drittlandsdatentransfers.[32] Trotz der vorstehend geäußerten Bedenken darf indes auch nicht unterschätzt werden, dass der Kommission durch die Erweiterung des Anwendungsbereichs der SCC-neu hinsichtlich alternativer Verarbeitungskonstellationen eine deutliche Erleichterung in der praktischen Handhabung gelungen ist.

## Über die Autoren

**Dr. iur. Tilman M. Dralle, LL.M.**
ist Senior Data Governance, Privacy & Compliance Manager bei der 1&1 IONOS SE sowie Lehrbeauftragter für Datenschutzrecht an der TU Dresden.

**Jonathan Schröer, LL.M**
ist Group Legal Privacy Manager bei der United Internet Corporate Services GmbH. In dieser Rolle berät er Unternehmen der United Internet-Gruppe in strategischen und operativen Belangen des Datenschutzes.

**Dipl.-Wi.-Ing. Dominik Smasal, DSB-TÜV**
ist Experte für Datenschutz bei der 1&1 IONOS SE. Als fachliche Führungskraft mit Vergangenheit in der Leitung internationaler Software-Projekte berät er das IONOS Management und sorgt für die effektive, zielgerichtete Ausrichtung der Datenschutz-Organisation im Vorstandsbereich Technik & Entwicklung.

▶ https://www.ionos.de/

▶ https://www.united-internet.de/


[31] Ref. Ares(2020)6654686 - 12/11/2020, COMMISSION IMPLEMENTING DECISION, EG. 24.
[32] Siehe hierzu: https://www.golem.de/news/datenschutz-task-force-will-nutzung-von-us-clouddiensten-pruefen-2102-154206.html.

# PRIVACY SHIELD – DER VORHANG ZU UND ALLE FRAGEN OFFEN?

Prof. Dr. Tobias Straub

*Nach der Schrems-II-Entscheidung des EuGH können Verantwortliche Übermittlungen personenbezogener Daten in die USA nicht mehr auf einen Angemessenheitsbeschluss stützen. Unter den alternativen Transfer-Instrumenten bieten sich vor allem die Standarddatenschutzklauseln an, doch auch sie sind mit Unwägbarkeiten behaftet, wie dieser Beitrag darstellt.*

Seit der Entscheidung des EuGH im Juli vergangenen Jahres ist nun etwas Zeit vergangen, während der Fachwelt, Verantwortliche und Aufsichtsbehörden das Urteil und dessen Implikationen diskutieren konnten.[1] Auf die einschlägigen Verpflichtungen der Verantwortlichen, insbesondere zu Dokumentation, Überprüfung sowie nötigenfalls Anpassung oder Aussetzung von Übermittlungen personenbezogener Daten in Drittstaaten wurde schon vielfach hingewiesen.[2] Dieser Beitrag betrachtet den Mechanismus der Standarddatenschutzklauseln mit zusätzlichen Maßnahmen, speziell solcher technischer Natur, als Ersatz für den entfallenden Privacy Shield und setzt sich dazu mit den Empfehlungen des Europäischen Datenschutzausschusses (EDSA) auseinander.

## Typische Anwendungsfälle

Das Gros der Datentransfers von der EU in Drittstaaten (also in Länder außerhalb der EU und des Europäischen Wirtschaftsraums) geht in Richtung USA und dort zu Anbietern standardisierter Cloud-Dienste, die im Abonnement bezogen werden.

Zu *Software-as-a-Service* gehören etwa webbasierte Office- und Kollaborations-Anwendungen, Werkzeuge zur Vertriebsunterstützung oder für den Kundensupport. Organisationen nutzen für die Bereitstellung eigener Dienste auch regelmäßig virtuelle Speicher- und Computing-Plattformen als *Infrastructure-as-a-Service*, um selbst keine entsprechende Hardware vorhalten und

[1] Zum Urteil und ersten Handlungsempfehlungen siehe etwa Littger/Splittgerber/Schonhofen, BvD News 3/2020, S. 24 ff.

[2] Dralle/Schröer/Smasal gehen in dieser Ausgabe auf die vom Europäischen Datenschutzausschuss hierzu vorgeschlagene Vorgehensweise näher ein.

administrieren zu müssen. Zu Übermittlungen personenbezogener Daten kann es ferner durch *Telemetriefunktionen* oder im Rahmen von *Fernwartungszugriffen* oder *Supportanfragen* kommen.

Rechtlich handelt es sich in den vorgenannten Fällen üblicherweise um Datenverarbeitung im Auftrag, die den Vorgaben von Art. 28 DSGVO unterliegt, aber Konstellationen einer gemeinsamen Verantwortung[3] gem. Art 26 DSGVO sind ebenso denkbar.

Die Zulässigkeit der Verarbeitung, insbesondere der Übermittlung, ist anhand der üblichen Anforderungen der DSGVO sowie zusätzlich speziell der für Drittstaatentransfers maßgeblichen Regelungen in Kapitel V zu bewerten (zweistufige Prüfung), wobei insbesondere darauf zu achten ist, dass es zu keiner Absenkung des durch die DSGVO gewährleisteten Schutzniveaus kommt (Art. 44 Satz 2). Es darf nicht übersehen werden, dass ein Drittstaatenbezug auch häufig indirekt dadurch entsteht, dass ein Verantwortlicher zwar einen Auftragsverarbeiter in der EU beauftragt, dieser jedoch für die Bereitstellung seines Dienstes wiederum auf Unter-Auftragnehmer in den USA zurückgreift. Sofern es dabei zu Übermittlungen personenbezogener Daten kommt, ist diese Verarbeitung ebenfalls dem Verantwortlichen zuzurechnen.

## Alternativen zum Privacy Shield

Datentransfers in die USA sind, anders als teilweise wahrgenommen, mit dem Aus des Privacy Shield nicht grundsätzlich unzulässig geworden, denn neben dem Angemessenheitsbeschluss gem. Art. 45 Abs. 3 sieht die DSGVO ja noch eine ganze Reihe weiterer Möglichkeiten für Übermittlungen in Drittstaaten vor.[4] Allerdings darf die vermeintlich große Auswahl der Transferinstrumente und Ausnahmen gem. Art. 46 bzw. 49 DSGVO (bei denen zum Teil die Aufsichtsbehörde einzubinden ist) nicht darüber hinwegtäuschen, dass unter praktischen Gesichtspunkten primär der Mechanismus der Standarddatenschutzklauseln gem. Art. 46 Abs. 2 lit. c (SCC )[5] eine breite Anwendbarkeit verspricht. Insbesondere sind die in Art. 49 genannten Tatbestände für bestimmte – und eng auszulegende – Ausnahmen keine Basis für dauerhafte und über Einzelfälle hinausgehende Übermittlungen.[6]

Ohne Vorliegen eines Angemessenheitsbeschlusses dürfen personenbezogene Daten in ein Drittland nur dann übermittelt werden, wenn der Exporteur geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 46 Abs. 1).

Der EuGH hat die SCC in seiner Entscheidung nicht wie den Privacy Shield für grundsätzlich ungültig erklärt, jedoch betont, dass durch die SCC ein der Sache nach gleichwertiges Schutzniveau für personenbezogene Daten sichergestellt sein muss. Eine Prüfung, ob dieses Ziel erreicht wird, ist vom Datenexporteur im Einzelfall vorzunehmen, wobei insbesondere die vertraglichen Regelungen mit dem Datenimporteur sowie die maßgeblichen Elemente der Rechtsordnung (entsprechend Art. 45 Abs. 2) des Drittlandes im Hinblick auf etwaige behördliche Zugriffe zu berücksichtigen sind. Erkennbar haben Verantwortliche also einen nicht unerheblichen Aufwand bei der Prüfung, ob ein angemessenes Schutzniveau vorliegt, zu betreiben.[7]

## SCC+

Früh schon wurde, etwa durch den baden-württembergischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI), darauf hingewiesen, dass die SCC als zweiseitiger Vertrag zwischen Datenexporteur und -importeur die Behörden im Drittland nicht binden können und – sofern diese über entsprechende Eingriffsbefugnisse verfügen – die SCC *alleine* daher kein ausreichendes Schutzniveau gewährleisten.[8]

Der LfDI sieht im Fall des Drittlandes USA die SCC ohne zusätzliche Garantien als „nur in seltenen Fällen" ausreichend an (ohne allerdings Beispiele für solche besonderen Konstellationen zu nennen).[9] Gemeinhin werden daher die Standarddatenschutzklauseln in Kombination mit zusätzlichen Garantien („SCC+") als die erfolgversprechendste Variante für eine Fortsetzung von Datentransfers in die USA gesehen. Die EU-Kommission unterstützt diesen Weg mit dem jüngsten Entwurf überarbeiteter und modular aufgebauter SCC.[10] Jedoch kann nicht davon ausgegangen werden, dass bei Verwendung der neuen SCC gänzlich auf zusätzliche Maßnahmen verzichtet werden kann.[11]

[3] Eine solche hat der EuGH in seiner Entscheidung vom 5. Juni 2018 – C-210/16 für die Betreiber einer so genannten Fanpage auf Facebook bejaht.
[4] Für eine Übersicht siehe etwa Straub, DuD 3/2021, S. 198.
[5] Die Abkürzung spiegelt die noch aus der Datenschutz-Richtlinie 95/46/EG stammenden Bezeichnung „standard contractual clauses" wider.
[6] EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 (https://EDSA.europa.eu/sites/EDSA/files/files/file1/EDSA_guidelines_2_2018_derogations_de.pdf).
[7] Vgl. dazu Dralle/Schröer/Smasal, a.a.O.
[8] LfDI, Orientierungshilfe Schrems II (https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfe-des-lfdi-bw-was-jetzt-in-sachen-internationaler-datentransfer/).
[9] Deutlicher noch Golland, NJW 2020, S. 2593 f., der Datentransfers allein auf Basis der SCC als unmöglich ansieht.
[10] Siehe dazu ausführlich Dralle/Schröer/Smasal, a.a.O.
[11] EDSA und Europäischer Datenschutzbeauftragter, Joint Opinion 2/2021. (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf).

### Maßnahmenkatalog des EDSA

Nachdem der EuGH selbst auf eine Konkretisierung möglicher zusätzlicher Maßnahmen verzichtet hatte, hat der EDSA in seinen Empfehlungen[12] nun dargelegt, welcher Natur diese sein können und auch gleich eine längere Liste von Beispielen und Anwendungsfällen gegeben. Unterschieden werden dabei

- *vertragliche Maßnahmen* (z.B. eine Verpflichtung des Datenimporteurs, sich gegen behördliche Anordnungen zur Offenlegung von Daten zu wehren),
- *organisatorische Maßnahmen* (z.B. Dokumentation behördlicher Zugriffsersuchen und deren Beantwortung) sowie
- *technische Maßnahmen* (auf die unten im Detail eingegangen wird).

Der EDSA sieht seine Liste nicht als erschöpfend oder verpflichtend an, so dass den Vertragsparteien eine gewisse Entscheidungsfreiheit bleibt, geeignete Maßnahmen der drei Kategorien zu kombinieren, um damit das Ziel eines angemessenen Schutzniveaus zu erreichen.

Lediglich eine vertragliche Klausel, in der der Datenimporteur bestätigt, nicht absichtlich Hintertüren in seine Software eingebaut oder seine Prozesse geschwächt zu haben und nach dem Recht des Drittlandes auch nicht dazu oder zur Zugänglichmachung von personenbezogenen Daten oder Verschlüsselungsschlüsseln verpflichtet ist, sollte laut EDSA „in der Regel erforderlich sein".

Diese Maßnahme ist daher Verantwortlichen anzuraten, gerade auch weil Datenimporteuren, die die Aussagen wahrheitsgemäß bestätigen können, dadurch kein Zusatzaufwand für die Anpassung von Software oder Prozessen entsteht.

### Kriterien für die Auswahl

Die Umsetzung einer oder mehrerer der genannten Maßnahmen genügt aber nicht schon per se, um das geforderte angemessene Schutzniveau zu gewährleisten. Vielmehr muss die Auswahl derart getroffen werden, dass die aufgrund der Rechtslage im Drittland bestehenden Rechtsschutzlücken tatsächlich effektiv geschlossen werden.[13]

Der EDSA gibt exemplarisch einige Merkmale an, die für die Beurteilung der Geeignetheit zusätzlicher Maßnahmen herangezogen werden können:

- *Art der Daten*
- und deren *Format* (womit die Unterscheidung zwischen Daten im Klartext, in pseudonymisierter oder verschlüsselter Form gemeint ist),
- *Dauer und Komplexität* der Verarbeitung, auch im Hinblick auf die beteiligten Akteure
- sowie die Möglichkeit der Weiterübermittlung (*onward transfer*).

Wer angesichts der großen Zahl der vom EDSA zusammengestellten Vorschläge darauf gehofft hatte, dass sich daraus stets relativ leicht zusätzliche Maßnahmen auswählen und umsetzen lassen, muss jedoch enttäuscht werden: Nach Auffassung des EDSA genügen nämlich vertragliche und organisatorische Maßnahmen im Allgemeinen nicht, Zugriffen staatlicher Stellen zu Überwachungszwecken entgegenzuwirken. Es gebe Situationen, in denen nur technische Maßnahmen helfen könnten, wenngleich flankierende vertragliche und organisatorische Maßnahmen dabei zumindest das Schutzniveau insgesamt stärken könnten.[14]

## Technische Maßnahmen

Insofern lohnt es sich also, den Blick auf die technischen Maßnahmen zu richten, die von den Aufsichtsbehörden ins Spiel gebracht wurden:[15]

### Verschlüsselung

An erster Stelle der technischen Maßnahmen ist dabei Verschlüsselung (nach dem Stand der Technik und unter Nutzung zuverlässiger Software) zu nennen. Werden Daten bei einem Importeur in einem Drittland ohne angemessenes Datenschutzniveau gespeichert, so können behördliche Zugriffe dadurch verhindert werden, dass *vor dem Datentransfer verschlüsselt* wird. Wichtig dabei ist, dass die Schlüssel dem Datenimporteur nicht zugänglich sein dürfen, sondern unter der alleinigen Kontrolle des Datenexporteurs (oder eines Beauftragten innerhalb des EWR oder eines sicheren Drittlandes) verbleiben. Diese Anforderung schließt also explizit durch den Datenimporteur erzeugte oder verwaltete Schlüssel aus. Eine *Transportverschlüsselung* zwischen Exporteur und Importeur wird dagegen nur in den beiden

[12] EDSA, Recommendations 01/2020 (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf).

[13] EDSA, a.a.O., Rn. 69.

[14] EDSA, a.a.O., Rn. 48.

[15] LfDI, a.a.O. und EDSA, a.a.O.

Fällen als ausreichend angesehen, in denen der Importeur nach dem Recht des Drittlandes besonderen (etwa berufsständischen) Schutz genießt bzw. es zu einer bloßen Durchleitung der personenbezogenen Daten durch ein unsicheres Drittland kommt (auf dem Weg zu einem Importeur, der sich selbst in einem Land mit angemessenem Schutzniveau befindet).

Ein Cloud-Backup, bei dem es zu einer reinen Datenspeicherung beim Anbieter kommt, lässt sich unter der Bedingung, dass dieser keinen Zugriff auf das Schlüsselmaterial hat, noch gut realisieren.[16] Beim überwiegenden Teil der Anwendungsfälle in der Praxis benötigen Anbieter aber *personenbezogene Daten im Klartext*, um Cloud-Dienste oder Dienstleistungen (etwa im Rahmen konzerninterner Aufgabenteilung) zu erbringen.

Sofern in diesem Zusammenhang Verschlüsselung genutzt wird (für data at rest, um etwa dem Diebstahl von Speichermedien vorzubeugen), geschieht dies in einer Weise, die den Zugriff des Anbieters ermöglicht, so dass dessen Administratoren prinzipiell eine Entschlüsselung vornehmen können.

**Pseudonymisierung und Anonymisierung**

Eine vor dem Datentransfer vorgenommene Pseudonymisierung kann in manchen Anwendungsfällen durchaus praktikabel sein, zum Beispiel im Bereich der Forschung und Statistik oder bei Diensten, bei denen keine namentlichen Benutzerkennungen vorausgesetzt werden und auch sonst keine personenbezogenen Daten anfallen. Dabei hat bereits der Datenexporteur die Pseudonymisierung vorzunehmen und die zusätzlichen, der Identifizierung dienenden Informationen bei sich (oder zumindest außerhalb des Drittlandes des Datenimporteurs) zu behalten.

Zur Bewertung der Wirksamkeit der Pseudonymisierung ist auch das Risiko einer Re-Identifizierung von Zielpersonen durch Behörden des Drittlandes zu berücksichtigen, die möglicherweise nicht nur Zugriff auf Daten beim Datenimporteur selbst, sondern auch bei anderen Stellen erhalten und beide Quellen verknüpfen könnten.[17]

Leider ist schwer vorstellbar, wie sich etwa webbasierte Kollaborationswerkzeuge in einem Unternehmen auf vollständig pseudonyme und gleichzeitig benutzerfreundliche Weise nutzen lassen.

Das Vorgenannte gilt analog für den Fall, dass der Datenexporteur eine Anonymisierung vornimmt und – unter der Voraussetzung ihrer Wirksamkeit – somit den Anwendungsbereich der DSGVO verlässt und die Transferproblematik dadurch gänzlich umschifft.

**Nutzung mehrerer Anbieter**

Der EDSA bringt ferner die Möglichkeit ins Spiel, die Datenverarbeitung auf zwei oder mehrere Anbieter aufzuteilen, so dass jeder für sich alleine keine Informationen über die verarbeiteten personenbezogenen Daten erhält. Im Zuge der Forschung zu so genannter Secure *Multi-Party Computation* (MPC )[18] wurde eine Reihe leistungsfähiger kryptographischer Techniken für verteilte Berechnungen zwischen sich untereinander nicht vertrauenden Stellen entwickelt, deren Sicherheitseigenschaften sich selbst unter der Annahme, dass ein gewisser Teil der Beteiligten „angegriffen" wird und von dem vorgesehenen Protokoll abweicht, beweisen lassen.

Für die Anwendung im Kontext eines Datentransfers bedeutet dies, dass nicht alle beteiligten Anbieter im selben Land ansässig sein dürfen. Ansonsten wäre es den Behörden dieses Landes möglich, die einzelnen Anteile zusammenzufügen und somit die personenbezogenen Daten zu rekonstruieren.

MPC hat bereits in Softwareprodukte Eingang gefunden und die Anwendbarkeit etwa für statistische Auswertungen oder den Schutz kryptographischer Schlüssel gezeigt. Die Anforderung, dass in dieser Konstellation nun gleich mehrere Anbieter, zudem in unterschiedlichen Ländern, einzusetzen sind, erhöht aber die Komplexität für Verantwortliche.

**Problematik Meta-Daten**

Aus den Ausführungen ergibt sich, dass es also prinzipiell möglich ist, die SCC so durch technische Maßnahmen zu ergänzen, dass Zugriffe von Behörden im Drittland tatsächlich wirksam verhindert werden. Allerdings dürften diese Maßnahmen, gerade in den eingangs genannten Anwendungsfällen, häufig als nicht praktikabel empfunden werden. Hinzu kommt, dass ja nicht nur die eigentlichen Inhalts-, sondern eben auch Rahmendaten (wie z.B. IP-Adressen, Geräte-/ Browser-Kennungen, Beziehungen zwischen Nut-

[16] Das deutlich weitergehende Konzept der homomorphen Verschlüsselung erlaubt es, zumindest elementare Rechenoperationen direkt auf verschlüsselten Daten vorzunehmen, ist aber aufgrund der Limitationen und des erforderlichen Zusatzaufwands momentan nicht für eine breitere Anwendung geeignet.
[17] EDSA, a.a.O., Rn. 81 ff.
[18] Für eine Einführung siehe Lindell, Commun. ACM, 1/2021, S. 86 ff.

zenden) einen Personenbezug aufweisen können, letztere sich aber schwerlich schützen lassen. Entsprechend pessimistisch äußerte sich in dieser Hinsicht auch die Datenschutzkonferenz in Bezug auf Videokonferenzsysteme, da bestimmte Rahmendaten einem Anbieter aus technischen Gründen zugänglich sein müssen.[19]

## Wir stehen selbst enttäuscht und sehn betroffen …

Da Cloud-Anbieter, die sich bisher auf den Privacy Shield stützten, ihren Kunden vielfach den Umstieg auf SCC angeboten haben, sind abrupte Unterbrechungen im internationalen Datenverkehr bislang ausgeblieben. Der EuGH hat auf die Pflicht der Aufsichtsbehörden hingewiesen, Drittstaatentransfers zu untersagen, wenn dabei das von der DSGVO geforderte Schutzniveau nicht gewährleistet wird. Zwar üben sich die Aufsichtsbehörden – verständlich in Anbetracht der komplexen Aufgabe der Datenexporteure – noch in Zurückhaltung im Vollzug, fordern aber zum Teil bereits pauschal die Abkehr von Dienstleistern in den USA[20] oder drohen Untersagungen zumindest für Transfers, deren „Alternativlosigkeit" Datenexporteure nicht belegen können, an.[21]

Das Instrument SCC+ ist treffend als ein unter dem „Damoklesschwert einer Intervention der Aufsicht" stehendes „Experiment" bezeichnet worden.[22] Dies muss insbesondere auch deshalb gelten, als dass sich in vielen Fällen keine wirksamen und praktikabel umzusetzenden technischen Maßnahmen erkennen lassen. Erste von Datenimporteuren vorgeschlagene vertragliche Ergänzungen der SCC sind ebenso deutlich kritisiert worden wie die Empfehlungen des EDSA an sich.[23]

Man kann den Aufsichtsbehörden nicht vorwerfen, dass sie in den zurückliegenden Monaten tatenlos geblieben wären, sind doch eine ganze Reihe von Handreichungen entstanden. Allerdings werden nun zusehends die Grenzen deutlich, die der EuGH mit dem Schrems-II-Urteil gezogen hat. Es wurde schon vorgeschlagen,[24] das – der DSGVO ja durchaus nicht fremde – Konzept des risikobasierten Ansatzes auf Drittstaatentransfers anzuwenden, um zumindest Übermittlungen unter schwächeren Schutzmaßnahmen zu ermöglichen, wenn Risiken für die betroffenen Personen nicht hoch erscheinen. So „elegant" ein solcher Ansatz in manchen Augen sein mag, um damit zumindest einen Teil der Datentransfers fortsetzen zu können, so fraglich ist es, ob die dahinterstehende Lesart des Urteils statthaft ist.

Im Ergebnis dürften sich Verantwortliche, die an ihren bestehenden Übermittlungen festhalten wollen, damit aktuell wohl an Brechts bekannte Verse erinnert fühlen.

> *Der einzige Ausweg wär aus diesem Ungemach:*
> *Sie selber dächten auf der Stelle nach.*

Anders als der Privacy Shield verlangt das Instrument SCC, was auch EuGH und Aufsichtsbehörden nachdrücklich betonen, dem Datenexporteur weitaus mehr Eigenverantwortung ab. So sehr man es sich wünschen mag: Ob die nicht unerheblichen Mühen der Datenexporteure bei der Überprüfung und Anpassung ihrer Transfers und der dabei gezeigte gute Wille ausreichend sein werden oder es nicht vielmehr veränderte Randbedingungen (hinsichtlich der Rechtslage in den USA oder der Etablierung von Clouds mit EU-Datentreuhand[25]) braucht, um zu mit dem Urteil konformen und praktikablen Lösungen zu kommen, muss sich erst noch weisen.

> *Verehrtes Publikum, los, such dir selbst den Schluss!*
> *Es muss ein guter da sein, muss, muss, muss!*

[19] Datenschutzkonferenz, Orientierungshilfe Videokonferenzsysteme (https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-videokonferenzsysteme_final.pdf).
[20] Berliner Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung vom 17.07.2020 (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf).
[21] Brink, BvD-News 3/2020, S. 50.
[22] Golland, NJW 2020, S. 2596.
[23] CR-online.de Blog (https://www.cr-online.de/blog/2020/11/12/steine-statt-brot-empfehlungen-des-edsa-zu-datentransfers-nach-schrems-ii/, https://www.cr-online.de/blog/2020/11/12/steine-statt-brot-empfehlungen-des-edsa-zu-datentransfers-nach-schrems-ii/).
[24] Etwa vom Bitkom und anderen Verbänden (https://www.bitkom.org/sites/default/files/2020-09/verbandepapier-zu-privacy-shield.pdf). Jungkind/Raspé/Schramm, NZG 2020, S. 1056, schlagen für den Fall konzerninterner Datentransfers ein an der DSFA orientiertes Vorgehen vor.
[25] Etwa in der Art des Modells, wie es Microsoft und die Deutsche Telekom eine Zeitlang angeboten haben (siehe dazu https://heise.de/-4152650).


Über den Autor

**Dr. Tobias Straub**
ist Professor für Wirtschaftsinformatik an der Dualen Hochschule Baden-Württemberg in Stuttgart sowie behördlicher Datenschutzbeauftragter.

▶ tobias.straub@dhbw-stuttgart.de

Anzeige

# Steckt auch in Ihnen die **Service-DNA**?

**Dann verbinden Sie sich jetzt mit dem größten Service-Netzwerk Europas*:**

Werden Sie Mitglied im Service-Verband KVD e. V. und profitieren Sie neben dem professionellen Netzwerk mit den Verbindungen in Praxis, Forschung und Politik auch von der internationalen Zusammenarbeit des KVD, zum Beispiel mit dem österreichischen Verband KVA und dem Schweizer Pendant, dem SKDV.

Informieren Sie sich jetzt unter **www.kvd.de**.

* Der KVD gilt mit seinen 1.600 Mitgliedern als größtes verbandliches Service-Netzwerk seiner Art in Europa. Er unterstützt Fach- und Führungskräfte bei der Gestaltung ihres technischen Kundendienstes. Über Netzwerkveranstaltungen, Aus- und Weiterbildungen sowie die Einbindung neuester Forschungsergebnisse erhalten Mitglieder einen entscheidenden Wissens- und damit Marktvorsprung.

# DAS GESCHÄFTSGEHEIMNISGESETZ

## Von Compliance und konkreten Maßnahmen bis zur Durchsetzung von Ansprüchen

Regina Mühlich, Dr. Jens Eckhardt

**Lange Zeit regelte das Gesetz gegen unlauteren Wettbewerb (konkret §§ 17 ff. UWG) in Deutschland den Schutz von Betriebs- und Geschäftsgeheimnissen. Am 26.04.2019 ist das Geschäftsgeheimnisgesetz (GeschGehG) in Kraft getreten. Seitdem hat sich für Unternehmen vieles verändert.**

Das GeschGehG und damit eine komplett neue Herangehensweise ist die Antwort auf ein sich laufend veränderndes Umfeld. Die Strafvorschriften haben sich verschärft. Gerichte gehen härter gegen Wirtschaftskriminalität vor. Dies ist auch dem Umstand geschuldet, dass Medien und die Öffentlichkeit beispielsweise von Korruption und Vorteilsnahme viel stärker Notiz nehmen als noch vor ein paar Jahren.

### Richtlinien werden zu nationalem Recht

Bereits am 08.06.2016 verabschiedeten das Europäische Parlament und der Europäische Rat die Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen, sprich Geschäftsgeheimnisse, vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Im Gegensatz zur Datenschutz-Grundverordnung (DSGVO), welche unmittelbar und direkt gilt, waren die Mitgliedsstatten der Europäischen Union verpflichtet, die Regelungen in nationales Recht umzusetzen. Was auch geschah. Doch mit welchen Überlegungen und Herausforderungen haben die Unternehmen seitdem zu tun?

### Compliance – neu oder nur alter Wein in neuen Schläuchen?

„Verhalten im Einklang mit geltendem Recht" – das ist eine der gängigen Beschreibungen von Compliance. Compliance bedeutet allerdings mehr, nämlich den Grad der Einhaltung von Regeln (Regelkonformität). Wer „compliant" (engl. für übereinstimmend) ist, hält sich nicht nur an Recht, Gesetz und Ordnung, sondern idealerweise auch an die Leitlinien und das Wertesystem der eigenen Organisation.

Der Begriff Compliance ist noch relativ jung in seiner Verwendung für die Rechtstreue von Unternehmen und Betrieben. Eine Selbstverständlichkeit ist es allerdings, dass Unternehmen Gesetze einhalten müssen. Vorstände und Geschäftsführer haben die Sorgfalt eines ordnungsgemäßen Geschäftsleiters anzuwenden (§ 93 Abs. 1 AktG; § 43 Abs. 1 GmbHG). Dies bedeutet nichts anderes, als dass sie dafür Sorge tragen müssen, dass das Unternehmen die geltenden Gesetze befolgt.

Also doch nur alter Wein in neuen Schläuchen? Die erwähnten Paragraphen des Aktiengesetzes

(AktG) und dem Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) sind schließlich nicht neu. Zumindest nicht ganz neu. Neu ist die Herangehensweise, die Aufgabe „compliant" zu werden und zu sein. Es bedarf eines „Managementsystems" – vor allem vor dem Hintergrund der sich ändernden Gesetze, wie beispielsweise im Datenschutzrecht mit der DSGVO im Mai 2018 oder eben das neue GeschGehG im April 2019. Die rechtlichen Risiken nehmen also zu durch

- dynamische Änderung des regulatorischen Umfelds auf internationaler und nationaler Ebene
- extra-territoriale Wirkung ausländischer Normen (z.B. FCPA, UK Bribery Act, Loi Sapin II)
- Ausweitung der Haftung von Unternehmen und Geschäftsleiter durch Gesetzgeber, Gerichte und Behörden

Waren Buffet sagte: „It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." Ein Auf- und Ausbau eines Compliance-Systems ist für Unternehmen heute unerlässlich – um Risiken zu erkennen, zu minimieren und um vorzubeugen.

## Unternehmerisches Handeln ist stets mit Risiken verbunden

Ob neue Produkte erfolgreich am Markt bestehen können, ob sich Investitionsentscheidungen letztlich auszahlen oder wie sich externe Rahmenbedingungen entwickeln, vieles hängt von einer bewussten Inkaufnahme bestimmter Risiken durch die Unternehmensleitung ab, ohne die erfolgreiches Wirtschaften nicht möglich wäre. Im Compliance geht es aber um viel mehr als „nur" um die Einhaltung von Gesetzen, die Minimierung von Risiken und die Vermeidung von Gesetzesverstößen. Sie beinhaltet neben verpflichtenden Regeln auch solche, denen sich eine Unternehmung freiwillig unterwirft, wie ISO-Standards, Verhaltensregeln oder Verhaltenskodizes (Codes of Conduct).

## Das Geschäftsgeheimnis in der Praxis

In § 1 Abs. 1 GeschGehG heißt es: „Dieses Gesetz dient dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung." Um die Definition des Geschäftsgeheimnisses zu erfüllen, müssen (alle) vier Voraussetzungen vorliegen. Gemäß § 2 Nr. 1 GeschGehG ist ein Geschäftsgeheimnis

1. eine Information, die weder insgesamt noch in genauer Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich ist und daher
2. von wirtschaftlichem Wert ist und
3. Gegenstand von – den Umständen nach angemessenen – Geheimhaltungsmaßnahmen durch den rechtmäßigen Inhaber ist und
4. bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Das Geschäftsgeheimnis beinhaltet die Vorgänge innerhalb eines Unternehmens, die nicht der Öffentlichkeit zugänglich gemacht werden sollen. Diese sind nur bestimmten Mitarbeitern innerhalb eines Unternehmens bekannt und unterliegen der absoluten Verschwiegenheitspflicht. Der Inhaber eines Betriebes hat an diesen Sachverhalten den Willen zur Geheimhaltung und dieser beruht auf einem wirtschaftlichen Interesse, das als besonders schutzwürdig deklariert ist.

Im Vergleich zur bisherigen Rechtslage in Deutschland gelten dabei teilweise strengere Anforderungen an das Vorliegen eines Geschäftsgeheimnisses. So müssen Unternehmen zum Beispiel angemessene Geheimhaltungsmaßnahmen treffen, um von dem Schutz durch das Gesetz profitieren zu können. Die Einordnung als Geschäftsgeheimnis steht der Tätigkeit von Journalisten und Hinweisgebern jedoch nicht entgegen. Denn die Ausnahmeregelungen für Journalisten und Hinweisgeber gelten für sämtliche Geschäftsgeheimnisse. Beispiele sind:

- Angebote, Preiskalkulationen, Verhandlungstaktiken und Ausschreibungsunterlagen
- Rezepte, Stoffzusammensetzungen, Materialbeschaffenheit und Beistoffe
- Buchführungsunterlagen, Abschlüsse, Budgets und (unveröffentlichte) Bilanzen
- Computerprogramme, Software und Tools sowie Erfahrungen mit deren Umgang
- Geschäftsstrategien, Forecasts, Unternehmensdaten und Planungen
- Vorlagen und Vorschriften technische Art (unmittelbar aus § 23 GeschGehG) sowie Zeichnungen

## Konkrete Vorgehensweise: strukturierter Schutz

Die wichtigste Gesetzesänderung besteht wohl darin, dass Geschäftsgeheimnisse nur noch geschützt sind, wenn angemessene Geheimhaltungsmaßnahmen getroffen sind. In der Vergangenheit war es ausreichend, dass Geschäftsinformationen geheim bleiben sollten. Mit dem GeschGehG müssen Unternehmen ihre angemessenen Schutzmaßnahmen zur Geheimhaltung nachweisen können, damit Informationen auch weiterhin als Geschäftsgeheimnis Schutz genießen. Es sind also auch, aber nicht nur, interne Anweisungen und Richtlinien für Mitarbeiter erforderlich. Vergleichbar mit der Nachweis- und Rechenschaftspflicht („Accountability") aus Art. 5 Abs. 2 DSGVO. Welche Maßnahmen genau zu treffen sind, um nachweisen zu können, dass es sich um ein Geschäftsgeheimnis handelt, sagt das Gesetz leider nicht.

## Angemessene Maßnahmen: eher präventiv

Der Begriff der Maßnahme in der Gesetzesbegründung ist weit auszulegen und nicht nur auf rechtliche Maßnahmen beschränkt. Neben vertraglichen Geheimhaltungsmaßnahmen, die mehr oder weniger durchsetzbar sind, sind vor allem organisatorische und technische Maßnahmen zum Schutz von Geschäftsgeheimnissen zu ergreifen, also präventiv und nicht nur reaktiv zur Schadensbegrenzung. Diese technischen und organisatorischen Maßnahmen sind aus dem Datenschutzrecht (z. B. Sicherheit der Verarbeitung gem. Art. 32 DSGVO) bekannt. Dort geht es aber in erster Linie um den materiellen Datenschutz (Schutz des Rechtes auf informationelle Selbstbestimmung) und die Datensicherheit (zum Beispiel Integrität, Vertraulichkeit und Verfügbarkeit). Weitere Empfehlungen für die Umsetzung von technischen und organisatorischen Maßnahmen zur IT-Sicherheit liefert das IT-Grundschutz-Kompendium mit BSI-Standards. Aus der Datensicherheit nach DSGVO und IT-Sicherheit können Maßnahmen zum Informationsschutz angewandt und abgeleitet werden. Die technischen und organisatorischen Maßnahmen aus dem Datenschutz-Managementsystem sind auf jeden Fall eine sehr gute Grundlage und ein guter Ansatz für die im Rahmen des GeschGehG zu ergreifenden Maßnahmen.

Die Datensicherheit nach DSGVO und IT-Sicherheit sind allerdings nicht ausreichend, um den erforderlichen Schutz durch das GeschGehG zu erreichen. Dies ist darin begründet, dass die Datenschutzrechte die personenbezogenen Daten der betroffenen Person schützen. Das GeschGehG dagegen schützt jegliche Daten (auch ohne Personenbezug), sofern sie aus Sicht des Unternehmens der Vertraulichkeit unterliegen, sprich ein definiertes Betriebs- und Geschäftsgeheimnis darstellen.

## Exkurs Whistleblowing

Ausdrücklich hervorgehoben wurde bereits in der Gesetzesbegründung, dass § 5 Nr. 2 GeschGehG dem Schutz der so genannten Whistleblower dienen soll. Zunächst wurde, konsequenterweise gemäß Rechtfertigungslösung, ergänzend ausgeführt, die Regelung stelle klar, dass neben der Erlangung, die Nutzung und die Offenlegung von Informationen über rechtswidrige Handlungen und ein berufliches oder sonstiges Fehlverhalten unter den genannten Voraussetzungen gerechtfertigt sei. Es ist zu klären, ob und wenn ja, unter welchen Voraussetzungen Beschäftigte, die Kenntnis von solchen Informationen über rechtswidrige Handlungen oder sonstige Fehlverhaltensweisen haben, sich unmittelbar an Dritte, beispielsweise an Aufsichtsbehörden oder gar die Staatsanwaltschaft wenden dürfen.

Am 23.10.2019 trat die Richtlinie (EU) 2019/1973 des Europäischen Parlaments und des Rates zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, in Kraft.

## Durchsetzung von Ansprüchen

Das Geschäftsgeheimnisgesetz enthält spezielle zivilrechtliche Ansprüche für den Fall einer Geschäftsgeheimnisverletzung. Als Anspruchsnehmer kommt der Inhaber des Geschäftsgeheimnisses in Betracht. Anspruchsgegner ist der Rechtsverletzer. Ist dieser ein Beschäftigter eines Unternehmens, so kann der Inhaber dieses Unternehmens als weiterer Anspruchsschuldner hinzutreten. Sofern der Rechtsverletzer aus grober Fahrlässigkeit oder mit Vorsatz, also schuldhaft, gehandelt hat, steht dem Inhaber des Geschäftsgeheimnisses ein Anspruch auf Schadensersatz des aus der Rechtsverletzung (konkret) entstandenen Schadens zu. Bei der Bemessung des Schadens kann der Gewinn berücksichtigt werden, den der Rechtsverletzer erzielt hat.

Grundsätzlich kann auch Schadensersatz für immateriellen Schaden verlangt werden. Verjährungsansprüche ergeben sich unter anderem nach § 61 Abs. 2 HGB.

## Metadaten als Geschäftsgeheimnis: Eine Entscheidung des BVerwG macht die Reichweite deutlich

Metadaten sind strukturierte Informationen über Daten wie Zeitstempel und Namen. In einem Beschluss des Bundesverwaltungsgerichts (BVerwG, Beschl. V. 05.03.2020 – Az. 20 F 3. 19) ging es unter anderem um Metadaten zu Prüfunterlagen eines Bauartzulassungsverfahrens, zu der ein Ingenieurbüro Zugang begehrte. Das BVerwG stellte fest, dass der Schutz von Geschäftsgeheimnissen auch die Verhinderung des Zugangs von Metadaten von Dateien umfasst, zu denen Dateiname, Größe und die aus der Dateiendung abgeleitete Programmiersprache gehören.

Für nur ein einzelnes dieser Metadaten wäre ein Zugang wohl möglich gewesen, doch je mehr Metadaten offengelegt sind und miteinander verknüpft werden können, desto eher lässt sich das Geschäftsgeheimnis aus ihnen ableiten – weshalb ein Zugriff durch Dritte in der Gesamtschau nicht zulässig ist, sondern die Metadaten schützenswert macht. Das Gericht hatte sich zum Informationsfreiheitsgesetz (IFG) geäußert, jedoch zugleich klargestellt, dass der Begriff des Geschäftsgeheimnisses nach IFG parallel zum GeschGehG auszulegen ist.

## Strafbarkeit des Verstoßes

Strafbare Verletzung des Schutzes von Geschäftsgeheimnissen ist in § 23 GeschGehG geregelt: *„Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,*

1. *entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt,*
2. *entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder*
3. *entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt.“* (Abs. 1)

Gemäß Abs. 2: wird ebenso bestraft „[…] *wer … ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach …“*

In Abs. 3 findet sich eine Sonderregelung für *„… Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt …“*

### Über die Autoren

**Regina Mühlich**
ist Geschäftsführerin der Managementberatung AdOrga Solutions GmbH und Expertin für Datenschutz sowie Compliance Officer und Datenschutz-Auditorin (TÜV, DEKRA). Vorstandsmitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

▶ www.adorgasolutions.de

**Dr. Jens Eckhardt**
ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie Datenschutz-Auditor (TÜV) und Compliance-Officer (TÜV). Vorstandsmitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

▶ www.derra.eu

Das nächste BvD-Webinar der beiden Autoren findet am 16.04.2021 um 10:00 Uhr statt.

Über den QR-Code kommen Sie direkt zur Seminarankündigung.

# UMGANG MIT DATENSCHUTZPANNEN

Stefan Sander

## I. Was ist eine „Panne" im Datenschutz?

Ist die Bezeichnung „Datenschutzpanne" verharmlosend – und was genau ist damit gemeint? Die Auswahl an Synonymen ist groß, die Wortwahl vielgestaltig. Da ist die Sprache von einem Incident, einem Vorfall, einem Data Breach oder Datenleck, um nur einige Beispiele aufzugreifen. Doch sollten jene, die sich von Berufs wegen mit dem Thema befassen, idealerweise bei der festgelegten Fachsprache bleiben und – falls der Gesetzgeber selbst Begriffe definiert hat – auch nur die definierten Vokabeln benutzen. Dies erzeugt eine größere Eindeutigkeit und Verbindlichkeit von Aussagen, Ansichten und Argumentationssträngen. Für den vorliegenden Sachverhalt ist der Begriff der „Verletzung des Schutzes personenbezogener Daten" vorgegeben. Diesem feststehenden Ausdruck ist in Art. 4 Nr. 12 DS-GVO ein Tatbestand zugeordnet. Nach dem Willen des Gesetzgebers bezeichnet der Ausdruck „Verletzung des Schutzes personenbezogener Daten"

> *eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.*

Definiert wurde dieser Ausdruck als Kurzbezeichnung für den Tatbestand, der zentraler Dreh- und Angelpunkt des „risikoorientierten Ansatzes" der DS-GVO ist. Die Sicherheit der Verarbeitung, die verletzt wurde, findet sich sprachlich wieder in der amtlichen Überschrift von Art. 32 DS-GVO – dem Auftakt eben jenes Abschnittes der DS-GVO, in dem der risikoorientierte Ansatz niedergelegt ist (Art. 32 bis Art. 36 DS-GVO).

## II. Zur Systematisierung von technischen und organisatorischen Maßnahmen

Zur Abgrenzung des Themas ist darauf hinzuweisen, dass die DS-GVO – im Unterschied zur Rechtslage in Deutschland vor dem 25.05.2018 – etwa ein halbes Dutzend verschiedener Bündel von technischen und organisatorischen Maßnahmen im Wortlaut ihrer Artikel kennt, die sich hauptsächlich in zwei große Gruppen systematisieren lassen:

Es gibt einerseits diejenigen technischen und organisatorischen Maßnahmen, die auf Einhaltung der Zulässigkeit der Verarbeitung abzielen. Sie flankieren das bereits in Art. 8 der EU-Grundrechte-Charta (GRCh) verankerte Verbot mit Erlaubnisvorbehalt, finden ihre Grundnorm in Art. 24 Abs. 1 DS-GVO und sind nicht risikoorientiert – vielmehr lautet die Zielvorgabe vollständige Einhaltung der Zulässigkeit (Compliance).

Dem gegenüber stehen andererseits diejenigen technischen und organisatorischen Maßnahmen, die dem Zwecke der Risikobewältigung dienen und die ihre Grundnorm in Art. 32 Abs. 1 DS-GVO finden. Ihre Zielvorgabe lautet nicht, dass alle Risiken vermieden werden müssen. Vielmehr ist das System, welches eben als „der risikoorientierte Ansatz der DS-GVO" bezeichnet wurde, zweiteilig angelegt: Der eine Teil der Risiken soll, bei Erfüllung der gesetzlichen Pflichtenlage, vermieden werden. Das Maß des insoweit zur Pflichtenerfüllung Erforderlichen liegt in dem (eben auch nur) „angemessenen" Schutzniveau. Weil kein vollständiger Schutz verlangt wird, ergibt sich daraus zwanglos, dass es nach Ansicht des Gesetzgebers Risiken gibt, deren Verwirklichung durch technische und organisatorische Maßnahmen, die im Umfang des gesetzlich Erforderlichen getroffenen wurden, nicht verhindert wird (und auch bewusst nicht verhindert werden muss). Der Gesetzgeber hat daraufhin den zweiten Teil der Pflichtenlage so konzipiert, dass er weitergehende beziehungsweise andere Pflichten statuiert hat, die an die – wie es systemimmanent vorhergesehen ist – Verwirklichung jener Risiken anknüpfen. Um diese Pflichten zu formu-

lieren, wie es in den Art. 33, 34 DS-GVO geschah, war es mehr als nützlich, durch eine Begriffsbestimmung den feststehenden Ausdruck „Verletzung des Schutzes personenbezogener Daten" zu prägen, damit die Formulierung jener Pflichten besser lesbar, die Regelungen also übersichtlicher wurden.

Wichtig ist es zu verstehen, dass eine „Panne" im hier erläuterten Sinne nicht immer etwas sein muss, was schief gegangen ist, also wodurch gegen Pflichten verstoßen wurde. Eine Verletzung des Schutzes personenbezogener Daten kann auftreten, ohne dass ihr Auftreten ein Indiz für etwas vorausgegangenes Pflichtwidriges ist. Indes: Tritt eine Verletzung des Schutzes personenbezogener Daten auf, sind an das Auftreten in allen Fällen, also zu 100 Prozent, weitergehende Pflichten geknüpft (dazu weiter unten), deren Verletzung ihrerseits dann zu einer nachlaufenden Pflichtwidrigkeit führen kann. Quintessenz: Der DS-GVO geht es nicht darum, jede Verletzung des Schutzes personenbezogener Daten zu verhindern, sondern darum, dass auf jede Verletzung des Schutzes personenbezogener Daten richtig reagiert wird.

## III. Zielrichtung der diversen Maßnahmen

Während vor dem Risiko einer unzulässigen Verarbeitung, also dem Risiko eines rechtswidrigen Eingriffs in das Grundrecht aus Art. 8 GRCh, nach Art. 24 Abs. 1 DS-GVO vollständiger Schutz zu gewähren ist, ist zur Vermeidung der Risiken für alle anderen Grundrechte (dieses Ergebnis sei hier in der Gegenüberstellung vorweggenommen, die Herleitung folgt) nur ein angemessenes Schutzniveau i.S.v. Art. 32 Abs. 1 DS-GVO vorzusehen.

Der Begriff des Risikos ist in der DS-GVO nicht ausdrücklich definiert. Aus den ErwG 75, 94 DS-GVO kann jedoch nach – inhaltlich zutreffender – Ansicht der deutschen Datenschutzkonferenz (DSK), welche sie in ihrem Kurzpapier zur DS-GVO Nr. 18 geäußert hat, folgende Definition hergeleitet werden:

> *Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.*

Sowohl das Schadenausmaß, als auch die Eintrittswahrscheinlichkeit unterscheidet die DSK in je vier Abstufungen und wählt dafür die Bezeichnungen geringfügig, überschaubar, substantiell und groß. Soweit der Wortlaut des Art. 32 Abs. 1 DS-GVO ausführt, dass es um

> *das Risiko für die Rechte und Freiheiten natürlicher Personen*

geht, ist nebenbei zu bemerken, dass dort auf „natürliche" Personen und nicht auf „betroffene" Personen abgestellt wird und sodann auf die ErwG 75, 85 DS-GVO hinzuweisen: Danach kann sich aus der Verwirklichung eines Risikos ein physischer, materieller oder immaterieller Schaden ergeben. Aus dieser breiten Formulierung und den am angegebenen Ort genannten Beispielen für Schäden ergibt sich die Schlussfolgerung, dass die Auslegung der Passage in Art. 32 Abs. 1 DS-GVO („Rechte und Freiheiten") als Verweis auf alle grundrechtlich geschützten Positionen zu verstehen ist.

## IV. Wen trifft die Pflicht zu Maßnahmen zwecks Risikovermeidung?

Eine Verletzung des Schutzes personenbezogener Daten kann natürlich auch etwas vorausgegangenes Pflichtwidriges belegen. Waren die tatsächlich umgesetzten technischen und organisatorischen Maßnahmen nicht in der Lage, die Verwirklichung eines konkreten Risikos zu verhindern, wäre dies aber durch Maßnahmen in dem von Art. 32 Abs. 1 DS-GVO geforderten Maß verhindert worden, so liefert die im Einzelfall eingetretene Verwirklichung des Risikos den Beweis dafür, dass zuvor gegen Art. 32 Abs. 1 DS-GVO verstoßen wurde. Der Verstoß gegen die Norm liegt dabei nicht im Eintritt des Schadens, sondern im Unterlassen der Maßnahmen, die den Schadenseintritt verhindert hätten. Fälle dieser Art dürften der allgemeinen Vorstellung entsprechen, die vom Wortsinn her mit einer „Panne" assoziiert werden – versteht doch beispiels-

weise der Duden unter Panne einen „Fehler" oder ein „durch gedankenloses oder unvorsichtiges Handeln verursachtes Missgeschick". Die Wortwahl „Datenschutzpanne" impliziert also einen Vorwurf, der mitschwingt – und so stellt sich die Frage, an wen sich dieser Vorwurf richtet. Wessen Aufgabe ist es, für die Sicherheit der Verarbeitung zu sorgen, die im Falle der Verletzung des Schutzes personenbezogener Daten „verletzt" wurde?

Während es im Bereich der technischen und organisatorischen Maßnahmen, die auf Einhaltung der Zulässigkeit der Verarbeitung abzielen (Compliance), durch Art. 24 Abs. 1 DS-GVO eindeutig geregelt ist, dass dafür der Verantwortliche zuständig ist, ist es im Gegensatz dazu im Detail offen, wer welche Maßnahmen zur Risikovermeidung umsetzen muss. Solange nur Verarbeitungen betrachtet werden, an deren Ausführung nur der Verantwortliche beteiligt ist, ist die Rechtslage einfach zu bestimmen und mit jener in Art. 24 Abs. 1 DS-GVO deckungsgleich. Damit liegt auch die Umsetzung solcher Maßnahmen nach Art. 32 Abs. 1 DS-GVO in der Zuständigkeit des Verantwortlichen. Werden jedoch Verarbeitungen betrachtet, an deren Ausführung neben dem Verantwortlichen auch ein Auftragsverarbeiter beteiligt ist, ist nichts mehr eindeutig, weil der Wortlaut des Art. 32 Abs. 1 DS-GVO unterschiedslos beide in einem Atemzug in die Pflicht nimmt. Es gibt also zwei gesetzlich zugewiesene Pflichtenkreise, die technischen und organisatorischen Maßnahmen umfassen, welche dem Zwecke der Risikobewältigung dienen – den des Verantwortlichen und jenen des Auftragsverarbeiters.

Aus dem Umstand, dass ein Verstoß gegen Art. 32 Abs. 1 DS-GVO sowohl für Verantwortliche als auch für Auftragsverarbeiter mit einer Geldbuße sanktioniert werden kann, ergibt sich das Postulat, dass die beiden Pflichtenkreise – von Verantwortlichem einerseits sowie Auftragsverarbeiter andererseits – keine inhaltlichen Überschneidungen aufweisen. Denn andernfalls würde der aus dem römischen Recht herrührende Grundsatz „nulla poena sine lege certa", der in Europa als gemeinschaftliche Wertevorstellung verbreitet ist, unterlaufen (vgl. Art. 49 GRCh, Art. 7 MRK). Denn eine Überschneidung der Pflichtenkreise, die die Bildung einer gemeinsamen Schnittmenge zur Folge hätte, würde für die in Schnittmenge liegenden technischen und organisatorischen Maßnahmen eine Zuständigkeitsverwirrung zur Folge haben, die kategorisch Sanktionsmöglichkeiten entgegenstünde. Dabei sind Zuständigkeitsverwirrungen ein dem Gesetzgeber der DS-GVO bewusstes Problem gewesen, hat er doch an anderer Stelle dieselbe Gefahr durch die Pflicht zur Zuständigkeitszuweisung durch Vereinbarung i.S.v. Art. 26 DS-GVO gebannt. Da es eine vergleichbare Pflicht zur Zuständigkeitszuweisung durch Vereinbarung im Kontext von Art. 32 Abs. 1 DS-GVO nicht gibt, kann nur geschlussfolgert werden, dass der Gesetzgeber der DS-GVO davon ausging, dass die beiden von Art. 32 Abs. 1 DS-GVO angeordneten Pflichtenkreise keine Überschneidung aufweisen (zu Art. 28 Abs. 3 DS-GVO, siehe unten).

Der unmittelbar kraft Gesetzes in Art. 32 Abs. 1 DS-GVO dem Auftragsverarbeiter zugewiesenen Pflichtenkreis umfasst jene technischen und organisatorischen Maßnahmen, die ihrer Art nach geeignet sind zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Maßnahmen der sog. Auftragskontrolle). Darüber hinaus ist die Bestimmung der Inhalte der Pflichtenkreise eine derzeit offene Rechtsfrage und es ist nur eine Randbemerkung, dass der heute anzutreffende Mangel an Gewissheit nicht nur eine Schwäche der Konstruktion von Art. 32 Abs. 1 DS-GVO ist, sondern auch der Untätigkeit der (deutschen) Aufsichtsbehörden in der Vergangenheit zuzuschreiben ist. Denselben Konstruktionsfehler enthielt nämlich bereits § 9 BDSG (alte Fassung) – im Gegensatz zu Art. 17 Abs. 1 der Richtlinie 95/46/EG, welche den Pflichtenkreis insgesamt nur dem Verantwortlichen zuschrieb. Hätten die deutschen Aufsichtsbehörden in den Jahren 2001 bis 2018 Verstöße gegen § 9 BDSG (a.F.) häufig und spürbar sanktioniert, hätte dies wahrscheinlich Gerichtsentscheidungen zur Folge gehabt, welche Licht ins Dunkel gebracht hätten.

So bleibt es aktuell der zukünftigen Rechtsprechung vorbehalten, die Inhalte der Pflichtenkreise gegeneinander abzugrenzen, was mutmaßlich im Rahmen von Entscheidungen über Einsprüche gegen Geldbußen aufgrund von Art. 83 Abs. 4 lit. a) DS-GVO erfolgen wird. Mit Blick auf alle anderen Arten von technischen und organisatorischen Maßnahmen zum Zwecke der Risikobewältigung – also abgesehen von jenen zur Auftragskontrolle – dürfte die einzig überzeugende Sichtweise jene sein, dass sie allesamt allein in den gesetzlich angeordneten Pflichtenkreis des Verantwortlichen fallen.

Denn es ist nicht zu erklären, warum der gesetzliche Pflichtenkreis des Verantwortlichen kleiner werden sollte, sobald ein Auftragsverarbeiter hinzutritt – erst recht ergibt sich keine Rechtssicherheit, wenn man eine Verschiebung von technischen und organisatorischen Maßnahmen heraus aus dem Pflichtenkreis des Verantwortlichen, hinein in den Pflichtenreis des Auftragsverarbeiters annehmen würde. Abgesehen davon, dass für die Begründung einer derartigen Verschiebung schon kein

Anhaltspunkt erkennbar ist, wäre die Bestimmung des Umfangs solcher Verschiebungen gänzlich willkürlich, so dass sie von vornherein insgesamt abzulehnen ist.

Dazu ist abschließend anzumerken, dass vor einem solchen Hintergrund der unmittelbar aus dem Gesetz erwachsenden Pflichtenkreise von Verantwortlichem und Auftragsverarbeiter auch Sinn und Zweck von Art. 28 Abs. 3 S. 2 lit. c) DS-GVO gut zu erklären ist. Das Gesetz bestimmt an dieser Stelle, dass der Vertrag oder das sonstige Rechtsinstrument, welcher bzw. welches der Auftragsverarbeitung zugrunde liegt, sich inhaltlich mit dem Thema Maßnahmen i.S.v. Art. 32 Abs. 1 DS-GVO befassen muss. Weil sich durch den bloßen Umstand des Hinzutretens des Auftragsverarbeiters der gesetzliche Pflichtenkreis des Verantwortlichen i.S.v. Art. 32 Abs. 1 DS-GVO nicht verändert, ist es nur folgerichtig, das Thema „Delegation dieser Maßnahmen an den Auftragsverarbeiter" zum Mindestvertragsinhalt zu bestimmen. Unterstrichen wird die Stringenz dieses Regelungszusammenhangs durch den faktischen Umstand, dass es mit der Auftragsverarbeitung als solcher, also der Auslagerung einer Verarbeitung, in aller Regel einhergeht, dass der Verantwortliche sich selbst der faktischen Einflussmöglichkeiten begibt und deshalb seinen Pflichtenkreis außerhalb i.S.v. Art. 32 Abs. 1 DS-GVO gar nicht mehr erfüllen kann.

Von diesem Stereotyp der Auftragsverarbeitung ausgehend erscheint die gleichzeitige Delegation der Erfüllung der Pflichten aus Art. 32 Abs. 1 DS-GVO durch Vertrag an den Auftragsverarbeiter als die einzige sinnvolle Lösung. Im Ergebnis hat der Auftragsverarbeiter sodann seinen eigenen, unmittelbar aus Art. 32 Abs. 1 DS-GVO folgenden Pflichtenkreis und die durch Vertrag vom Verantwortlichen übernommenen Pflichten zur Umsetzung technischer und organisatorischer Maßnahmen zu erfüllen. Dieses Auslegungsergebnis hält auch der Gegenprobe stand, denn es würde keinen Sinn ergeben, wenn das Gesetz in Art. 28 Abs. 3 S. 2 lit. c) DS-GVO fordern würde, dass dem Auftragsverarbeiter durch den Vertrag oder ein anderes Rechtsinstrument Pflichten aufzuerlegen sind, welche ihn ohnehin selbst unmittelbar aus dem Gesetz, also aufgrund von Art. 32 Abs. 1 DS-GVO treffen würden.

## V. Die richtigen Reaktionen auf Datenschutzpannen

Wenn noch keine Kenntnis von der Verwirklichung des Tatbestands der Verletzung des Schutzes personenbezogener Daten vorliegt, ist nichts zu tun. Diese scheinbare Trivialität ist deshalb hier betont, weil die DS-GVO keine Verpflichtung vorsieht, die an den bloßen Verdacht einer Verletzung des Schutzes personenbezogener Daten anknüpft. Im Gegensatz dazu hat sich in der Vergangenheit eine Praxis der Vertragsgestaltung im Kontext der Auftrags(daten)verarbeitung herausgebildet, die vertragliche Pflichten bereits an das Vorhandensein von Verdachtsfällen knüpft; diese wären unabhängig von den gesetzlichen Pflichten zu beachten.

Liegt Kenntnis von einer Verletzung des Schutzes personenbezogener Daten i.S.v. Art. 4 Nr. 12 DS-GVO vor, so müssen – völlig losgelöst von jeglicher Beurteilung der Risiken – jedenfalls der Auftragsverarbeiter den Vorgang an den Verantwortlichen melden (Art. 33 Abs. 2 DS-GVO) und jedenfalls der Verantwortliche den Vorgang dokumen-

tieren (Art. 33 Abs. 5 DS-GVO). Die Dokumentation muss für die Aufsichtsbehörde nachvollziehbar die Verletzung des Schutzes personenbezogener Daten beschreiben und deren Auswirkungen sowie die ergriffenen Abhilfemaßnahmen festhalten. Klargestellt sei, dass der Auftragsverarbeiter entlang der Leistungskette (nur) nach oben zu melden hat – und dass nur soweit es um andere Verarbeitungen geht, wegen derer er selbst in der Rolle des Verantwortlichen ist, eine ihn treffende Meldepflicht gegenüber einer Aufsichtsbehörde in Betracht kommen kann.

Allgemein bekannt sein dürfte, dass im Weiteren die Verletzung des Schutzes personenbezogener Daten vom Verantwortlichen unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der Aufsichtsbehörde zu melden ist, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hierzu weist die DSK in ihrem Kurzpapier zur DS-GVO Nr. 18 – inhaltlich zu Recht – darauf hin, dass es vollständig risikolose Verarbeitungen nicht geben kann, so dass die Formulierung „nicht zu einem Risiko" von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko" führend verstanden wird. Mit dieser öffentlichen Bekanntgabe einer Rechtsauffassung dürfte, über das Institut der Selbstbindung der Verwaltung, die Gefahr behördlicher Sanktionen für Verantwortliche, die bei Verletzungen des Schutzes personenbezogener Daten mit voraussichtlich nur geringen Risiken für betroffene Personen von einer Meldung an die Aufsichtsbehörde absehen, nahezu nicht gegeben sein. Da die Aufsichtsbehörden unter einer Flut von Meldungen nach Art. 33 DS-GVO ohnehin zu leiden haben, haben diese auch selbst ein Interesse daran, dass Meldungen der Vorfälle in derartigen Konstellationen unterbleiben – wobei von einem geringen Risiko dann auszugehen sein dürfte, wenn die Schwere des möglichen Schadens maximal überschaubar ist, bei gleichzeitig nur geringfügiger Eintrittswahrscheinlichkeit des Schadens oder – alternativ dazu – die Schwere des möglichen Schadens nur geringfügig ist, während die Eintrittswahrscheinlichkeit maximal überschaubar sein dürfte.

Sollte die Risikobeurteilung, also die Risikoidentifikation und anschließende Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden, welche in einer Zuordnung zu den Risikoabstufungen führt, im Ergebnis auf ein voraussichtlich hohes Risiko hinauslaufen, sind zusätzlich zu den vorgenannten Maßnahmen die betroffenen Personen zu benachrichtigen. Die Anforderungen an die Benachrichtigung ergeben sich aus Art. 34 DS-GVO. In diesem Zusammenhang sei auf eine besondere Art von technischen und organisatorischen Maßnahmen aufmerksam gemacht, die ergriffen werden, nachdem eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist: Gem. Art. 34 Abs. 3 lit. b) DS-GVO entfällt die Verpflichtung des Verantwortlichen zur Benachrichtigung der betroffenen Personen, wenn der Verantwortliche durch „nachfolgende" Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht.

Am Ende des Tages ist unterm Strich festzuhalten: „Nach der Datenschutzpanne ist vor der Datenschutzpanne." Nimmt man den Tatbestand der Begriffsdefinition in Art. 4 Nr. 12 DS-GVO nur hinreichend ernst, ist in allen größeren Organisationen festzustellen, dass es sich bei Verletzungen des Schutzes personenbezogener Daten eher um ein Alltagsphänomen denn um eine Rarität handelt. Diese „Incidents" sollten jeweils als Auslöser verstanden werden, um den PDCA-Zyklus anzusteuern. Gemeint ist damit ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Auf die Evaluierung folgt natürlich noch die Umsetzung eines erkannten Verbesserungspotentials, zwecks Schließung etwaiger vorhandener Lücken bis zum Erreichen des angemessenen Schutzniveaus i.S.v. Art. 32 Abs. 1 DS-GVO. Sollte eine Verletzung des Schutzes personenbezogener Daten hohe Risiken für die Rechte und Freiheiten natürlicher Personen nach sich ziehen, mag dies – neben der Benachrichtigung der betroffenen Personen zum Zwecke der Risikominderung beziehungsweise Schadensbegrenzung – ein triftiger Anlass sein, den ursprünglichen Planungsprozess für die technischen und organisatorischen Maßnahmen i.S.v. Art. 32 Abs. 1 DS-GVO nochmals aufzurollen, d.h. erneut in die Datenschutz-Folgenabschätzung (DSFA) einzusteigen – oder eine solche erstmals durchzuführen, falls dieser Prozess zuvor noch nicht durchlaufen wurde. Eine entsprechende Verpflichtung besteht unter den Voraussetzungen von Art. 35 Abs. 11 DS-GVO.

Insoweit sei abschließend auf das Gesamtkonzept des risikoorientierten Ansatzes der DS-GVO hingewiesen: Mit der Verpflichtung des Verantwortlichen zur Durchführung einer DSFA wird dieser in einen strukturierten Prozess gezwungen, der die Planung von technischen und organisatorischen Maßnahmen zum Gegenstand hat, welche dem Zwecke der Risikobewältigung dienen. Die Verpflichtung zur Umsetzung eben dieser Maßnahmen ergibt sich aus Art. 32 Abs. 1 DS-GVO, während danach die tatsächlich umgesetzten Maßnahmen noch gem. Art. 30

Abs. 1 lit. g) DS-GVO zu dokumentieren sind. Diese insoweit als Schlusspunkt eines Zyklus aufgefasste Dokumentationspflicht sollte nicht vernachlässigt werden, auch wenn es im Gesetz nur heißt, dass „wenn möglich" eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO in das Verzeichnis von Verarbeitungstätigkeiten aufzunehmen ist. Denn der Gesetzgeber stellte sich ausweislich ErwG 82 DS-GVO vor, dass die Aufsichtsbehörden einen Teil ihrer Kontrolltätigkeiten „vom Schreibtisch" aus bewerkstelligen sollten, wozu insbesondere die Kontrollen gehören, ob der Verantwortliche und der Auftragsverarbeiter jeweils ihre Pflichten aus Art. 32 Abs. 1 DS-GVO de facto erfüllt haben:

> *Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.*

Im eigenen Interesse sollten daher zur Vermeidung von unnötigen Streitigkeiten mit den Aufsichtsbehörden die technischen und organisatorischen Maßnahmen eher zu ausführlich dokumentiert sein als zu knapp.


Über den Autor

**Stefan Sander LL.M., B.Sc.**

ist Rechtsanwalt und Fachanwalt für IT-Recht, zudem Software-Systemingenieur und Datenschutzbeauftragter (TÜV). Er führt mit Heiko Schöning die Kanzlei sds Rechtsanwälte Sander Schöning PartG mbH.

▶ www.sds.ruhr

sds Rechtsanwälte Sander Schöning PartG mbB



Anzeige

# Beeindrucken Ihre Datenschutzberichte Ihr Management?

2B Advice ®
The Privacy Benchmark

Auf Knopfdruck eine Powerpoint für den Chef

**Bestellen Sie unsere KOSTENLOSE Einzelplatzversion**

2B Advice GmbH - the privacy benchmark | Joseph-Schumpeter-Allee 25, Bonn | 0228 926165-100 | sales.de@2b-advice.com | www.2b-advice.com

# CONSENT TOOLS FÜR WEBSEITEN IM PRAXISTEST

Dr.-Ing. Klaus Meffert

Spätestens seit dem Urteil des Europäischen Gerichtshofs (EuGH) zur Einwilligung bei Cookies (Planet49) sind sogenannte Consent Tools, oft auch als Cookie Consent bezeichnet, populär geworden. Dieser Beitrag zeigt, dass solche Tools überbewertet werden, ein Vertrauen in diese Tools nicht gerechtfertigt ist und deren ungeprüfte Nutzung erhebliche rechtliche Gefahren mit sich bringt.

## 1. Einleitung

Zunächst werden die Grundlagen für Datenschutzregeln auf Webseiten vermittelt. Anschließend werden die Ergebnisse der Untersuchung von Consent Tools in der Praxis dargestellt. Danach folgt eine kritische Würdigung der Ergebnisse. Abschließend gibt der Beitrag Empfehlungen für Webseiten und eine mögliche Neuausrichtung des BDSG.

## 2. Grundlagen

Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten bleiben oft nur das berechtigte Interesse oder die **Einwilligung durch den Dateninhaber** (im Weiteren Nutzer genannt). Das berechtigte Interesse bedarf einer subjektiven Abwägung, die mit rechtlichen Unsicherheiten behaftet ist. Urteile zur Ungültigkeit des Privacy Shield oder zu Cookies zeigen auf, dass das Einholen einer Einwilligung beim Nutzer oft die einzige Möglichkeit ist, eine sichere Rechtsgrundlage zu schaffen.

Auf Webseiten spielen die genannten Urteile eine besonders große Rolle, denn IP-Adressen sind laut höchstrichterlichem Urteil personenbezogene Daten. Jeder Aufruf einer Webseite kommt damit einer Verarbeitung personenbezogener Daten gleich.

### 2.1. Grundlagen zu Datenübertragungen auf Webseiten

Der Begriff Domäne ist in Zusammenhang mit Datenübertragungen besonders wichtig. Eine Webseite uvwabc.de/kontakt hat die Domäne uvwabc.de. Eine Domäne ist ein symbolischer Name, der Teil einer Internet-Adresse ist.

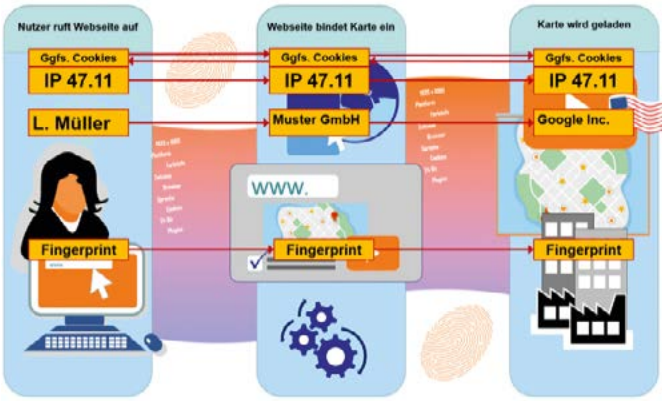



Abb. 1 Copyright: Dr. Klaus Meffert Fundamentale Datenübertragungen auf Webseiten

In der Abbildung 1 sind die Datenübertragungen dargestellt, die beim Aufruf einer Webseite stattfinden. Für die Abbildung wurde angenommen, dass die Webseite eine Karte von Google Maps einbindet.

Ruft ein Nutzer die Webseite auf, passiert aufgrund des

Internet-Protokolls folgendes:

1. Die IP-Adresse des Nutzers wird zur Webseite übertragen. Dies ist notwendig, damit eine Zustellung der Antwort möglich ist.
2. Alle Cookies, die im Browser (Endgerät) des Nutzers zur Domäne uvwabc.de gespeichert sind, werden an die Webseite übertragen.
3. Die Verkehrsdaten des Nutzers, auch als Fingerabdruck bezeichnet, werden an die Webseite übertragen. Verkehrsdaten sind etwa die Browserkonfiguration oder Merkmale zum verwendeten Betriebssystem.
4. Die IP-Adresse des Nutzers wird zum Google-Maps-Server übertragen.
5. Alle Cookies für alle Domänen, von denen Google Maps Dateien abruft, und die im Browser des Nutzers gespeichert sind, werden zu den Google-Servern übertragen, die für das Bereitstellen von Google Maps verantwortlich sind.
6. Die Verkehrsdaten des Nutzers werden an die für das Bereitstellen der Karte beteiligten Google-Server übertragen.

Weil IP-Adressen personenbezogene Daten sind, unterliegt jeder auf einer Webseite eingesetzte Dienst eines Dritten den Anforderungen der DSGVO.

### 2.2. Grundlagen zu Cookies

Ein Cookie ist an eine Domäne gebunden. Eine Domäne ist beispielsweise google.com. Wird die Domäne, an die ein Cookie gebunden ist, aufgerufen, wird das Cookie automatisch mit an den aufgerufenen Server übertragen. Wird also die Webseite google.com im Browser aufgerufen, werden alle Cookies, die auf dem Endgerät des Nutzers zur Domäne google.com gespeichert sind, automatisch zum Server, auf dem sich die Webseite google.com befindet, übertragen. Dies ist durch das Internet-Protokoll definiert.

Rein technisch lassen sich First-Party- und Third-Party-Cookies unterscheiden. Diese technische Einordnung hat zunächst wenig mit einer datenschutzrechtlichen Einordung zu tun.

First-Party-Cookies sind solche, die dieselbe Domäne besitzen wie die gerade besuchte Webseite. Wird auf einer Webseite ein Dienst wie Google Analytics geladen, kann dieser Dienst über JavaScript-Befehle First-Party-Cookies erzeugen, auslesen und ändern.

Außerdem kann der von der Webseite geladene Dienst die aktuellen Werte potenziell aller Cookies an einen beliebigen Zielpunkt senden, also auch an einen Google Server.

Wie man hieran sieht, handelt es sich bei Google-Analytics-Cookies nur aus technischer Sicht um First-Party-Cookies, aus fachlicher Sicht offensichtlich um Cookies, die von Google Analytics als Drittem (Third Party) verwaltet werden. Auch die Webseite selbst, die den Dienst geladen hat, kann First-Party-Cookies verwalten.

Third-Party-Cookies können nur von einem Dienst eines Dritten, der von einer Webseite geladen wird, erzeugt, ausgelesen oder geändert werden.

Ein First-Party-Cookie kann auch zu einem Third-Party-Cookie werden, wie dieses Beispiel zeigt:

1. Ein Nutzer ruft die Google-Suchmaschine auf, indem er die Webseite google.com im Browser öffnet. Dabei werden First-Party-Cookies für die Domäne google.com gesetzt.
2. Der Nutzer ruft irgendwann später die Webseite uvwabc.de auf, die Google Maps einbindet. Zur Darstellung der Karte werden Dateien von der Domäne google.com geladen. Dabei werden die schon aus dem Aufruf der Suchmaschinen vorhandenen Cookies übertragen. Es handelt sich jetzt um Third-Party-Cookies. Der Grund ist, dass die Domäne uvwabc.de nicht mit der Domäne google.com übereinstimmt.

Daraus resultiert eine unüberwindbare Gefahr für sämtliche Webseiten, die Consent-Tools einsetzen. Gibt es nur eine einzige Webseite weltweit, die ein Cookie für eine Domäne wie beispielsweise googletagmanager.com setzt, ist diese Domäne potenziell immer mit einem Cookie-Datentransfer behaftet. Der Autor kann nachweisen, dass beispielsweise das NID-Cookie für die Google-Tag-Manager-Domäne übertragen wird. Gleiches gilt für Google-Schriften.

### 2.3. Einwilligungspflichtige Vorgänge auf Webseiten

Für einwilligungspflichtige Datenverarbeitungsvorgänge folgen zwei Beispiele, jeweils unter Nennung der Rechtsgrundlagen.

#### Übertragung von Cookies

Die ePrivacy Richtlinie 2009/136/EG, vormals Richtlinie 2002/58/EG, besagt in Artikel 5 Absatz 3 eindeutig:

„Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat."

Weiter heißt es dort, dass eine technisch notwendige Speicherung erlaubt ist. Das Nutzen von Cookies zum Laden einer Karte von einem Google-Server ist technisch nicht notwendig, denn die Anzeige der Karte funktioniert auch ohne Cookies.

Dies ist daran erkennbar, dass das *Google Maps* Cookie namens NID nicht vom Kartendienst selbst gesetzt wird, sondern beim Aufruf der Suchmaschine unter www.google.com. Mit Hilfe der Entwicklerkonsole eines Browsers wie Mozilla Firefox kann das jederzeit nachvollzogen werden (mit der Taste F12 kann die Konsole anzeigt werden; dort sind die gesetzten Cookies zu sehen).

Gemäß Artikel 5 Absatz 3 der ePrivacy-Richtlinie bedarf es also einer Einwilligung, wenn auf Informationen, die im Endgerät des Nutzers gespeichert sind, zugegriffen wird. Der Abruf von Cookies beim Laden von Google Maps ist eindeutig ein solcher Zugriff. Hierbei spielt es keine Rolle, ob es sich um personenbezogene Daten handelt oder nicht. Dies hat der EuGH (Urteil vom 01.10.2019 – C-673/17 – Planet49) festgestellt. Dass §15 Abs. 3 des Telemediengesetzes gemäß der ePrivacy-Richtlinie auszulegen ist, hat der BGH in einem Urteil am 28.05.2020 – I ZR 7/16 (Einwilligung in die Speicherung von Cookies) festgestellt.

**Zwischenfazit:** Das Laden von Google Maps, Google reCAPTCHA, Google Schriften und Google Tag Manager bedarf aufgrund von Cookie-Transfers einer Einwilligung.

### Nachverfolgen des Nutzers ohne Cookies

Unter Tracking oder Web Tracking wird das möglichst eindeutige Identifizieren von Nutzern in Netzwerken wie dem Internet verstanden, um die Gewohnheiten dieser Nutzer zu erforschen und auszubeuten. Da beim Tracking mit Cookies die Rechtsgrundlagen aus dem vorigen Abschnitt gelten, soll hier das Tracking ohne Cookies thematisiert werden. Ein solches Tracking ohne Cookies findet beispielsweise beim Einbinden von YouTube-Videos auf Webseiten statt. Aktiviert man für den YouTube Einbettungscode die sogenannten erweiterten Datenschutzeinstellungen beziehungsweise verwendet als Einbettungsadresse youtube-nocookie.com, verspricht die Firma Google als Anbieter von YouTube, keine Cookies zu setzen.

Was beim Laden eines derartigen YouTube-Scripts zum Einbetten eines Videos passiert, kann hier nur ansatzweise beschrieben werden:

- Scripte und andere Dateien werden von den Domänen *youtube-nocookie.com*, *ytimg.com* und *ggpht.com* geladen.
- *Google Schriften* werden von der Domäne *gstatic.com* geladen.
- Der *DoubleClick* Tracker wird von der Domäne *doubleclick.net* geladen.
- Das *YouTube Script* sendet nach dem Laden der Seite Daten in erheblichem Umfang an Google.
- *DoubleClick* sendet in unbestimmten Abständen Daten an Google

Diese Vorgänge finden statt, ohne dass ein Video abgespielt wird.

Laut Nutzungsbedingungen von YouTube und Google ([1] mit Verweis auf [2]) muss für folgende Aktivitäten eine Einwilligung eingeholt werden: *„...die Erhebung, Weitergabe und Nutzung von personenbezogenen Daten zur Personalisierung von Werbeanzeigen."*

Da *YouTube* und *DoubleClick* Nutzerdaten in erheblichem Umfang erheben, handelt es sich um eine Erhebung und Weitergabe personenbezogener Daten zur Personalisierung von Werbeanzeigen. Daraus folgt aus den Google Nutzungsbedingungen die Einwilligungspflicht beim Einsatz von *YouTube Videos* jeder Art. Falls die Google-Nutzungsbedingungen ignoriert werden, ist als Rechtsgrundlage für ein Einwilligungserfordernis Artikel 6 DSGVO anzuführen. Dort könnte höchstens das berechtigte Interesse angeführt werden. Wie in diesem Abschnitt beschrieben, kann es aber kein berechtigtes Interesse sein, zahlreiche Datenerhebungen inklusive der Nachverfolgung des Nutzers durchzuführen, ohne dass ein Video abgespielt werden soll. Bekanntlich kann ein Video auch ohne Nachladen von DoubleClick abgespielt werden (vgl. Art. 5 Abs. 1 c DSGVO).

**Zwischenfazit:** Das Einbinden eines YouTube-Video-Scripts und vergleichbarer Tools, die nichtfunktionale, nicht durch berechtigtes Interesse gedeckte Datenverarbeitungen durchführen, bedarf einer Einwilligung.

## 3. Praxistest von Consent Tools

### 3.1 Art des Tests

Für folgende Consent Tools wurde ein Praxistest durchgeführt:

- Borlabs Cookie
- consent manager
- Cookiebot
- CCM19
- Klaro!
- OneTrust (synonym: Optanon, Cookie Law)
- UserCentrics

Nach dem Test wurde der Autor auf das Consent Tool CookieFirst aufmerksam. Weil es vergleichbare Charakteristiken wie die betrachteten Tools aufweist, wurde auf einen Nachtest von CookieFirst verzichtet.

Der Test fand statt, indem pro Consent Tool drei deutsche Webseiten, die das jeweilige Tool einsetzen, untersucht wurden. Insgesamt wurden also 21 Webseiten untersucht.

Dabei wurden insbesondere Webseiten größerer deutscher Unternehmen betrachtet. Außerdem wurden nach Möglichkeit die Webseiten der Anbieter, die ihr eigenes Tool einsetzen, untersucht.

Pro Webseite und Consent Tool wurden jeweils mehrere Kriterien wohlwollend geprüft. Eine tiefergehende rechtliche Betrachtung, etwa von Datenschutztexten, fand nicht statt.

Zu den geprüften Kriterien gehörten insbesondere:

- Laden von einwilligungspflichtigen Diensten ohne Einwilligung
- Möglichkeit der Ablehnung
- Nennung einer Widerrufsmöglichkeit (Art. 7 Abs. 3 DSGVO)
- Nennung und Beschreibung eingesetzter Dienste (Art. 12 DSGVO)
- Nennung und Beschreibung eingesetzter Cookies (Art. 12 DSGVO)
- Nennung der Übermittlung von Daten in Drittländer (Art. 49 DSGVO)
- Vollständiges Ausführen des Widerrufs (Art. 7 Abs. 3 DSGVO)

Das Laden von einwilligungspflichtigen Diensten ohne Einwilligung wurde sowohl automatisiert mit einer eigenen Software geprüft als auch manuell nachgeprüft. Dazu wurden automatisiert maximal 100 Seiten jeder getesteten Webseite untersucht.

Die Nennung von eingesetzten Diensten und Cookies bedingt auch die Nennung der zugehörigen Anbieter. Die Notwendigkeit der Beschreibung eingesetzter Cookies gemäß Art. 13 DGSVO wurde durch Urteil des EuGH vom 01.10.2019 – C-673/17 bestätigt.

### 3.2 Testergebnis

Keine der 21 getesteten Webseiten war auch nur annähernd datenschutzkonform. Im Durchschnitt wies jede der Webseiten zehn Mängelkategorien auf. Pro Kategorie waren meist mehrere Einzelmängel vorhanden. Die Mängel können oft als Verstöße gewertet werden. Einige der Mängel sind den strukturellen Schwächen der Consent Tools anzulasten. Dies kann auch deshalb behauptet werden, weil für die eigenen Webseiten von Anbietern der Consent Tools zahlreiche Mängel festgestellt werden konnten.

Das umfangreiche Gesamtergebnis kann beim Autor angefordert werden.

#### Unerlaubtes Laden einwilligungspflichtiger Dienste

Auf allen getesteten Webseiten wurden einwilligungspflichtige Dienste ohne Einwilligung geladen, nämlich ohne, dass die Einwilligungsabfrage bestätigend oder ablehnend geschlossen worden wäre. Zahlreiche der untersuchten Consent Tools konzentrierten sich ausschließlich oder überwiegend auf Cookies. Dies ist aus mehreren Gründen fatal und falsch. Wie in diesem Artikel in den Grundlagen beschrieben wurde, gibt es einwilligungspflichtige Vorgänge auf Webseiten, bei denen Cookies keine Rolle spielen. Außerdem können Consent Tools mit Fokus auf Cookies nur solche Cookies erkennen, die beim automatisierten Durchlaufen (Scannen) einer Webseite zur Bestandsaufnahme durch das Consent Tool vorhanden sind, weil sie von den geladenen Diensten frisch erzeugt wurden. Cookies, die auf den Endgeräten von Nutzern gespeichert sind, können hierbei nicht erkannt werden. Wie das Beispiel des Google Tag Manager aus dem Grundlagen-Abschnitt dieses Beitrags zeigt, besteht das Problem der unerkannten Cookies in relevantem Maße.

#### Keine freiwillige Einwilligung

Auf zahlreichen Einwilligungsfenstern ist eine direkte Ablehnung nicht möglich. Teilweise ist der Ableh-

nen-Button gegenüber der Einwilligungsoption optisch erheblich zurückgestellt. Eine Reihe von Vorschriften, Urteilen und Behördenmeinungen geben dem gesunden Menschenverstand recht und legen nahe, dass dies rechtswidrig sein könnte.

**Fehler bei rechtlichen Formvorschriften**

Nahezu jedes Consent Tool weist auf den getesteten Webseiten selbst für populäre Dienste mangelhafte Beschreibungen der Dienste und Cookies auf. Beispielsweise wird der Facebook Pixel einmal so benannt: „*Beiträge aus Facebook darstellen*". Als Zweck wird angegeben: „*Wird verwendet, um Facebook-Inhalte zu entsperren*". Hier bleibt unklar, ob ein Dienst oder ein zugehöriges Cookie beschrieben wurde. Eine Funktionsdauer (Lebensdauer) zum Cookie, wie sie seit dem EuGH-Urteil zu Planet49 notwendig ist, fehlt.

Diese Art von Mängeln in der Beschreibung von Diensten und Cookies kann für jedes genannte Consent Tool festgestellt werden. Hinzu kommt oft noch eine fehlende oder mangelhafte Nennung von Anbietern. Die Angabe „Google" ist jedenfalls nicht geeignet zur Identifikation eines Anbieters.

Die angemessene Beschreibung der einzuwilligenden Dienste und Cookies ist eine der Hauptaufgaben von sogenannten Einwilligungslösungen. Diese versagen in der Praxis hierzu in gravierendem Maße. Auf einigen der getesteten Webseiten war die Datenschutzerklärung erst nach Wegklicken des Consent Tools lesbar. Damit könnte diese als unverfügbar gelten.

## 4. Fazit

Consent Tools stellen sich in der Praxis als ungeeignet heraus, datenschutzkonforme Webseiten zu erhalten. Aus technischen Gründen können Consent Tools Ladevorgänge nicht zuverlässig selbst anhalten, bis ein Nutzer eingewilligt hat. Zudem sind die von den Consent Tools mitgelieferten Beschreibungen zu Diensten und Cookies nicht geeignet für einen rechtssicheren Einsatz. Hierfür gibt es zwei Gründe: Erstens durchdringen viele Anbieter von Consent Tools die Komplexität des Datenschutzes im Internet nicht vollständig. Zweitens sind für zahlreiche Dienste und Cookies die genaueren Zwecke unbekannt, weil die Dienstanbieter sie nicht klar kommunizieren. Dieses Ergebnis legt es nahe, Nutzen und Risiken sämtlicher eingesetzter Dienste gegeneinander abzuwägen. Alternativen zu populären Diensten bieten oft mehr Rechtssicherheit bei ähnlich guter Funktion. Im Hinblick auf eine mögliche Novelle des BDSG erscheint es sinnvoll, konkrete Vorgaben hinsichtlich des Datenschutzes im Internet einfließen zu lassen. So sollte etwa die Einwilligungspflicht klarer ausgestaltet werden. Eine kritische Betrachtung des Art. 7 DSGVO könnte nicht schaden. Eine Einwilligungsabfrage ist offenbar auch dann zulässig, wenn die Einwilligung Gefahren für den Nutzer mit sich bringt. Eine „unfaire", weil nur schwer nachweisbare algorithmisch bestimmte Personenbeziehbarkeit sollte bestmöglich gesetzlich unterbunden werden.

## 5. Quellen

[1] YouTube Nutzungsbedingungen:
https://dr-dsgvo.de/gnb

[2] Google-Richtlinie zur Einwilligung der Nutzer in der EU:
https://dr-dsgvo.de/ucp

Über den Autor

**Dr.-Ing. Klaus Meffert**

ist Diplom-Informatiker und Geschäftsführer der IT Logic GmbH. Er beschäftigt sich mit dem Datenschutz im Internet und hat die Datenschutz-Software wwwschutz entwickelt. Sein Fokus liegt auf einer gleichermaßen technischen und rechtlichen Betrachtung von Datenschutzbelangen.

▶ https://wwwschutz.de

# DATENSCHUTZBEAUFTRAGTE IM GESUNDHEITSWESEN – EINE SPEZIELLE HERAUSFORDERUNG

Bernd Schütze

## Einleitung

Datenschutzbeauftragte sind in den verschiedensten Sektoren bzw. Branchen anzutreffen. Ein Bereich ist die Gesundheitsversorgung. Datenschutzbeauftragte finden sich hier etwa bei Krankenkassen, in Krankenhäusern oder Arztpraxen, in Apotheken, Pflege- und Altenheimen, aber auch bei den „Lieferanten" wie den Herstellern von Arzneimitteln, Medizinprodukten oder speziellen Informationssystemen für die Gesundheitsversorgung. Jedoch handelt es sich um einen stark reglementierten Bereich mit einer Vielzahl an Gesetzen. Zudem existiert entsprechend Art. 74 GG im Bereich des Gesundheitswesens eine konkurrierende Gesetzgebung, sodass eher regelhaft eine länderspezifische Betrachtung der Rechtslage nicht zu umgehen ist.

Im folgenden Beitrag werden einige Besonderheiten (sehr) kurz dargestellt. Zum Teil wird auch auf allgemeinere Punkte eingegangen, die gleichermaßen auch auf andere Bereiche als das Gesundheitswesen zutreffen. Dies dient der Klarstellung beziehungsweise der Einführung, warum einige geregelte und dargestellte Aspekte betrachtet werden müssen.

## Benennung: Pflicht oder Kür?

Regelungen über die Verpflichtung zur Benennung eines Datenschutzbeauftragten finden sich in Art. 37 DS-GVO sowie in § 38 BDSG für nichtöffentliche Stellen sowie in § 5 BDSG für öffentliche Stellen. Speziell für den Gesundheitsbereich findet sich eine Regelung in Art. 37 Abs. 1 lit. b DS-GVO: Ein Datenschutzbeauftragter ist dann zu benennen, wenn die Kerntätigkeit des Verantwortlichen in der *umfangreichen* Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien von Daten, zu denen insbesondere genetische und Gesundheitsdaten gehören, besteht.

Allein schon durch die gesetzlichen wie auch berufsrechtlichen Dokumentationspflichten gehört die Verarbeitung von genetischen und Gesundheitsdaten zu den Kerntätigkeiten bei der Patientenversorgung, jedoch wurde der Begriff einer *umfangreichen* Verarbeitung leider gesetzlich nicht definiert, sodass hier eine gewisse Rechtsunsicherheit vorherrscht.

Der Europäische Datenschutzausschuss gibt im Abschnitt 2.1.3 in den von der Artikel-29-Datenschutzgruppe übernommenen „Leitlinien in Bezug auf Datenschutzbeauftragte" bei der Klärung, ob eine Verarbeitung umfangreich ist, an, dass folgende Faktoren zu berücksichtigen seien[1]:

- die Zahl der betroffenen Personen – entweder als bestimmte Zahl oder als Anteil an der maßgeblichen Bevölkerung,
- das Datenvolumen und/oder das Spektrum an in Bearbeitung befindlichen Daten,
- die Dauer oder Permanenz der Datenverarbeitungstätigkeit und
- die geografische Ausdehnung der Verarbeitungstätigkeit.

Damit kann leider auch keine eindeutige Aussage getroffen werden, ab wann eine „umfangreiche" Verarbeitung vorliegt. Lediglich nach unten kann eine Grenze angegeben werden: In ErwGr. 91 findet sich die Aussage, dass die Verarbeitung personenbezogener Daten nicht als umfangreich gelten sollte, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. Niedergelassene Arztpraxen, in denen ausschließlich eine Ärztin oder ein Arzt arbeitet, führen wohl keine „umfangreiche" Verarbeitung durch. Aber ob die Aussage bei zwei Ärzten/Ärztinnen immer noch gilt, kann wohl nur im Einzelfall betrachtet werden.

In der Fassung der DS-GVO vom Europäischen Parlament war in den ErwGr. 63 und 75 und auch im Art. 32a („Risk analysis") von der Verarbeitung der Daten von 5.000 betroffenen Personen innerhalb von zwölf Monaten die Rede[2]. Auch wenn dieser Ansatz nicht in der finalen Version der DS-GVO Einzug fand, bietet dieser Wortlaut einen Hinweis, was sich der europäische Gesetzgeber unter einer großen Anzahl von betroffenen Personen vorstellte.

Allgemein wird aber davon ausgegangen, dass Einrichtungen der Gesundheitsversorgung, in denen mehrere Angehörige eines Gesundheitsberufes arbeiten, beispielsweise in Krankenhäusern, Altenheimen oder Rehabilitationseinrichtungen, auf jeden Fall einen Datenschutzbeauftragten benennen müssen.

In § 38 Abs. 1 S. 2 BDSG findet sich zudem die Pflicht zur Benennung eines Datenschutzbeauftragten, wenn eine Datenschutz-Folgenabschätzung für eine Verarbeitung erforderlich ist. Eine Datenschutz-Folgenabschätzung ist immer dann erforderlich, wenn „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" besteht. Hier ist natürlich ebenfalls eine individuelle Betrachtung bei der Verarbeitung der besonders sensiblen Gesundheitsdaten erforderlich. Ob bei der Verarbeitung von Gesundheitsdaten in niedergelassenen Versorgungseinrichtungen ein hohes Risiko besteht, kann angesichts der verschiedenen Berichte, wie sie regelmäßig auf dem Jahreskongress des Chaos Computer Clubs vorgestellt werden und in Artikeln von Fachzeitschriften und Online-Journals zu finden sind, wahrscheinlich bejaht werden.

Im nationalen Recht wird von Autoren in § 22 Abs. 4 Nr. 4 BDSG eine Bestärkung der in Art. 37 DS-GVO resp. § 38 BDSG festgelegten Pflicht zur Benennung eines Datenschutzbeauftragten gesehen[3]. Um evtl. Rechtsfolgen wie Bußgeldern zu entgehen, sollte daher immer dann, wenn eine Pflicht zur Benennung nicht sicher ausgeschlossen werden kann, ein Datenschutzbeauftragter benannt werden. Zudem müssen die datenschutzrechtlichen Anforderungen unabhängig von der Benennung eingehalten werden, jedoch fehlt dem Verantwortlichen wie beispielsweise dem Inhaber einer Arztpraxis ohne Datenschutzbeauftragten die fachkundige Beratung. Und dass gerade viele niedergelassene Arztpraxen eine fachkundige Beratung benötigen, kann man an den vielen unnötig eingeholten Einwilligungen zur Verarbeitung von Daten zu Behandlungszwecken sehen; Rechtsgrundlage ist hier immer der Behandlungsvertrag, eine Einwilligung ist somit unnötig und kann im Falle eines Widerrufs auch zu ernsten Problemen führen – was ein auf das Gesundheitswesen spezialisierter Datenschutzbeauftragter wissen sollte.

Sofern eine fehlende Pflicht zur Benennung nicht offensichtlich ist – was angesichts der Regelung in Art. 37 Abs. 1 lit. c DS-GVO bei genetischen

[1] Europäischer Datenschutzausschuss: von der Artikel-29-Datenschutzgruppe übernommenen Papiere. Online, zitiert am 2021-01-12; verfügbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de. pdf-Papier der Leitlinie unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 abrufbar

[2] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Online, zitiert am 2021-01-12; verfügbar unter http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212#BKMD-6

[3] So z. B. Weichert T.: § 22 Rn. 35. In: Kühling/Buchner, DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325

und Gesundheitsdaten eher regelhaft der Fall sein dürfte – und kein Datenschutzbeauftragter benannt wurde, muss entsprechend Art. 24 DS-GVO ein Nachweis hinsichtlich der fehlenden Benennungspflicht erbracht werden können, was natürlich nur durch eine entsprechende Dokumentation erfolgen kann[4].

## Aufgaben

Art. 39 DS-GVO regelt die Mindest-Aufgaben des Datenschutzbeauftragten[5], diese sind:

- Unterrichtung und Beratung (auch im Zusammenhang mit der Datenschutz-Folgenabschätzung),
- Überwachung der Einhaltung der Datenschutzregelungen,
- Sensibilisierung und Schulung von Mitarbeitern,
- Zusammenarbeit mit der Aufsichtsbehörde,
- die indirekt in Art. 38 DS-GVO enthaltenen Aufgaben
  - Berichterstattung
  - Tätigkeit als Ansprechpartner betroffener Personen.

Nicht explizit aufgeführt, aber aufgrund der bestehenden Nachweispflichten natürlich unverzichtbar, ist die Erstellung von regelmäßigen Tätigkeitsberichten. Mindestens alle zwei Jahre ist dem Verantwortlichen ein entsprechender Bericht vorzulegen. Bei Aufbau und Struktur kann man sich an den Berichten der Landesbeauftragten oder des Bundesbeauftragten orientieren, wenngleich die eigentlichen Inhalte sich natürlich unterscheiden.

In Art. 39 Abs. 2 DS-GVO ist zudem der risikobasierte Ansatz der DS-GVO abgebildet worden, sodass der Datenschutzbeauftragte die Erfüllung seiner Aufgaben und insbesondere die Bewertungen der technischen und organisatorischen Maßnahmen am Risiko ausrichten muss, welches die jeweilige Verarbeitung für die Rechte und Freiheiten betroffener Personen beinhaltet. Dieser risikoorientierte Ansatz verlangt vom Datenschutzbeauftragten unter anderem, dass die Aufgaben mit „Augenmaß" bearbeitet werden. Zum risikoorientierten Ansatz gehört jedoch gleichermaßen, dass er kritische Datenverarbeitungen in den Mittelpunkt seiner Tätigkeit stellt[6].

Die Regelungen in der DS-GVO sind dabei nicht abschließend, sondern der Katalog an Aufgaben kann erweitert werden, jedoch müssen ergänzende Tätigkeiten mit den normativ geregelten Aufgaben vereinbar sein und dürfen insbesondere keine Interessenskonflikte auslösen[7]. Dies könnte beispielsweise die in Art. 47 Abs. 2 lit. h DS-GVO verankerte Pflicht zur Überwachung der Einhaltung von Binding Corporate Rules sein. Auch die Koordinierung der erforderlichen Aktionen bei einem Datenschutzvorfall inklusive der Dokumentation kann zu den ergänzenden Aufgaben eines Datenschutzbeauftragten gehören. Gerade im Gesundheitsbereich wird viel mit Einwilligungen gearbeitet, etwa im Bereich der medizinischen Forschung. Hier kann der Datenschutzbeauftragte bei der Erstellung der Einwilligungsformulare unterstützen. Weiterhin kann er ein Verfahren zur Bearbeitung von Betroffenenanfragen für das Unternehmen erarbeiten oder Templates für Konzepte wie Lösch- oder Berechtigungskonzept zur Verfügung stellen – kurz: Ein Datenschutzbeauftragter kann ein Unternehmen auf vielerlei Weise unterstützen und somit entlasten.

## Fachkunde

Grundlage für die Benennung eines Datenschutzbeauftragten ist, dass die zu benennende Person die Qualifikation und insbesondere die benötigte Fachkunde besitzt. Dies bedeutet aber auch, dass die Person schon zum Zeitpunkt der Benennung die erforderliche Fachkunde aufweist[8]. Dies heißt nicht, dass nicht auch Kenntnisse hinzugewonnen werden können oder sogar müssen; Verarbeitungen personenbezogener Daten verändern sich und entsprechend diesen Veränderungen muss der Datenschutzbeauftragte mitunter zusätzliches Wissen oder weitergehende Fertigkeiten erwerben. Aber eine Benennung ohne die zum Zeitpunkt der Benennung erforderliche Qualifikation ist nicht statthaft.

Entsprechend ErwGr. 97 der DS-GVO richtet sich das erforderliche Niveau des Fachwissens insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz verarbeiteter personenbezogener Daten. ErwGr. 51 der DS-GVO sieht bei besonderen Kategorien

[4] So z. B.
- Bergt, M. Art. 37 Rn. 32. In: Kühling/Buchner, DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325
- Drews S.: Art. 37 Rn. 33. In Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag. 1. Auflage 2019. ISBN 978-3-8487-3590-7

[5] Bergt, M. Art. 39 Rn. 1. In: Kühling/Buchner, DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325

[6] Drews S.: Art. 39 Rn. 39. In Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag. 1. Auflage 2019. ISBN 978-3-8487-3590-7

[7] So z. B.
- Bergt, M. Art. 39 Rn. 10. In: Kühling/Buchner, DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325
- Drews S.: Art. 39 Rn. 5. In Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag. 1. Auflage 2019. ISBN 978-3-8487-3590-7

[8] So z. B.
- Bergt, M. Art. 37 Rn. 33. In: Kühling/Buchner, DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325
- Drews S.: Art. 37 Rn. 46. In Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag. 1. Auflage 2019. ISBN 978-3-8487-3590-7

von personenbezogenen Daten einen besonders hohen Schutzbedarf: „Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können." Eine Verarbeitung dieser Datenkategorien beinhaltet also immer „erhebliche Risiken für die Grundrechte und Grundfreiheiten" betroffener Personen (ErwGr. 51 DS-GVO). Diese Daten haben daher immer einen hohen Schutzbedarf, bei in der Gesundheitsversorgung verarbeiteten Daten sind also auch entsprechende Anforderungen an die benötigte Fachkunde zu stellen.

Die erforderliche (Mindest-)Fachkunde ist natürlich gesetzlich geregelt, lässt sich aber auch aus den normativ geregelten Aufgaben direkt ableiten. Um beispielsweise das Risiko abschätzen zu können, muss der Datenschutzbeauftragte die Verarbeitung kennen und bewerten können, wozu natürlich entsprechende Fachkenntnisse der Informatik erforderlich sind. Wenn im Folgenden daher Anforderungen an die Fachkunde dargestellt werden, muss immer bedacht werden, dass aus konkreten geplanten und stattfindenden Verarbeitungen weitergehende Anforderungen entstehen können, denen – falls erforderlich - durch entsprechende Fortbildungen genügt werden muss.

Natürlich muss jeder Datenschutzbeauftragte im Gesundheitssektor die allgemeinen Anforderungen erfüllen, denen auch alle in anderen Gebieten tätigen Datenschutzbeauftragten genügen müssen. Im Parlamentsentwurf zur DS-GVO[9] findet sich in ErwGr. 75a:

> *„Der Datenschutzbeauftragte sollte zumindest die folgenden Qualifikationen besitzen: umfassende Kenntnisse des Datenschutzrechts und seiner Anwendung, einschließlich technischer und organisatorischer Maßnahmen und Verfahren; Beherrschung der fachlichen Anforderungen an den Datenschutz durch Technik, die datenschutzfreundlichen Voreinstellungen und die Datensicherheit; sektorspezifisches Wissen entsprechend der Größe des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters und der Sensibilität der zu verarbeitenden Daten; die Fähigkeit, Überprüfungen, Konsultationen, Dokumentationen und Protokolldateianalysen durchzuführen; sowie die Fähigkeit, mit Arbeitnehmervertretungen zu arbeiten."*

Auch wenn dieser Entwurf des EU Parlaments nicht in die finale Fassung übernommen wurde, wird deutlich, welche Anforderungen die europäischen Gesetzgeber im Sinn hatten. Zudem entsprechen diese Anforderungen regelhaft der Praxis[10]. Entsprechend sind an die Qualifikation eines Datenschutzbeauftragten zumindest zu stellen:

- Kenntnis das Datenschutzrechts; neben dem europäischen Datenschutzrecht muss auch das nationale Datenschutzrecht beherrscht werden. Gerade im Gesundheitswesen ist das Recht breit verteilt, sodass das erforderliche branchenspezifische Wissen des Datenschutzrechts umfangreich ausfällt.
- Anwendung einschließlich technischer und organisatorischer Maßnahmen und Verfahren; die technischen Maßnahmen erfordern entsprechende Fachkenntnisse insbesondere der Informatik. Nur mit entsprechenden informationstechnischen Kenntnissen können Maßnahmen in Bezug auf ihre Eignung beurteilt werden. Gleichermaßen ist für die Bewertung organisatorischer Maßnahmen entsprechendes betriebswirtschaftliches Wissen unabdingbar. Gerade bei technischen und organisatorischen Maßnahmen ist ein entsprechend tiefes branchenspezifisches Wissen unabdingbar, da im Gesundheitswesen eingesetzte informationstechnische Systeme oder Workflows sich naturgemäß gegenüber den Inhalten anderer Branchen unterscheiden.
- Sektorspezifisches Wissen ist insbesondere im Gesundheitswesen unabdingbar. Fehlerhafte Vorgaben können dafür sorgen, dass sensible Gesundheitsdaten nicht ausreichend geschützt werden oder – wohl schlimmer – durch Unkenntnis der Betriebsabläufe der im Behandlungsfall erforderliche Zugriff auf die Gesundheitsdaten nicht möglich ist, was im schlimmsten Fall den Tod eines Patienten bedeuten kann.
- Fähigkeit, Überprüfungen, Konsultationen, Dokumentationen und Protokolldateianalysen durchzuführen; eine der in Art. 39 DS-GVO definierten Aufgaben ist die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben, sodass Überprüfungen wie eine Auditierung einer Abteilung oder eines Auftragsverarbeiters sowie die Auswertung von Protokolldateien zu den Kernaufgaben von Datenschutzbeauftragten

[9] Europäisches Parlament: Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung). Stand 2013-11-21. Online, zitiert am 2021-01-16; verfügbar unter https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_DE.html?redirect

[10] So z. B. Ettig D., Bausewein C:. Art. 37, Rn. 17, 18. In: Tim Wybitul (Hrsg.) Handbuch EU-Datenschutzgrundverordnung. Deutscher Fachverlag GmbH, 1. Auflage 2017. ISBN 978-3-8005-1623-0

zählen. Natürlich gelten die in Art. 5 Abs. 2 DS-GVO verankerte Nachweispflicht auch in diesen Fällen, sodass eine entsprechende Dokumentation unerlässlich ist.

- Sozialkompetenz; nicht nur bei der Zusammenarbeit mit Arbeitnehmervertretern ist eine entsprechende Sozialkompetenz erforderlich. Auch bei der Erfüllung der in Art. 38 Abs. 4 DS-GVO enthaltenen Aufgabe als Ansprechpartner betroffener Personen zu agieren ist eine entsprechende Kompetenz erforderlich.
- Nicht ausdrücklich genannt aber unabdingbar ist natürlich die persönliche Zuverlässigkeit des Datenschutzbeauftragten[11]. Ein Datenschutzbeauftragter muss zur Erfüllung seiner Aufgabe geeignet sein, was bei einem derartigen Aufgabenspektrum natürlich beinhaltet, dass eine entsprechende Verschwiegenheit und Zuverlässigkeit gegeben ist: Integrität ist eine der wichtigsten Anforderungen an einen Datenschutzbeauftragten.

**Sektorspezifisches Wissen**

Branchenspezifisches Wissen ist für einen Datenschutzbeauftragten essenziell wichtig. Dies fängt schon mit der „Sprache" der Branche an. Nicht jeder wird „Leistungserbringer" mit Krankenhäusern, Arztpraxen oder Apotheken usw. gleichsetzen, nicht jeder wird wissen, dass Sozialämter und Krankenkassen „Leistungsträger" sind. Daher muss ein Datenschutzbeauftragter, der im Gesundheitswesen tätig wird, sich einen entsprechenden Sprachschatz aneignen.

Daneben sind natürlich Kenntnisse der Geschäftsabläufe wichtig. So ist es wichtig zu wissen, dass ein Geschäftsführer eines Krankenhauses den Chefärzten für bestimmte Belange keine Direktiven erlassen kann, sondern der Chefarzt selbst weisungsfrei agiert.

Dies ist immer im Bereich der Patientenbehandlung der Fall, aber je nach Chefarztvertrag kann dies auch Belange der Personalführung betreffen. Somit muss ein Datenschutzbeauftragter je nach Sachlage nicht nur die Geschäftsführung von seinem Vorgehen überzeugen, sondern auch alle involvierten Chefärztinnen und Chefärzte. Für einen Nicht-Arzt ist es mitunter nur schwer zu unterscheiden, welche Aufgaben Ärzte delegieren dürfen und welche nicht. Aufklärungsgespräche für medizinische Eingriffe sind grundsätzlich nicht delegierbar, Blutabnahmen an entsprechend ausgebildetes Personal schon, bei der Verabreichung von Medikamenten muss man mitunter zu erwartende Nebenwirkungen bei der Frage der Delegierbarkeit betrachten. Bei „Diagnose" wird gemeinhin davon ausgegangen, dass nur Ärzte Diagnosen stellen dürfen. Aber es gibt auch Pflegediagnosen.

Derartiges Wissen beeinflusst natürlich den Arbeitsalltag in medizinischen Versorgungseinrichtungen und muss berücksichtigt werden, wenn man über technische und organisatorische Maßnahmen nachdenkt und entscheidet. Der Einsatz von Bildschirmschonern beispielsweise kann in einem Bereich möglich sein, in einen anderen Bereich – je nach Umständen beispielsweise im Bereich der Operationssäle - sich aber verbieten.

**Rechtskunde**

Jeder Datenschutzbeauftragte muss über einschlägiges Wissen über das Datenschutzrecht verfügen, insbesondere sind hinsichtlich der DS-GVO vertiefte Kenntnisse notwendig, da diese das zentrale Regelwerk für jegliche Datenverarbeitung darstellt.[12] Neben der DS-GVO muss der Datenschutzbeauftragte auch über Kenntnisse nationaler Gesetze verfügen. Im Rahmen der Tätigkeit in Einrichtungen des Gesundheitswesens sind entsprechende Kenntnisse für die anzuwendenden Gesetze unabdingbar. Beispiele hierfür sind:

- für gesetzliche Kranken-, Unfall-, Pflegeversicherung: SGB I, SGB V, SGB VII, SGB X, SGB XI
- für Krankenhäuser: SGB V, Landesberufsordnung Ärzte, Landeskrankenhausgesetze, …
- für Arztpraxen: SGB V, Landesberufsordnung Ärzte, BDSG, …
- für Apotheken: SGB V, Landesberufsordnung Apotheker, ApBetrO, BDSG, …

Daneben gibt es natürlich diverse Gesetze und Verordnungen, die bestimmte Bereiche betreffen und weniger den Sektoren des Gesundheitsbereichs zuzuordnen sind. StrlSchG und StrlSchV adressieren in erster Linie Radiologen, unabhängig ob im niedergelassenen oder stationären Umfeld, aber einzelne Aspekte können auch Fachärzte mit Teilweiterbildungen in der

[11] Siehe z. B. LAG Mecklenburg-Vorpommern, Urt. v. 25.02.2020, Az. 5 Sa 108/19: Rn. 72. Online, zitiert am 2021-01-16; verfügbar unter http://www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml;jsessionid=0.jp35?showdoccase=1&doc.id=JURE200004715&st=ent

[12] Siehe auch Feil T (2019) Datenschutzgrundverordnung: Profil, Qualifikation und Aufgaben eines Datenschutzbeauftragten nach der DS-GVO. BBP: 26-28

Radiologie betreffen, etwa einige Orthopäden. Auch ist der Anwendungsbereich der Gesetze mitunter speziell. Für die in § 35 Abs. 1 SGB I genannten Sozialgeheimnisträger wie Krankenkassen wird – abgesehen von der DS-GVO – Datenschutz abschließend in den Sozialbüchern geregelt, die Anwendbarkeit anderer Regulierungen wird letztlich ausgeschlossen. Daher findet sich in § 81 Abs. 4 SGB X für die in § 35 SGB I genannten Stellen ein Verweis auf die §§ 5 bis 7 BDSG; ohne diesen Verweis wären die Regelungen des BDSG bezüglich Datenschutzbeauftragte nicht anwendbar.

**Informationstechnisches Know-how**

Ohne tiefergehende EDV-Kenntnisse kann ein Datenschutzbeauftragter seine Aufgaben in Unternehmen oder Behörden nicht erfüllen. Dies beinhaltet natürlich auch besondere Kenntnisse in der IT-Sicherheit etwa zur Kryptografie oder Netzwerksicherheit. Zudem muss er ein Grundwissen für die Standards wie ISO 27001 und speziell im Gesundheitswesen die ISO 27799 mitbringen. Daneben wird ein fundiertes Wissen um die eingesetzten informationstechnischen Systeme für den jeweiligen Bereich benötigt. Im Gesundheitswesen sind dies unter anderen Krankenhausinformationssysteme, Praxisverwaltungssysteme, Bildverwaltungssysteme (PACS) oder Laborinformationssysteme. Hierzu werden nicht nur Kenntnisse über Datenbankmanagementsysteme oder Protokollierung benötigt, sondern auch Kenntnisse über IT-Schnittstellen, mit denen im Gesundheitswesen Daten verarbeitet werden. Prominenteste Beispiele für derartig genutzte Standards sind HL7 v2, HL7 CDA, HL7 FHIR und DICOM. Daneben sind entsprechende Kenntnisse des medizinischen Workflows unverzichtbar, wie sie von der internationalen Organisation „Integrating the Healthcare Enterprise" (IHE) publiziert werden; letztlich wird durch die IHE-Workflow-Beschreibungen dargestellt, wie (internationale) Standards sinnvoll und sicher in der medizinischen Versorgung eingesetzt werden können.

**Betriebswirtschaft**

In der DS-GVO wird an verschiedenen Stellen gefordert, dass auch betriebswirtschaftliche Erwägungen berücksichtigt werden müssen. Art. 32 Abs. 1 DS-GVO verlangt beispielsweise die Berücksichtigung von Implementierungskosten bei der Auswahl geeigneter technisch-organisatorischer Maßnahmen. Daher muss ein Datenschutzbeauftragter zwingend in diesem Umfeld entsprechende Kenntnisse besitzen. Im Rahmen der Gesundheitsversorgung muss er natürlich insbesondere Kenntnisse darüber besitzen, wie dieses in Deutschland finanziert wird.

Die Gesundheitsversorgung ist ein gesetzlich regulierter Markt. Marktteilnehmer wie Arztpraxen oder Krankenhäuser können bei Mehrkosten nicht die Preise erhöhen und so die Einnahmeseite beeinflussen. Daher stehen gesundheitsversorgenden Einrichtungen nur sehr begrenzte finanzielle Mittel zur Erfüllung ihrer Pflichten zur Verfügung.

Beispiel Krankenhaus[13]: Die Bundesländer sind für die Finanzierung der Krankenhausinvestitionen zuständig, also für Kosten wie Neubeschaffung von Anlagegütern oder ähnliche Investitionen. Die Krankenkassen tragen die Kosten, die unmittelbar im Zusammenhang mit der Krankenbehandlung entstehen, also Kosten für Medikation oder für die Verpflegung von Patienten. Träger von Krankenhäusern wie Kommunen, Wohlfahrtsverbände (aber natürlich auch private Träger) gleichen Defizite durch Zuschüsse aus.

Die Finanzierung von Investitionen wird grundlegend bundesgesetzlich im KHG geregelt, landesspezifisch erfolgt die Ausgestaltung durch die jeweiligen Landeskrankenhausgesetze. Ob und inwieweit die Länder ihrer Pflicht zur Investitionsfinanzierung nachkommen, ist in erster Linie von der Haushaltslage und dem politischen Willen der Landesregierungen abhängig: Experten schätzen, dass bei Krankenhäusern aufgrund der fehlenden Finanzierung der Länder mittlerweile eine Förderlücke von fast elf Milliarden Euro besteht. Die meisten Länder erfüllen ihre diesbezüglichen Pflichten nicht oder nur unzureichend. Somit haben Krankenhäuser eher regelhaft eine Finanzierungslücke, sodass der Einsatz finanzieller Mittel grundsätzlich einen Konkurrenzkampf verschiedener Zwecke wie beispielsweise Patientenversorgung vs. IT-Sicherheit/Datenschutz darstellt.

Diese und andere Hintergründe müssen natürlich einem Datenschutzbeauftragten bekannt sein, damit diese Einflussgrößen bei den Entscheidungen entsprechend berücksichtigt werden können.

[13] Kurze Beschreibung der für Krankenhäuser geltenden dualen Finanzierung z. B. unter Bundeszentrale für politische Bildung: Krankenhausplanung und -finanzierung. Stand 2012-03-01. Online, zitiert am 2021-01-16; verfügbar unter https://www.bpb.de/politik/innenpolitik/gesundheitspolitik/72022/krankenhausplanung-und-finanzierung

**Sozialkompetenz**

Gerade in der Gesundheitsversorgung dreht es sich um besonders sensible Daten. Patienten haben ein Recht darauf, dass ihre personenbezogenen Daten entsprechend sorgfältig behandelt werden. Ein Bekanntwerden der medizinischen Informationen kann zu einem Jobverlust, zu einer gesellschaftlichen Stigmatisierung oder zu anderen negativen Auswirkungen führen. Derartige Sorgen können für manche Patienten belastend sein. Entsprechend umsichtig muss ein Datenschutzbeauftragter mit Anfragen von Patienten umgehen.

Aber auch das Personal in der Gesundheitsversorgung muss entsprechend begleitet werden. Gerade das Pflegepersonal bekam in den vergangenen bekam in den vergangenen Jahren immer mehr administrative Tätigkeiten zugewiesen, sodass die für die Versorgung von Patienten zur Verfügung stehende Zeit sich stetig verringerte. Maßnahmen zur Gewährleistung des Datenschutzes müssen dies berücksichtigen und den Arbeitsablauf so gering wie möglich stören, zugleich müssen entsprechende Erläuterungen die Notwendigkeit der Maßnahmen begleiten, damit das medizinische Personal die Maßnahmen mitträgt. Ähnliches gilt auch für andere Sektoren wie dem Bankenumfeld, nur stehen in diesen Sektoren regelhaft nicht Menschenleben zur Disposition – genau mit dieser Argumentation muss sich ein Datenschutzbeauftragter im Gesundheitswesen auseinandersetzen: "Willst Du Menschenleben riskieren?" Nicht nur in diesen Situationen ist eine entsprechende Sozialkompetenz des Datenschutzbeauftragten unabdingbar.

**… und die Aufsichtsbehörden?**

Die Datenschutz-Aufsichtsbehörden müssen natürlich auch über Personal verfügen, deren Fachkenntnisse den dargestellten Anforderungen entsprechen. Letztlich können die Aufsichtsbehörden ohne entsprechend qualifiziertes Personal ihren in Art. 57 DS-GVO verankerten Pflichten nicht genügen: Eine Beratungsfunktion (Art. 57 Abs. 1 lit. c) oder die Beurteilung von Verhaltensregeln (Art. 57 Abs. 1 lit. m) sind ohne Branchenkenntnisse schlichtweg nicht möglich. Daher müssen die Aufsichtsbehörden seitens Bund und Länder die Mittel erhalten, entsprechendes Personal einzustellen und zu vergüten.

## Extern oder intern benannt?

Entsprechend Art. 37 Abs. 6 DS-GVO kann sowohl die Benennung einer beim Verantwortlichen beschäftigten Person erfolgen (interne Benennung) als auch im Rahmen eines Dienstleistungsvertrages (externe Benennung). Beides hat Vor- und Nachteile.

Ein externer Datenschutzbeauftragter, der verschiedene Kunden in derselben Branche betreut, verfügt in der Regel über einen breiten Erfahrungsschatz und kann häufig bei anderen Kunden bereits erprobte Lösungen anbieten.

Ein interner Datenschutzbeauftragter hingegen ist regelhaft tiefer in die Arbeitsabläufe integriert und kann Fragestellungen aus einem internen Blickwinkel betrachten, die einem externen Datenschutzbeauftragten fehlen (müssen); zudem können Lösungen stärker die individuellen Arbeitsabläufe berücksichtigen.

Letztlich kann nur individuell entschieden werden, ob ein interner oder externer Datenschutzbeauftragter für den jeweiligen Verantwortlichen die bessere Lösung darstellt. Arztpraxen werden eher externe Datenschutzbeauftragte, größere Kliniken oder Krankenkassen eher einen internen Datenschutzbeauftragten benennen.

## Juristische Person als Datenschutzbeauftragter?

In der DS-GVO wird nicht explizit geregelt, ob ein Datenschutzbeauftragter eine natürliche Person sein muss oder juristische Personen ebenfalls zum Datenschutzbeauftragten benannt werden können. Die Anforderungen, die an eine Qualifikation gestellt werden, kann nur eine natürliche Person erfüllen, sodass der europäische Gesetzgeber vermutlich natürliche Personen adressieren wollte. Ohne ausdrückliche Regelung kann die Frage nicht abschließend beantwortet werden.

Vereinzelt wird aus Art. 37 Abs. 5 DS-GVO abgeleitet, dass nur eine natürliche Person benannt werden kann, weil juristische Personen die berufliche Qualifikation nicht aufweisen können[14]. Auch sehen einige Meldeformulare von Aufsichtsbehörden nur Meldungen von natürlichen Personen vor[15].

Der Europäische Datenschutzausschuss hinge-

[14] So z. B. Ettig D., Bausewein C:. Art. 37, Rn. 17, 18. In: Tim Wybitul (Hrsg.) Handbuch EU-Datenschutzgrundverordnung. Deutscher Fachverlag GmbH, 1. Auflage 2017. ISBN 978-3-8005-1623-0

[15] So z.B.
Berlin: https://www.datenschutz-berlin.de/meldeformular/
BW: https://www.baden-wuerttemberg.datenschutz.de/dsb-online-melden/
Hessen: https://datenschutz.hessen.de/service/benennung-eines-datenschutzbeauftragten
RP: https://www.datenschutz.rlp.de/de/themenfelder-themen/online-services/meldeformular-datenschutzbeauftragter-gem-art-37-abs-7-ds-gvo/

gen geht in der von der Artikel-29-Datenschutzgruppe übernommenen Leitlinie 243 davon aus, dass „die Funktion eines DSB auf Grundlage eines Dienstleistungsvertrags ausgeübt werden kann, der mit einer natürlichen oder juristischen Person geschlossen wird“[16]. Allerdings wird dann vom Europäischen Datenschutzausschuss die Anforderung erhoben, dass *jedes* Mitglied der juristischen Person, welche die Funktionen eines Datenschutzbeauftragten wahrnimmt, sämtliche Anforderungen erfüllt.

## Der Konzerndatenschutzbeauftragte

Natürlich gibt es auch im Gesundheitswesen Konzerne, zum Beispiel Krankenhausketten. Entsprechend Art. 37 Abs. 2 DS-GVO darf eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

Nach Ansicht des Europäischen Datenschutzausschusses gilt das Kriterium der „leichten Erreichbarkeit“ des Datenschutzbeauftragten sowohl für die Aufgabe als Ansprechpartner für Betroffene und Aufsichtsbehörden zu agieren, aber auch für die Aufgabe als einrichtungsinterner Ansprechpartner[17]. Durch entsprechende Bereitstellung der Kontaktdaten kann die (leichte) Erreichbarkeit des Datenschutzbeauftragten sowohl für betroffene Personen als auch für die Aufsichtsbehörden und ebenfalls für die Beschäftigten der Niederlassungen gewährleistet werden.

Allerdings muss beachtet werden, dass bei der Benennung eines Datenschutzbeauftragten für eine Unternehmensgruppe alle Anforderungen erfüllt sein müssen, insbesondere das Wissen um die Verarbeitungsprozesse. Gerade im Gesundheitswesen können sich in der Patientenversorgung deutliche Unterschiede zwischen verschiedenen Versorgungseinrichtungen innerhalb eines Konzerns ergeben. So kann eine medizinische Versorgungseinrichtung radiologische Untersuchungen selbst durchführen, bei einer anderen muss dies hingegen mindestens teilweise teleradiologisch erfolgen, was entsprechende Prozessanpassungen erfordert und aus Datenschutzsicht entsprechend betrachtet werden muss. Auch wenn ein Datenschutzbeauftragter für die gesamte Unternehmensgruppe benannt werden dürfte, kann sich aus den vorhandenen Bedürfnissen ergeben, dass einzelne Bereiche der Unternehmensgruppe einen eigenen Datenschutzbeauftragten benötigen.

In der Gesundheitsversorgung wird die Benennung eines Datenschutzbeauftragten in der jeweiligen Einrichtung eher die Regel als die Ausnahme sein. Dennoch kann die Benennung eines Konzerndatenschutzbeauftragten sinnvoll sein, da so zentrale Fragen wie

- Etablierung einer Datenschutzphilosophie im Unternehmen zur Darstellung der Ziele eines einheitlichen Datenschutzniveaus in der Unternehmensgruppe,
- Ausbildung einer unternehmensweiten Datenschutzstrategie zur Erreichung der in der Datenschutz-Philosophie festgelegten Ziele,
- Analyse bundesgesetzlicher Vorgaben und Erarbeitung von Handlungsempfehlungen für die Organisationseinheiten,
- Entwicklung von Umsetzungshilfen wie Templates für Datenschutz-Folgenabschätzung, Risikobewertung oder Datenschutzkonzept,
- Etablierung eines einheitlichen Berichtswesens innerhalb der Unternehmensgruppe,
- Organisationsfragen wie die Weiterbildung der im Konzern benannten Datenschutzbeauftragten

adressiert werden können. So wird einerseits eine einheitliche Konzernstrategie ermöglicht, andererseit bei den dezentralen Datenschutz-Einheiten die Arbeit verringert und zugleich die erforderliche Individualität bei der Patientenversorgung durch die jeweilige Einheit ermöglicht.

## Fazit

Betrachtet man die Anforderungen an einen Datenschutzbeauftragten, so wird man schnell feststellen, dass es keine Person gibt, die alle Anforderungen erfüllt. Bei einem im Gesundheitswesen tätigen Datenschutzbeauftragten würde dies den erfolgreichen Abschluss der folgenden Studiengänge bedeuten: Medizin (sektorspezifisches Wissen), Informatik (technische Kenntnisse), Betriebswirtschaft (Bewertung von Maßnahmen anhand Implementierungskosten)

[16] Artikel-29-Datenschutzgruppe: Leitlinie 243, Seite 14, Kapitel „Im Rahmen eines Dienstleistungsvertrags beschäftigte DSB“. Verfügbarkeit siehe Fußnote 1

[17] Artikel-29-Datenschutzgruppe: Leitlinie 243, Kapitel 2.3. Verfügbarkeit siehe Fußnote 1

und Rechtskunde (Datenschutzrecht). Eine entsprechende Anzahl von Personen mit Abschlüssen in allen vier Bereichen existiert nicht, was natürlich dem europäischen Gesetzgeber bei der Gestaltung der DS-GVO bekannt war.

In der Praxis muss es daher genügen, wenn der Datenschutzbeauftragte Teilbereiche abdecken kann und ihm für weitere Themen entsprechend fachkundige Mitarbeiter zur Verfügung stehen. Auch die Möglichkeit, bei besonders komplizierten Herausforderungen externe Kompetenz hinzuziehen, kann im Einzelfall unzureichende Qualifikation des Datenschutzbeauftragten ausgleichen.

Aber: Der Datenschutzbeauftragte muss selbst und unabhängig in der Lage sein, die Verarbeitungsvorgänge – wenn auch nicht in der Tiefe – zu verstehen und zu bewerten. Ein Jurastudium oder ein Informatikstudium alleine reicht für die Qualifikation zum Datenschutzbeauftragten nicht aus, Grundkompetenzen müssen in allen Wissensgebieten vorhanden sein, insbesondere natürlich im sektorspezifischen Umfeld.

Der BvD veröffentlichte schon vor einiger Zeit das berufliche Leitbild der Datenschutzbeauftragten. Die aktuelle Version 4 aus dem Jahr 2018 ist an die Vorgaben der DS-GVO angepasst und zudem zweisprachig verfügbar[18]. In diesem Leitbild werden persönliche und fachliche Voraussetzungen dargestellt, aber auch Aufgaben und Anforderungen beschrieben. Verantwortliche, die dieses Berufsbild als Grundlage für eine Benennung nehmen, sind hinsichtlich der Erfüllung der gesetzlichen Anforderungen bestens beraten.

Hat man sich in die Thematik eingearbeitet, erwartet uns Datenschutzbeauftragte jedoch ein sehr spannendes Feld mit interessanten, herausfordernden Fragestellungen und zumeist sehr engagierten Mitstreitern aus dem fachlichen Umfeld. Mein persönliches Fazit nach gut 30 Jahren: Gut, dass wir uns gefunden haben!

## Abkürzungen

| | |
|---|---|
| **ApBetrO** | Verordnung über den Betrieb von Apotheken (Apothekenbetriebsordnung) |
| **BDSG** | Bundesdatenschutzgesetz |
| **DICOM** | Digital Imaging and Communications in Medicine |
| **DS-GVO** | Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (Datenschutz-Grundverordnung) |
| **ErwGr** | Erwägungsgrund/Erwägungsgründe |
| **GG** | Grundgesetz |
| **HL7** | Health Level 7 |
| **ISO** | International Organization for Standardization |
| **KHG** | Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze (Krankenhausfinanzierungsgesetz) |
| **KHG** | Krankenhausgesetz |
| **lit.** | littera (lat. „Buchstabe“) |
| **PACS** | Picture Archiving and Communication System |
| **Rn.** | Randnote, -nummer, -zahl, -ziffer |
| **SGB** | Sozialgesetzbuch |
| **StrlSchG** | Gesetz zum Schutz vor der schädlichen Wirkung ionisierender Strahlung (Strahlenschutzgesetz) |
| **StrlSchV** | Verordnung zum Schutz vor der schädlichen Wirkung ionisierender Strahlung (Strahlenschutzverordnung) |


## Über den Autor

**Dr. Bernd Schütze**

beschäftigt sich seit 1995 mit den datenschutzrechtlichen Aspekten innerhalb der Gesundheitsversorgung. Nach gut dreißigjähriger beruflicher Tätigkeit in verschiedenen Krankenhäusern arbeitet Dr. Schütze seit 2014 als „Senior Experte Medical Data Security“ bei der Deutschen Telekom Healthcare and Security Solutions GmbH. Als Lehrbeauftragter ist er zudem an verschiedenen Hochschulen tätig und veröffentlicht regelmäßig Beiträge in Büchern und Fachzeitschriften.

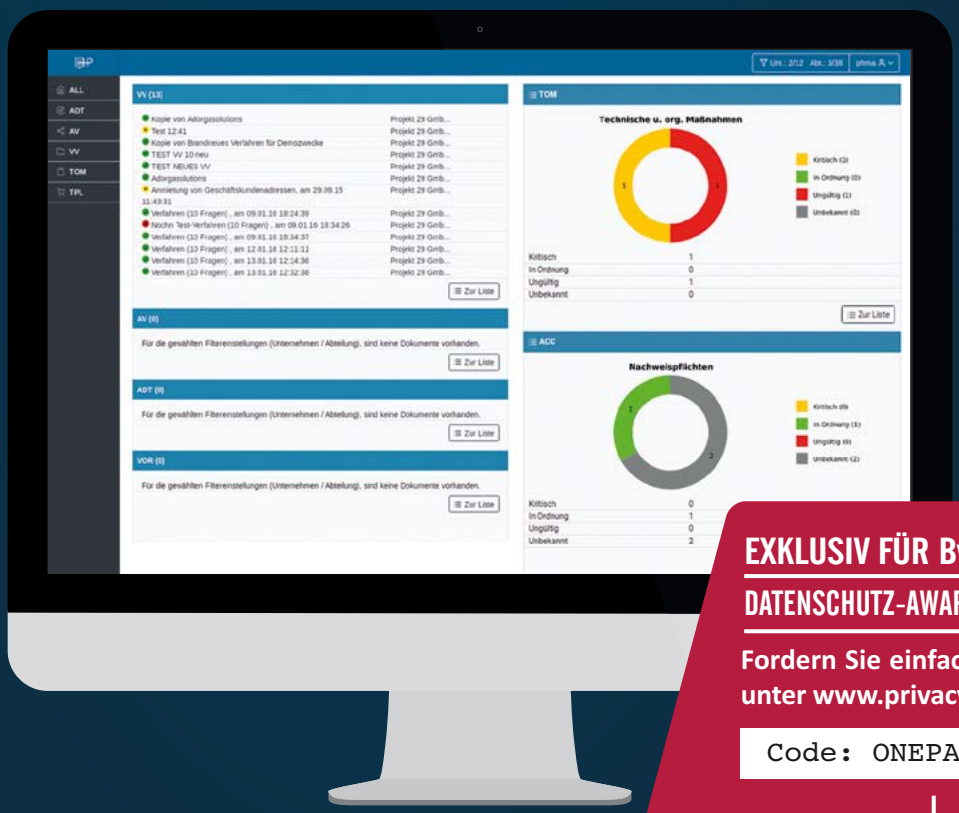

[18] Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.: Das berufliche Leitbild der Datenschutzbeauftragten. Online, zitiert am 2021-01-12; verfügbar unter https://www.bvdnet.de/berufsbild/

Anzeige

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

# PRIVACYSOFT

## IHR DSB-MULTI-TOOL FÜR ALLE AUFGABEN IM DATENSCHUTZMANAGEMENT




**EXKLUSIV FÜR BvD-MITGLIEDER**

**DATENSCHUTZ-AWARENESS-ONEPAGER**

**Fordern Sie einfach und kostenlos unter www.privacysoft.de an.**

Code: ONEPAGERBVD2021

BvD e.V. MITGLIED
DATENSCHUTZ GESTALTEN

- KOMPLETTE DATENSCHUTZDOKUMENTATION
- EXTRA VORLAGEN UND CHECKLISTEN
- NEUES AUDITMODUL
- BEWÄHRTE ONLINE-SCHULUNGEN
- MEHRSPRACHIG // DE / EN / FR
- ZUSAMMENARBEIT // TICKET

Ab sofort haben Sie die Möglichkeit eine ganz persönliche kostenlose Präsentation dieser praxisbewährten Datenschutzmanagement Software zu bekommen. Wir verschaffen Ihnen bei einem kleinen Rundgang durch unsere Lösung spannende Einblicke und interessante Perspektiven.

**Bitte hinterlassen Sie uns Ihren Terminwunsch im Kontaktformular unter www.privacysoft.de.**

**Oder rufen Sie einfach kurz bei uns an: 0941-29 86 93-0**

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

DATENSCHUTZ KNOW-HOW SEIT 1996

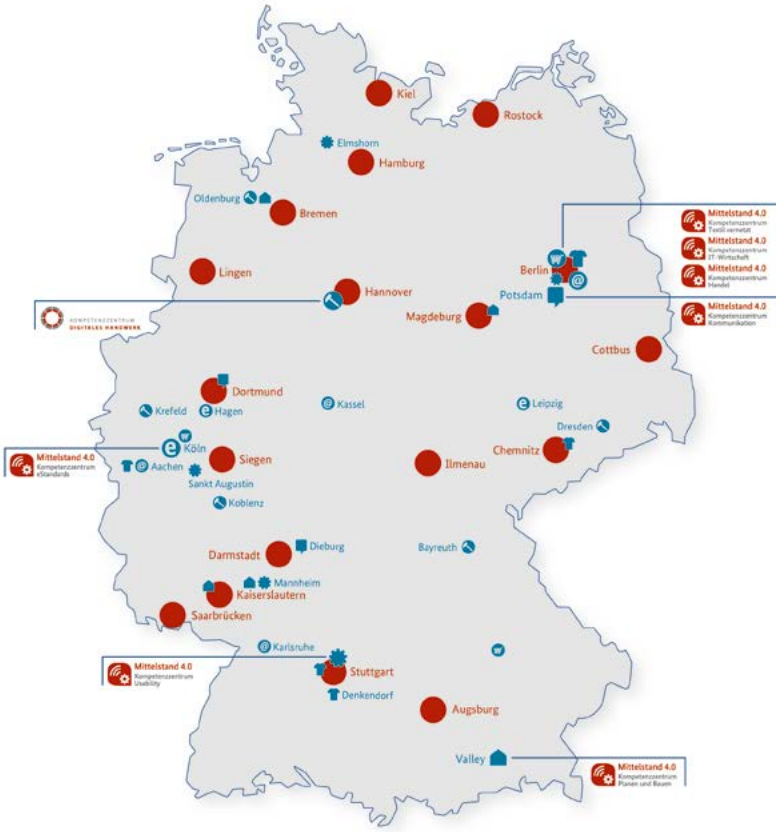
# MITTELSTAND-DIGITAL

## Kompetenzzentren unterstützen den Mittelstand bei der Digitalisierung

Christian Munk

Der Förderschwerpunkt Mittelstand-Digital des Bundesministeriums für Wirtschaft und Energie bietet insbesondere kleinen und mittleren Unternehmen sowie dem Handwerk mit den drei Säulen Mittelstand-4.0-Kompetenzzentren, Initiative IT-Sicherheit in der Wirtschaft und dem Förderprogramm Digital Jetzt umfassende Informations- und Unterstützungsangebote bei der Digitalisierung entlang der Befähigungskette. Fragen der Daten- bzw. IT-Sicherheit werden als Querschnittsthema in allen drei Säulen aufgegriffen. Mit diesem Artikel über die Mittelstand-4.0-Kompetenzzentren startet unsere Serie über Mittelstand-Digital. Die Initiative IT-Sicherheit in der Wirtschaft und das Förderprogramm Digital Jetzt stellen wir in den nächsten Ausgaben der BvD-News vor.

Die regionalen Mittelstand 4.0-Kompetenzzentren und Themenzentren mit ihren Stützpunkten




### Mittelstand-4.0-Kompetenzzentren

Digitalisierung und Vernetzung betreffen alle Branchen unserer Wirtschaft und Unternehmen jeder Größe. Ob anspruchsvollere Kunden oder neue Wettbewerber – Digitalisierungsprojekte sind oftmals von zentraler Bedeutung, um im Wettbewerb weiter bestehen zu können. Sie bieten für Unternehmen große Chancen und sind mitunter enorme Herausforderung zugleich. Kleine und mittlere Unternehmen werden aufgrund ihrer oft geringeren Ressourcen häufig besonders gefordert. Deshalb fördert das Bundesministerium für Wirtschaft und Energie im Förderschwerpunkt Mittelstand-Digital praxisnahe Unterstützung für digitale Transformation: 26 Mittelstand-4.0-Kompetenzzentren mit mehr als 130 Standorten sind seit 2015 bundesweit in vielen Regionen entstanden. Die meisten dieser Zentren verstehen sich als Generalisten in Sachen Digitalisierung – acht Zentren bieten fachliche Spezialisierungen zu den Themen Digitales Handwerk, eStandards, Handel, IT-Wirtschaft, Kommunikation, Planen und Bauen, Textil vernetzt und Usability an.

Die Mittelstand-4.0-Kompetenzzentren bieten kompetente und kostenlose Unterstützung. Ob Workshops, Schulungen, Praxistests, Webinare oder Sprechstunden: Mit anbieterneutralen und auf kleine und mittlere Unternehmen zugeschnittenen Informationen werden Unternehmen befähigt, den Stand der eigenen Digitalisierung einzuschätzen und gemeinsam mit den Zentren einen individuellen Digitalisierungsfahrplan zu entwickeln. Die Zentren unterstützen zudem bei der Auswahl und Umsetzung geeigneter Maßnahmen. Auch bei Fragen, ob eine technische Lösung wirtschaftlich sinnvoll ist und welche Sicherheitsaspekte berücksichtigt werden müssen, stehen sie den Unternehmen zur Seite. Um Digitalisierung mit ihren verschiedensten Facetten erlebbar zu machen, haben die Kompetenzzentren zahlreiche Demonstrationsorte eingerichtet: So lässt sich zum Beispiel in Augsburg die Lernfabrik für vernetzte Produktion, in Berlin der Erlebnisraum Gemeinsam Digital oder in Chemnitz IT-Sicherheit in der Testumgebung Live-Hacking hautnah erfahren.

## Schwerpunkt Künstliche Intelligenz

Die Digitalisierung entwickelt sich rasant fort. Die Kompetenzzentren bleiben deshalb auch bei neuen Technologien wie der Künstlichen Intelligenz (KI) für den Mittelstand am Ball: Im Zuge der Umsetzung der KI-Strategie der Bundesregierung ist seit Mitte 2019 das KI-Trainer-Programm bei den Mittelstand-4.0-Kompetenzzentren angesiedelt. Über 70 KI-Trainer vermitteln kleinen und mittleren Unternehmen die Grundlagen zu dieser Schlüsseltechnologie. Mittelstand und Handwerk für die technologischen und wirtschaftlichen Chancen und Herausforderungen Künstlicher Intelligenz zu informieren, gehört ebenso zu den Aufgaben der KI-Trainer wie konkrete Anwendungsmöglichkeiten zu identifizieren und ihre Umsetzung zu unterstützen. Potenzielle Anwendungsmöglichkeiten für Künstliche Intelligenz bieten sich bei Mittelstand und Handwerk entlang der gesamten Wertschöpfungskette.

Intelligente Assistenzsysteme, industrielle Analyse sowie intelligente Produkte und Services stehen dabei besonders im Fokus. Das KI-Trainer-Programm soll erweitert und noch stärker in die Fläche ausgedehnt werden. Die Mittelstand-4.0-Kompetenzzentren initiieren darüber hinaus Train-the-Trainer-Programme für Multiplikatoren in Kammern und Verbänden.

## IT- und Datensicherheit als Querschnittsthemen im Mittelstand-4.0-Netzwerk

Die zunehmende Digitalisierung stellt immer größere Ansprüche an die IT-Sicherheit im Mittelstand, um IT-Systeme stets funktionsfähig und sicher vorhalten zu können. Zudem wirft die Digitalisierung oftmals zahlreiche Rechtsfragen auf: Wie können Unternehmen personenbezogene Daten rechtskonform verarbeiten? Wer haftet im Falle von Datenverlust oder bei Cyberkriminalität? Diese und weitere Fragen werden bei Mittelstand-Digital im Bereich Recht 4.0 behandelt.

Im digitalen Zeitalter sind Daten die zentralen Güter: Datenschutz, Datenhoheit oder Datenhaftung werden oftmals diskutiert. Auch neue Formen der Zusammenarbeit zwischen Menschen und intelligent arbeitenden Maschinen können zahlreiche Rechtsfragen aufwerfen. Technologische Entwicklungen haben entsprechende rechtliche Fortentwicklungen zur Folge: Die EU-Datenschutzgrundverordnung (DSGVO), das Netzwerkdurchsetzungsgesetz (NetzDG), das IT-Sicherheitsgesetz (IT-SiG), das derzeit novelliert wird (IT-SiG 2.0), oder das Geschäftsgeheimnisgesetz (GeschGehG) stellen Mittelstand und Handwerk bei Digitalisierungsbestrebungen vor neue rechtliche Herausforderungen. Kleine und mittlere Unternehmen sehen sich zudem oft damit konfrontiert, ein Informationssicherheitskonzept erstellen zu müssen. Die Mittelstand-4.0-Kompetenzzentren liefern Antworten auf erste Fragen und leisten praktische Hilfestellung.

IT-Sicherheit wird auch aus einer technischen Perspektive von zahlreichen Kompetenzzentren als Querschnittsthema aufgegriffen. Denn mit sämtlichen Digitalisierungsbestrebungen sollte sie von Beginn an umfassend mitgedacht werden (Security by Design beziehungsweise Security by Default). Sorgen um IT-Sicherheit gelten zudem als Hemmnis für Digitalisierung: 15 Prozent der deutschen Unternehmen führen Sicherheitsbedenken als einen der Gründe gegen Digitalisierung an. Die Zentren sensibilisieren Mittelstand und Handwerk für IT-Sicherheit und unterstützen bei der Auswahl geeigneter Maßnahmen. Wie auch Studien aus der Initiative IT-Sicherheit in der Wirtschaft wiederholt zeigen, ist der Faktor Mensch mitentscheidend für ein hohes Sicherheitsniveau. Mitarbeiterinnen und Mitarbeiter zu sensibilisieren und zu schulen, unterstützen die Kompetenzzentren ebenfalls durch auf kleine und mittlere Unternehmen zugeschnittene Materialien. Die IT-Sicherheit ist – genauso wie die Informationstechnik an sich – durch Schnelllebigkeit gekennzeichnet. Deshalb haben sich Experten aus zahlreichen Kompetenzzentren in der Arbeitsgruppe IT-Sicherheit zusammengeschlossen, um gemeinsam dieses herausfordernde Thema effektiv zu bearbeiten.

## Aus den Mittelstand-4.0-Kompetenzzentren wird das Netzwerk Mittelstand-Digital

Seit die ersten Mittelstand-4.0-Kompetenzzentren ab 2015 entstanden sind, haben sich die technischen Herausforderungen der Digitalisierung und die Förderlandschaften in Bund und Ländern wesentlich verändert. Mit einer neuen Förderbekanntmachung hat das Bundesministerium für Wirtschaft und Energie den Startschuss für eine Neustrukturierung des bewährten Netzwerks gegeben. Künftig sollen auch Zukunftsthemen wie Nachhaltigkeit, Energie- und Ressourceneffizienz oder Angebote für den Dienstleistungssektor stärker aufgegriffen werden. Das Netzwerk der Kompetenzzentren soll gestärkt, strategische Leuchtturmprojekte noch besser gefördert und ein größerer Fokus auf unternehmensspezifische Leistungen gelegt werden. Die Mittelstand-Digital-Zentren werden die Arbeit der Mittelstand-4.0-Kompetenzzentren neu akzentuiert fortführen.

## Fazit und Ausblick

Die bestehenden Mittelstand-4.0-Kompetenzzentren und die Kompetenzzentren des künftigen Mittelstand-Digital-Netzwerks unterstützen Mittelstand und Handwerk bei der Digitalisierung und Fragen der IT-Sicherheit. Auch zu damit einhergehenden rechtlichen Fragestellungen, etwa zu Fragen des Datenschutzes, der Datenhoheit oder der Datenhaftung, geben sie zum Beispiel durch Materialien erste Hilfestellungen. In der nächsten Ausgabe der BvD-News stellen wir die Initiative IT-Sicherheit in der Wirtschaft als zweite Säule des Förderschwerpunkts Mittelstand-Digital des Bundesministeriums für Wirtschaft und Energie vor.

Mehr Informationen:
www.mittelstand-digital.de

Recht 4.0 bei Mittelstand-Digital:
https://www.mittelstand-digital.de/MD/Redaktion/DE/Dossiers/A-Z/recht.html

## Über den Autor

**Christian Munk**
Bundesministerium für Wirtschaft und Energie,
Referent im Referat Mittelstand-Digital.

Mittelstand 4.0
Kompetenzzentren
Deutschlandweit

Anzeige

# 100. DATENSCHUTZKONFERENZ – DIE WICHTIGSTEN ERGEBNISSE UND ENTSCHEIDUNGEN IM ÜBERBLICK

Andreas Schurig

Es gibt Ereignisse, deren historische Bedeutung uns erst Jahrzehnte später so richtig bewusst wird. Die Begebenheiten am 7. Dezember 1978 zählen aus Sicht von Datenschützern mit Sicherheit dazu. An jenem Donnerstag vor über 42 Jahren trafen sich in Hessen erstmalig die staatlichen Datenschutzbeauftragten des Bundes und der Länder – der Geburtstag der Datenschutzkonferenz (DSK). Rechtliche Änderungen haben dazu geführt, dass die Aufgaben und Zuständigkeiten der Datenschutzbehörden über die Jahrzehnte gewachsen sind. Die Themenvielfalt und die Anzahl der Tagesordnungspunkte aktueller DSK-Sitzungen verdeutlichen diese Entwicklung. Heute stellt dieses Gremium nicht nur Forderungen, sondern unterstützt mit seiner Arbeit Wirtschaft und Behörden gleichermaßen. Über die vergangenen vier Jahrzehnte hat sich vieles bei der DSK weiterentwickelt, der Leitgedanke ist jedoch stets derselbe geblieben: die Datenschutzgrundrechte der Menschen zu wahren und zu schützen. Daran hat auch die Coronavirus-Pandemie nichts geändert – ungeachtet der Tatsache, dass die 100. Datenschutzkonferenz am 25. und 26. November 2020 erstmalig als digitale Tagung stattfand. Nachfolgend sind die wichtigsten Ergebnisse und Entscheidungen zusammengefasst.

## Beschluss zum Einsatz von Windows 10 Enterprise

Erneut befasste sich die Konferenz sowohl mit den Telemetriefunktionen von Microsoft Windows 10, Version Enterprise, als auch mit den durch Microsoft zu MS Office 365 angekündigten Verbesserungen des Datenschutzes. Zu den Telemetriefunktionen hatte eine DSK-Arbeitsgruppe in drei Testszenarien zuvor festgestellt, dass Verantwortliche beim Einsatz der Enterprise-Version die Telemetriestufe „Security" nutzen müssen. Sie sind in der Pflicht, vertraglich, technisch oder organisatorisch sicherzustellen, dass keine Übermittlung personenbezogener Telemetrie-Daten an Microsoft stattfindet.

Angesichts offener Fragen, die sich auch aus der SiSyPHuS-Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) ergeben, sowie angesichts des Umstands, dass die vorliegenden Untersuchungen auf Grund laufender Fortentwicklungen der Software natürlich nur eine Momentaufnahme darstellen, können die bisherigen Untersuchungen Verantwortliche nicht abschließend von ihrer Prüf- und Nachweispflicht (Art. 5 Abs. 2 DSGVO) für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten entlasten. Dies gilt erst recht für Verantwortliche, die Windows 10 in der Pro- und Home-Edition einsetzen, in denen die Telemetriestufe derzeit nicht auf Security gesetzt werden kann. In diesen Fällen bleiben ohnehin andere Maßnahmen zur Unterbindung etwaiger Übermittlungen personenbezogener Telemetriedaten zu prüfen oder die Rechtmäßigkeit der Übermittlung nachzuweisen.

Deshalb sollte Windows 10 in allen angebotenen Editionen die Möglichkeit bieten, die Telemetriedatenverarbeitung durch Konfiguration zu deaktivieren. Dazu und zu den aufgezeigten verbliebenen Unwägbarkeiten sowie zum MS Office 365 werden die Datenschutzaufsichtsbehörden das weitere Gespräch mit Microsoft führen.

## Über die Datenschutzkonferenz

Die Datenschutzkonferenz besteht aus den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Sie hat die Aufgabe die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

Die DSK tagt jährlich unter wechselndem Vorsitz im Turnus von jeweils zwei Haupt- und Vorkonferenzen sowie drei Zwischenkonferenzen. Hinzu kommt eine Sitzung mit den sogenannten spezifischen Aufsichtsbehörden, zu denen unter anderem die Kirchendatenschutzbeauftragten und die Rundfunkdatenschutzbeauftragten für den öffentlich-rechtlichen Rundfunk gehören.

Mehr Informationen finden Sie auf

▶ *datenschutzkonferenz-online.de*

Sowohl bei Windows 10 als auch bei MS Office 365 legt die DSK dabei Wert auf die Berücksichtigung des Urteils des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in unsichere Drittstaaten vom 16. Juli 2020 (C-311/18, „Schrems II").

## Verschlüsselung in Messengern

Die Forderungen nach einem Zugriff der Sicherheitsbehörden und Nachrichtendienste auf die verschlüsselte Kommunikation in Messengerdiensten und der privaten Kommunikation lehnt die DSK klar ab. Sie weist in ihrer Entschließung vom 25. November 2020 darauf hin, dass die Aushöhlung von Verschlüsselungslösungen – wie sie im Rat der Europäischen Union im Resolutionsentwurf Nr. 12143/1/20 vom 6. November 2020 „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" nahegelegt wird – kontraproduktiv wäre. Sie könnte durch Kriminelle und Terroristen leicht umgangen werden.

Eine sichere und vertrauenswürdige Verschlüsselung ist dagegen essentielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung. Unternehmen müssen sich vor Wirtschaftsspionage schützen können. Bürgerinnen und Bürger müssen auf eine sichere und integre Nutzung digitaler Verwaltungsleistungen vertrauen können. Verschlüsselung ist ebenso ein zentrales Mittel für die Datenübermittlung in unsichere Drittländer. Das „Schrems II"-Urteil des Europäischen Gerichtshofs hat das erneut deutlich gemacht.

Die DSK sieht daher keine Veranlassung, dass der Rat der Europäischen Union von diesen grundrechtswahrenden Positionen abweicht, zumal weitere, massiv in die Privatsphäre der Nutzerinnen und Nutzer eingreifende Befugnisse auch nicht erforderlich sind. Der effektive Kampf gegen Terror ist zwar ein legitimes Anliegen, aber den Sicherheitsbehörden stehen für die verfolgten Ziele bereits umfangreiche und sehr eingriffsintensive Instrumente zur Verfügung.

## Gesetzliche Ausgestaltung der Telekommunikations-Bestandsdatenauskunft

Im Interesse der Rechtssicherheit appelliert die DSK mit einer weiteren Entschließung an den Bundesgesetzgeber, endlich die Vorgaben des Bundesverfassungsgerichts vom Mai 2020 zur Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens umzusetzen. Das Gericht hatte erkannt, dass sowohl die Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stellen (beispielsweise Staatsanwaltschaften) jeweils einer verhältnismäßigen und normenklaren Grundlage bedürfen („Doppeltürenmodell"). Die derzeitige Fassung des § 113 Telekommunikationsgesetz und die Abrufnormen auf Seiten der Empfängerkreise genügen diesen Anforderungen nicht.

Zwar bleiben die bisherigen Vorschriften bis zur Neuregelung, längstens jedoch bis 31. Dezember 2021, nach Maßgabe der Entscheidungsgründe weiter anwendbar. Im Interesse der Rechtssicherheit appelliert die DSK jedoch an die politisch Verantwortlichen, diese Frist nicht auszureizen, sondern das manuelle Auskunftsverfahren möglichst zeitnah verfassungskonform auszugestalten.

## ePrivacy-Richtlinie (RL 2002/58/EG) in deutsches Recht überführen

Die Konferenz fordert den Gesetzgeber in einer Entschließung auf, endlich die ePrivacy-Richtlinie der Europäischen Gemeinschaften aus dem Jahr 2002 (RL 2002/58/EG) vollständig und im Einklang mit der Datenschutz-Grundverordnung von 2018 in deutsches Recht umzusetzen. Nach Art. 5 Abs. 3 ePrivacy-Richtlinie bedarf es einer aktiven informierten Einwilligung des Nutzers insbesondere dann, wenn der Verantwortliche „Cookies" setzt. Webseitenbetreiber und andere Akteure, die ihre Dienste unter anderem in Bezug auf „Cookies" rechtmäßig gestalten müssen, brauchen Rechtsklarheit und -sicherheit.

## Kurz erklärt

*Entschließungen* sind öffentliche Stellungnahmen der DSK zu datenschutzpolitischen Fragen, beispielsweise zur Einführung eines neuen Gesetzes. Entschließungen benötigen eine zwei Drittel Mehrheit in der DSK.

*Beschlüsse* sind Positionen, die die Auslegung datenschutzrechtlicher Regelungen und entsprechende Empfehlungen betreffen.

*Orientierungshilfen und Standardisierungen* sind fachliche Anwendungshilfen für Verantwortliche, Auftragsverarbeiter, Herstellerinnen und Hersteller sowie die Öffentlichkeit.

*Stellungnahmen* sind Positionen, die unter anderem in gerichtlichen Verfahren oder Gesetzgebungsverfahren abgegeben werden.

*Festlegungen* sind Positionen zu internen inhaltlichen, technischen und organisatorischen Fragen einschließlich der Gremienarbeit.

## Zentralisierung der Datenschutzaufsicht

Deutlich wendet sich die DSK auch gegen Forderungen nach einer Zentralisierung der Datenschutzaufsicht im nicht-öffentlichen Bereich. Die Aufsichtsbehörden in Bund und Ländern genießen fachlich hohes Ansehen. Ihre Zentralisierung wäre ausgesprochen kontraproduktiv, denn Zentralisierung heißt auch, immer weiter weg von den Anliegen und konkreten Umständen der betroffenen Menschen zu sein. Die föderale Struktur der DSK fördert Ergebnisse und Entscheidungen, bei denen ein vielfältiges Spektrum an Positionen bedacht und berücksichtigt wird. Kurzum: Statt unnötiger Zentralisierungsdebatten sollte dafür gesorgt werden, dass alle Aufsichtsbehörden personell und organisatorisch ihre gesetzlichen Aufgaben vollauf erfüllen können.

Weitere Themen der 100. DSK waren die Verbesserung der Zusammenarbeit im Europäischen Datenschutzausschuss (EDSA), die Evaluation des Bundesdatenschutzgesetzes und die künftige Arbeitsweise der DSK.

Die 101. DSK, die für April 2021 angesetzt ist, wird unter dem Vorsitz des Saarlandes stehen. Das Protokoll sowie die Entschließungen und Beschlüsse der 100. Datenschutzkonferenz finden Sie auf

www.datenschutzkonferenz-online.de

### Über den Autor

**Andreas Schurig**
ist Sächsischer Datenschutzbeauftragter.
Im vergangenen Jahr war er Vorsitzender der Konferenz der 18 unabhängigen staatlichen Datenschutzaufsichtsbehörden von Bund und Ländern (DSK). Schurig, Mathematiker und Theologe, hat das Amt des Sächsischen Datenschutzbeauftragten seit 2004 inne. 2009 und 2015 wurde er jeweils mit großer Mehrheit durch den Sächsischen Landtag wiedergewählt. Seine Behörde beschäftigt derzeit über 30 Bedienstete, die ca. 180.000 Unternehmen, 29.000 Vereine, 2,2 Millionen Privathaushalte sowie zahlreiche öffentliche Stellen in Sachsen im Hinblick auf deren Umgang mit personenbezogenen Daten beaufsichtigen.

▶ https://www.saechsdsb.de/

Anzeige

**Hi, ich bin PIA! Ihre digitale Datenschutzassistentin!**

**So einfach & schnell wie mit mir haben Sie Ihre Kunden als Datenschutzberater noch nie betreut!**

Ich führe Ihre Kunden mit intuitiven Fragebögen durch die Ersterhebung und weitere Audits.

Ich erstelle für Ihre Kunden selbstständig das Verarbeitungsverzeichnis und erhebe alle TOMs, die bei Ihren Kunden im Einsatz sind.

Ich überprüfe gemeinsam mit dem Kunden seine Website und erstelle ihm auch die passende Datenschutzerklärung.

Ich ordne Ihren Kunden automatisiert Aufgaben und Datenschutzmaßnahmen zu.

Ich sensibilisiere die Mitarbeiter Ihrer Kunden mit 12 innovativen Online-Trainings und generiere für Sie so zusätzlichen Umsatz.

**Das Einzige, das Sie noch zu tun haben: Ihren Kunden Zugriff auf die jeweiligen DSGVO-Fragebögen geben!**

DSGVO APP

**Hier erfahren Sie mehr über mich: www.dsgvoapp.eu**

# VERTRAULICHKEIT UND VERSCHWIEGENHEIT

## Wie weit geht die gesetzliche Verschwiegenheitspflicht des Datenschutzbeauftragten?

Regina Mühlich, Dr. Jens Eckhardt

Bereits im antiken Rom hängte man bei Zusammenkünften eine Rose an die Decke. Sie sollte die Anwesenden an ihre Verschwiegenheitspflicht erinnern. Die Rosen in den Beichtstühlen dienen eben diesem gleichen Zweck – „sub rosa dictum".

Die Verschwiegenheitspflicht – vertraglich auch als Vertraulichkeit geregelt und im Strafgesetzbuch als Verletzung von Privatgeheimnissen genannt – ist die rechtliche Verpflichtung anvertraute und auch nur bekannt gewordene Geheimnisse nicht unbefugt an Dritte weiterzugeben. Die Verschwiegenheitspflicht ist ebenfalls eng mit dem Datenschutzrecht sowie dem Geschäftsgeheimnisgesetz verknüpft.

### Wie weit geht die gesetzliche Verschwiegenheitspflicht des Datenschutzbeauftragten (DSB)?

Nach Art. 38 Abs. 5 Datenschutz-Grundverordnung (DSGVO) ist der DSB „bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden". Das „was" und „wie lange" ist in der DSGVO allerdings nichts geregelt. Reicht das soweit, wie bei Berufsgeheimnisträgern, dass nicht einmal der Auftraggeber benannt werden darf?

Sicherlich nicht. Der Schutz geht aber wohl über das Geschäftsgeheimnisgesetz (GeschGehG) hinaus. Ist er aber auch zur Vertraulichkeit einer betroffenen Person im Verhältnis zu seinem Auftraggeber verpflichtet? Nach der DSGVO möglicherweise nicht. § 6 Abs. 5 S. 2 BDSG sieht dies für den Datenschutzbeauftragten aber vor.

### Wie lange dauert die Verschwiegenheitspflicht?

Vertragspartner (etwa Rechtsanwälte, Ärzte, Heilpraktiker, Psychotherapeuten und Datenschutzbeauftragte) sind grundsätzlich auch ohne explizite vertragliche Regelung zur Verschwiegenheit im Rahmen ihrer Tätigkeit verpflichtet. Die Verschwiegenheitspflicht ist eine Ausprägung der allgemeinen Schutz- und Rücksichtnahmepflichten der Vertragspartner zueinander, wonach ein Partner auf die geschäftlichen Interessen seines Vertragspartners während des Vertragsverhältnisses Rücksicht zu nehmen hat.

Aus dieser allgemeinen Schutz- und Rücksichtnahmepflicht folgt, dass der Vertragspartner generell über alle Angelegenheiten Stillschweigen zu wahren hat, die ihm im Rahmen des Auftrages und/oder Stellung innerhalb der Organisation bekannt geworden sind und an denen der Vertragspartner ein berechtigtes Interesse hat. Die Verschwiegenheitspflicht gilt grundsätzlich während der gesamten Dauer eines Vertrags-, Behandlungs-, Beratungs- und Arbeitsverhältnisses. Es ist jedoch umstritten, ob und inwiefern die Verschwiegenheitspflicht eines Arbeitnehmers auch nach Beendigung des Arbeitsverhältnisses fortbesteht. Das Bundesarbeitsgerichts ist der Ansicht, dass auch eine über die Beendigung des Arbeitsverhältnisses hinaus bestehende Verschwiegenheitspflicht vertraglich möglich ist. Um ein faktisches Wettbewerbungsverbot eines ehemaligen Arbeitnehmers zu verhindern, kann sich eine solche nachvertragliche Verschwiegenheitspflicht allerdings nur auf einzelne und konkret bezeichnete Geschäfts- und Betriebsgeheimnisse beziehen.

Verstößt einer der Vertragspartner gegen seine Verschwiegenheitspflicht, macht sich dieser bezüglich des hierdurch entstehenden Schadens schadensersatzpflichtig (§ 280 BGB – Schadensersatz wegen Pflichtverletzung).

Allerdings ist diese grundsätzliche Pflicht als vertragliche Nebenpflicht nicht konturenscharf, sodass sich hieraus Unsicherheiten in Bezug auf den Schutzumfang ergeben. Aus diesem Grund sind stets konkrete vertragliche Ausgestaltungen geboten und daher auch typischerweise in Verträgen zu finden. Allerdings darf dabei der Bogen nicht überspannt werden. Denn dies kann zur Unwirksamkeit der Regelung führen.

## Datenschutzbeauftragte als (Berufs-) Geheimnisträger?

Angehörige bestimmter Berufe (etwa Rechtsanwälte, Ärzte und Journalisten), die im Strafverfahren zur Zeugnisverweigerung berechtigt sind, sind gemäß § 53 Strafprozessordnung (StPO) Berufsgeheimnisträger. Der Umfang des Zeugnisverweigerungsrechts ist auf die bei der Berufsausübung anvertrauten oder bekannt gewordenen Tatsachen beschränkt. Die gesellschaftliche Bedeutung und Anerkennung dieses Geheimnisses zeigt sich darin, dass es über die Bindung des Geheimnisträgers auch den Geheimnisträger schützt. Eine Entbindung des Berufsgeheimnisträgers vom Zeugnisverweigerungsrecht ist gemäß § 53 Abs. 2 StPO nur bedingt möglich und führt in den Fällen des Abs. 1 Nr. 2 b zur Aussagepflicht. Geschützt sind auch die Berufshelfer der Berufsgeheimnisträger, wie der Datenschutzbeauftragte (§ 53a StPO)[1].

Die DSGVO verpflichtet zur Verschwiegenheit. Vor allem Berufsgeheimnisträger sind verpflichtet, berufsgeheimnisrelevante Daten besonders zu schützen. So sind diese Berufsgruppen verpflichtet, angemessene technische und organisatorische Maßnahmen (Art. 32 DSGVO) zu implementieren, die gewährleisten, dass vor allem nicht nur sondern auch besondere Kategorien (sensible) von personenbezogenen Daten (Art. 9 DSGVO) gegenüber Dritten nicht offengelegt und/oder in falsche Hände geraten.

Der DSB ist nicht originärer Berufsgeheimnisträger wie die oben genannten freien Berufe. Allerdings ist dieser, soweit er für Berufsgruppen gemäß § 203 Abs. 1 und 2 StGB tätig ist, „in seiner Tätigkeit als mitwirkende Person" verpflichtet „fremdes Geheimnis nicht zu offenbaren." Bei einem Verstoß kann der DSB entsprechend Abs. 4 mit Freiheitsstrafe oder Geldstrafe bestraft werden.

## Fazit

Der Schutz von Geheimnissen zeigt, dass er nicht nur den Eigeninteressen einer Vertragspartei dient, sondern auch Vertrauen schaffen und sicherstellen soll. Die Berufsgeheimnisse erfüllen insoweit ebenfalls eine gesellschaftliche Funktion und erfahren einen gesetzlichen Schutz gegenüber Dritten.

[1] http://www.rechtslexikon.net/d/berufsgeheimnistraeger/berufsgeheimnistraeger.htm zuletzt abgerufen am 10.02.2021


### Über die Autoren

**Regina Mühlich**
ist Geschäftsführerin der Managementberatung AdOrga Solutions GmbH und Expertin für Datenschutz sowie Compliance Officer und Datenschutz-Auditorin (TÜV, DEKRA). Vorstandsmitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

▶ www.adorgasolutions.de

**Dr. Jens Eckhardt**
ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie Datenschutz-Auditor (TÜV) und Compliance-Officer (TÜV). Vorstandsmitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

▶ www.derra.eu

Anzeige

www.bvdnet.de

# BvD-Webinare & Online-Seminare

BvD e.V.
DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

| Termin | Thema |
|---|---|
| 06.04.2021 | **Webinar** – Was ist KI eigentlich genau? |
| 12.04.2021 | **Online-Seminar** – Beschäftigtendatenschutz |
| 14.04.2021 | **Webinar** – Videokonferenzsysteme aus datenschutzrechtlicher Sicht bewerten |
| 16.04.2021 | **Webinar** – Geschäftsgeheimnis: Ziehen Sie an einem Strang! |
| 23.04.2021 | **Online-Seminar** – Joint Controllership & Datenschutzverträge |
| 26.04.2021 | **Online-Seminar** – Schadensersatz, Schmerzensgeld, Geschäftsmodell? |
| 27.04.2021 | **Online-Seminar** – Umgang mit Datenschutzpannen – die Uhr tickt |
| 30.04.2021 | **Webinar** – Brexit: „5 vor 12“ – UK wird Drittland mit allen Konsequenzen |
| 06.05.2021 | **Online-Seminar** – Tipps & Tricks für erfolgreiche Datenschutzbeauftragte |
| 10.06.2021 | **Online-Seminar** – Technische und organisatorische Maßnahmen – Verstehen und Prüfen |
| 22. - 25.06.2021 | **Online-Seminar** – Get Ready: Datenschutz für Koordinatoren |

Zeitsparend Fachwissen erhalten nach Artikel 37, Absatz 5 DSGVO

**PREISE:**

| | |
|---|---|
| Webinare | 95,00 - 145,00 €* BvD-Mitglieder |
| | 145,00 - 195,00 €* Nichtmitglieder |
| Online-Seminare | 295,00 - 495,00 €* BvD-Mitglieder |
| | 395,00 - 595,00 €* Nichtmitglieder |

(*Alle Preise zzgl. gesetz. MwSt.)

**JETZT ANMELDEN:**

https://www.bvdnet.de/termine/

BERUFSVERBAND DER DATENSCHUTZBEAUFTRAGTEN DEUTSCHLANDS (BVD) E.V. | BUDAPESTER STRASSE 31, 10787 BERLIN

# DATENSCHUTZ MEDIENPREIS 2020: JURY GIBT DREI FINALISTEN BEKANNT

Karsten Füllhaase

Arbeitsreiche Wochen liegen hinter der Jury des Datenschutz Medienpreises: Mit 49 Einreichungen aus ganz Deutschland und der Schweiz hatte der vierte Jahrgang des vom BvD initiierten und nun erstmals durch die gemeinnützige „privacy4people" GmbH fortgeführten Wettbewerbs einen neuen Bewerberrekord verzeichnet. Aufgabenstellung des Wettbewerbs ist es, das Thema Datenschutz oder einzelne Aspekte daraus anschaulich darzustellen und damit zugleich den Nerv der jeweiligen Zielgruppe zu treffen. Zu sichten gab es erneut eine große Bandbreite von Beiträgen – von (mittlerweile höchst anspruchsvoll produzierten) Videos junger YouTuber über Hörfunkbeiträge professioneller Journalisten des öffentlich-rechtlichen Rundfunks bis hin zu aufwändigen Social-Media-Stories. Erstmals waren auch Print-Beiträge zugelassen, die auf Anhieb fast 30 Prozent der Einreichungen ausmachten.

Einer dieser Print-Beiträge gehört nun neben einem Video-Beitrag über Smart Speaker und einer Instagram-Story über eine Dating-App zu den drei Finalisten, die von der Jury nominiert wurden. „Die Nominierten greifen Aktuelles rund um das Thema Datenschutz in einer digitalen Welt gekonnt auf und transportieren Botschaften, die zum ganz persönlichen Nachdenken anregen", erläutert Juror Dr. Sebastian Sprenger von der DATEV-Stiftung Zukunft die Auswahl.

„Mit dem DAME möchten wir Medienmacher dazu anregen, das komplexe Thema Datenschutz für die Öffentlichkeit greifbar zu machen und dessen Alltagsrelevanz zu vermitteln", so BvD-Vorstandsvorsitzender und Juror Thomas Spaeing. „Der erneute Bewerberrekord in diesem Jahr zeigt, dass wir dabei auf einem guten Weg sind." Weitere Jury-Mitglieder sind neben Sprenger und Spaeing erneut Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachen, der Vorstand der Stiftung Datenschutz, Frederick Richter, Birgit Kimmel und Stefanie Rack von der EU-Initiative klicksafe sowie erstmals Marion Zinkeler, geschäftsführender Vorstand der Verbraucherzentrale Bayern. Gefördert wird der Datenschutz Medienpreis auch dieses Jahr wieder von der DATEV-Stiftung Zukunft, Medienpartner ist die EU-Initiative klicksafe.

Der Gewinner wird am 19. Mai 2021 im Rahmen der BvD-Verbandstage in Berlin bekannt gegeben. Die feierliche Preisverleihung, durch die in gewohnt charmanter Art Fernsehmoderator Ralph Caspers führt, wird zwar unter Einhaltung der geltenden Abstands- und Hygieneregelungen vor Ort stattfinden, anders als in den Vorjahren werden die Kongress-Teilnehmenden die Veranstaltung jedoch aufgrund der aktuellen Lage im Livestream verfolgen.

Bei weiterem Interesse, etwa zur Einbindung der Beiträge in Schulungen oder Veranstaltungen der Initiative „Datenschutz geht zur Schule", wenden Sie sich bitte an die Projektkoordinatorin für den Datenschutz Medienpreis (DAME), Nadja Bunk, telefonisch unter 030/26367758 oder per Mail an mail@datenschutzmedienpreis.de

Über den Autor

**Karsten Füllhaase**
ist Kulturwissenschaftler, erfahrener Kommunikationsprofi und Leiter des BvD-Hauptstadtbüros. Neben der Leitung und Betreuung der Geschäftsstelle begleitet er die Entwicklung des europäischen Dachverbands EFDPO und unterstützt den Vorstand bei der Ausschussarbeit sowie der politischen Kommunikation.

# DIE NOMINIERTEN FÜR DEN DAME 2020

## » Tobias Schießl, Max Osenstätter, Oliver Schnuck und Robert Schöffel

mit der mehrteiligen Instagram-Story „Dating-App Lovoo“

In dem Story-Videobeitrag der „News-WG“, eines jungen Politik-Formats des Bayerischen Rundfunks auf Instagram, haben die Journalisten in einem Selbstversuch eine Schwachstelle in der millionenfach genutzten Dating-App Lovoo aufgedeckt. Die problematische Radar-Funktion von Lovoo und anderen Dating-App-Anbietern macht die Standort- und Nutzerdaten öffentlich, so dass sich ein detailliertes Bewegungsmuster ganzer Personengruppen erstellen lässt.

**Jurorin Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen:**

> *„Diese Instagram-Story macht sehr deutlich, wie leicht sich Standortdaten missbrauchen lassen, die Nutzer mit bestimmten Apps teilen. Die besondere Stärke des Beitrags liegt darin, dass er inhaltliche Tiefe bietet und zugleich durch Aufmachung und Sprache die junge Zielgruppe passgenau abholt.“*

## » Hannes Munzinger und Felix Ebert

mit dem Print-Beitrag „Wie wir uns verraten / Auf Sendung“

Der Print-Beitrag aus der Süddeutschen Zeitung (SZ) beschreibt anschaulich und informativ, welches Ausmaß der Tracking-Wahn auf dem Smartphone mittlerweile angenommen hat. Denn zahlreiche Apps erstellen in einer pausenlosen Überwachung des Nutzers ein umfassendes Profil ohne dessen Wissen, verkaufen dieses oder nutzen es für eigene Werbezwecke. Hannes Munzinger und Felix Ebert liefern neben interessanten Fakten auch fachliche Zusammenhänge und erklärende Grafiken.

**Stefanie Rack, Päd. Referentin EU-Initiative klicksafe, National Awareness Centre Germany, Medienanstalt RLP:**

> *„Der Print-Artikel veranschaulicht in eindrucksvoller Art und Weise, wie Handydaten einer gewöhnlichen Nutzerin an einem gewöhnlichen Tag von Apps und Anbietern gesammelt und ausgewertet werden. In Zeiten der schnellen Unterhaltung durch kurze Videoformate ist es wohltuend, einen gut recherchierten Artikel zu lesen, der in die Tiefe geht!“*

## » Svea Eckert und Henning Wirtz

mit dem Video-Beitrag „Smart Speaker: Wobei Alexa, Siri & Co. heimlich mithören“

„Strg+f“ ist ein junges YouTube-Format von funk. Die Reporterin Svea Eckert findet im Selbstversuch mit ihrem Amazon Echo Smart Speaker heraus, dass das Gerät ihr auch dann zuhört, wenn es nicht zuhören soll. Denn die Smart Speaker machen Fehler. Sie verstehen Sprachbefehle, die keine sind. Wie oft passieren diese Fehler? Und wer hört bei der Auswertung der Daten mit? In der knapp 20-minütigen Reportage begibt sie sich auf die Spur ihrer eigenen Daten.

**Juror Dr. Sebastian Sprenger von der DATEV-Stiftung Zukunft:**

> *„Die allermeisten Personen, die sich einen Smart Speaker zulegen, tun das ja mit einer gewissen Akzeptanz dafür, dass Ton beispielsweise in der eigenen Wohnung mitgeschnitten und dann verarbeitet wird. Die Reportage von Frau Eckert macht allerdings transparent, wieviel Privatheit wir mit der Nutzung von Alexa und Co. tatsächlich aufgeben: Geschäftsgeheimnisse aus Meetings oder auch Inhalte aus Streitgesprächen – Inhalte, die wir nicht mal mit Nachbarn teilen dürfen oder wollen, treten wir mit der Einwilligung der Nutzungsbedingungen freiwillig an die Betreiber ab. Darüber sollte man sich ernsthaft bewusst sein.“*

Die Beiträge können Sie ansehen unter:
www.datenschutzmedienpreis.de

Über den QR-Code gelangen Sie direkt auf die DAME-Seite mit den aktuell nominierten Beiträgen sowie den Nominierten und Gewinnern der vorherigen DAME-Wettbewerbe.

# WO DSGZS-DOZENTEN NOCH WAS LERNEN

## Der Dozententag der BvD-Initiative „Datenschutz geht zur Schule“ fand 2020 online statt

David Heimburger

Rund 70 Datenschützerinnen und Datenschützer engagieren sich in der BvD-Initiative „Datenschutz geht zur Schule“. Wenn sich keine Pandemie in den Weg stellt, treten die Ehrenamtlichen an Schulen im ganzen Bundesgebiet auf und informieren Schülerinnen und Schüler, weshalb Datenschutz wichtig ist und vor allem, wie man darauf achten kann, dass die eigenen Daten möglichst gut geschützt bleiben. Koordiniert wird die Initiative vom AK Schule des BvD, gefördert wird sie von der DATEV-Stiftung Zukunft.

Die finanzielle Förderung fließt unter anderem in die Ausrichtung eines jährlichen Dozententags. Die Veranstaltung dient dem Austausch der Dozentinnen und Dozenten miteinander und soll vor allem ein Dankeschön für das Engagement sein. Statt Blumen oder Fresskörben steht eine deutlich nachhaltigere Form des Danks im Mittelpunkt der Veranstaltung: Vorträge zu aktuellen Datenschutzthemen von renommierten Expertinnen und Experten. Beim Dozententag von „Datenschutz geht zur Schule“ nehmen die Dozentinnen und Dozenten selbst auf der Schulbank Platz.

Die Initiative hatte für den Dozententag 2020 eine Einladung des Unabhängigen Landeszentrums für Datenschutz (ULD) in Schleswig-Holstein nach Kiel erhalten, musste aber wie die meisten Veranstaltungen als Onlinetreffen stattfinden. Der persönliche Austausch fiel dementsprechend eher knapp aus, dafür war die Zahl der Teilnehmenden ungewöhnlich groß und der Fokus auf die Expertenvorträge noch stärker als in zurückliegenden Jahren.

Dem AK Schule ist es gelungen, Vertreterinnen und Vertreter aus Behörden, Verbänden und Gerichten zu gewinnen. Die Beinahe-Gastgeberin Marit Hansen, Leiterin des ULD, sprach zu einem der meist diskutierten Themen 2020: „Schule goes digital – Trends und Wünsche aus der Datenschutzperspektive“. Die Corona-Thematik stand auch im Mittelpunkt des Vortrags von Michael Will, Präsident des Bayerischen Landesamts für den Datenschutz (BayLDA): „Datenschutz in Zeiten der Pandemie – aktuelle Fragestellungen aus der aufsichtsrechtlichen Praxis“.

Eine angenehme Ablenkung von der Pandemie war der Beitrag von Tatjana Helm, Referatsleiterin Markt und Recht bei der Verbraucherzentrale Bayern e.V., zu einem zentralen Datenschutzthema: „DSGVO-Einwilligung aus der Verbraucherarbeit“. Topaktuelle Infos zum wahrscheinlich größten Datenschutzthema 2020 hat Alexander Filip, ebenfalls aus dem BayLDA, vorgestellt: „Schrems II und die Folgen“.

Praxistipps lieferte die Präsentation von Kristin Benedikt, Richterin am Verwaltungsgericht Regensburg und früher Referatsleiterin beim BayLDA: „Personenbezogene Daten sind langweilig? Wie man mit praktischen Tools und Tipps richtig sensibilisiert“.

Ein fünfter Vortrag musste kurzfristig verschoben werden. So gab es noch einen zweiten Mini-Dozententag mit Mike Kuketz, Blogger, IT-Security-Berater und Mitarbeiter des Landesbeauftragten für Datenschutz und Informationssicherheit Baden-Württemberg zum technischen Datenschutz: „Eindämmung der Kommunikationsfreudigkeit mobiler Endgeräte (Android)“

Der Dozententag 2020 ist kein reiner Lerntag geblieben. Nach den Vorträgen wurde den Dozentinnen und Dozenten die grafisch rundherum erneuerte und modernisierte Präsentationsvorlage für die Auftritte vor den Schülerinnen und Schülern vorgestellt und angeregt diskutiert. Neben der optischen Neuausrichtung sind auch die Inhalte gestrafft worden, so dass es in Zukunft noch leichter fallen dürfte, die Schüler für den Datenschutz mindestens zu sensibilisieren und optimaler Weise sogar zu begeistern.

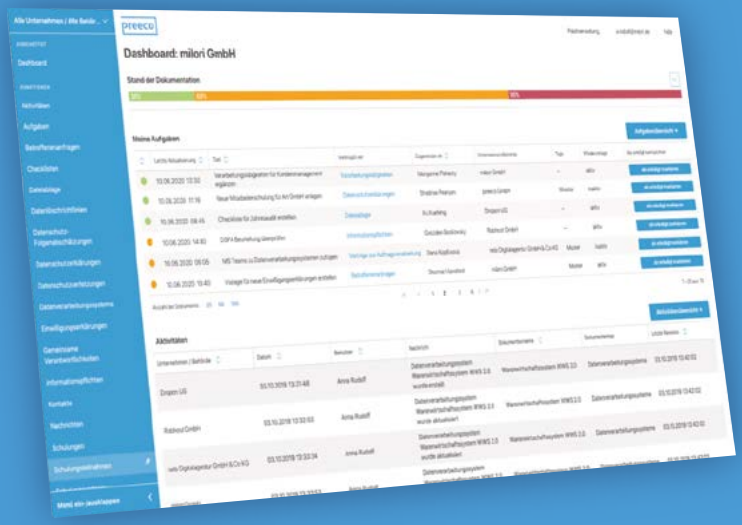
Begeistert waren zumindest die Teilnehmenden am Dozententag 2020. Es kam der Wunsch auf, dass künftige Dozententage als Hybrid-Veranstaltungen angeboten werden. So können Dozentinnen und Dozenten, denen die Zeit für eine Reise zum Ort der Veranstaltung fehlt, zumindest den Präsentationen folgen. Die meisten Aktiven freuen sich aber schon auf ein persönliches Wiedersehen und rege Diskussionen beim Dozententag 2021 – wahrscheinlich im Spätsommer in Kiel beim ULD, das seine Einladung freundlicher Weise aufrechterhält.

## Über den Autor

**David Heimburger**
hat sich als Rechtsanwalt auf die Arbeit als Datenschutzbeauftragter spezialisiert. Der Hamburger prüft Geschäftsmodelle und unterstützt bei der Bereitstellung der erforderlichen Datenschutzdokumente. Seine Kunden sind kleine und mittlere Unternehmen sowie Vereine. Seine Schwerpunkte sind zum einen die Grundsatzberatung von Start-ups und zum anderen medizinische Einrichtungen wie Rettungsdienste und Arztpraxen.

▶ https://www.davidheimburger.de/

Anzeige




preeco

Smarte Software
für Datenschutzbeauftragte

**Schnell**:
Mit Textbausteinen und Mustervorlagen

**Vollständig**:
Alle DSGVO relevanten Dokumente

**Flexibel**:
Mandantenfähig und auch für kleine und große Organisationen

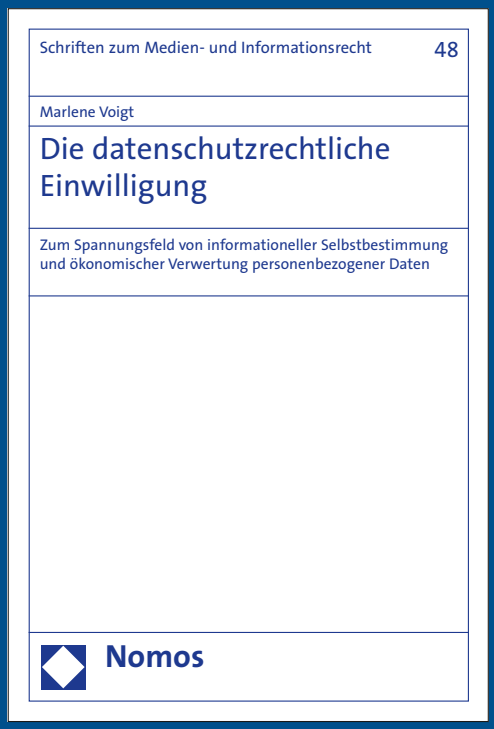
Weitere Infos, Testversion und persönliche Demo unter:

www.preeco.de/bvd

preeco GmbH, Magirus-Deutz-Straße 14, 89077 Ulm, Mo-Fr 9-17 Uhr, Tel. 0731 96589258, E-Mail support@preeco.de

# DIE DATENSCHUTZRECHTLICHE EINWILLIGUNG

Marlene Voigt




Marlene Voigt
**»Die datenschutzrechtliche Einwilligung«**

**Nomos Verlagsgesellschaft**

1. Auflage 2020
138,00 Euro
ISBN 978-3-8487-7831-7, für E-Book ISBN 978-3-7489-2234-6

Die mit „summa cum laude" bewertete Dissertation von Frau Dr. Marlene Voigt wurde mit dem Rudolph-Haufe-Nachwuchsförderpreis für hervorragende wissenschaftliche Leistungen mit besonderer praktischer Relevanz und Bezug zum Steuer- und Wirtschaftsrecht ausgezeichnet. Eine so ausgezeichnete Dissertation erweckt bei DSB natürlich Neugierde. Und zugleicht stellt sich die Frage: Einwilligung mit Relevanz und Bezug zum Steuer- und Wirtschaftsrecht?

Der Bezug zum Steuer- und Wirtschaftsrecht wird in der Einleitung dargestellt. Die Fragestellung der Arbeit ist auch, ob eine Einwilligung sowohl den Anforderungen der Datenökonomie gerecht wird, als auch eine freie und informierte Entscheidung betroffener Person ermöglicht. Die Frage ist also: Genügen die europarechtlichen Vorgaben den Bedürfnissen der Datenwirtschaft?

Zunächst wird sich dem Thema „persönliche autonome Selbstbestimmung" über das deutsche Zivilrecht genähert und dessen Anforderungen an eine Einwilligung betrachtet, beginnend mit dem Erlass des BDSG im Jahre 1977 bis hin zur EU Datenschutz-Richtlinie und deren Umsetzung im BDSG. Ein Ergebnis: Eine Einwilligung ist sowohl im Bereich des Datenschutzrechts als auch im Privatrecht als einseitige, rechtsgeschäftliche Erklärung zu qualifizieren.

Im nächsten Kapitel werden die in der DS-GVO enthaltenen Regelungen vorgestellt. Dabei wird dargestellt, dass Unklarheiten hinsichtlich des genauen Umfangs der Informationspflicht des Verantwortlichen, der Reichweite eines Ausschlusses der Einwilligungseinholung im Wege des Opt-Out sowie hinsichtlich der konkreten Voraussetzungen und der Wirkung des Koppelungsverbots bestehen.

Im 4. Kapitel werden die Interessen von Datenverarbeiter und betroffenen Personen sowie deren Rechtspositionen untersucht. Wenig überraschend ergibt sich, dass eine vielfältige Interessenslage existiert, dabei Datenverarbei-

ter und betroffene Personen teilweise gegenläufige Interessen haben.

Das 5. Kapitel widmet sich der Auslegung der Anforderungen in klassischer Weise: Wortlaut, Systematik, Historie/Genese sowie Telos. Bei der Beurteilung der Informationspflichten wird als Ergebnis dargestellt, dass aufgrund des nicht eindeutig dargelegten Umfangs der Informationspflichten einem Verantwortlichen bei Bereitstellung sämtlicher in Art. 13 DS-GVO enthaltenen Angaben kein Verstoß gegen das in der DS-GVO enthaltene Transparenzgebot unterstellt werden kann. Bzgl. Opt-In/Opt-Out wird als Resultat dargestellt, dass ein Opt-Out-Modell nicht mit den Vorgaben der DS-GVO vereinbar ist. Zum Kopplungsverbot wird gesagt, dass die DS-GVO weder ein striktes noch ein absolutes Kopplungsverbot beinhaltet.

Im 6. Kapitel erfolgt die Bewertung der erzielten Resultate in Bezug auf die Fragestellung. Es wird festgestellt, dass die in der DS-GVO normierten Pflichten für den Verantwortlichen zu einem Mehraufwand führen, dabei die unklaren Voraussetzungen für eine wirksame datenschutzrechtliche Einwilligung ein Haftungsrisiko bergen, ohne dass durch diese Anforderungen eine Stärkung der Betroffenenrechte erzielt werden. Die Autorin schlägt ein Alternativkonzept vor, welches eine Neuausrichtung der Einwilligung im Verhältnis der Verarbeitungsgrundlagen vorsieht.

Im Fazit beschreibt die Autorin, dass die Regelungen der DS-GVO zur Einwilligung ökonomische Implikationen nur bedingt berücksichtigen. Die DS-GVO greife zwar die Problematiken datenintensiver Geschäftsfelder auf, führe bestehende Konfliktpunkte der Datenwirtschaft mit den datenschutzrechtlichen Prinzipien aber keiner alltagspraktikablen Lösungen zu. Die Arbeit wurde 2020 als Dissertation angenommen, die inhaltliche Arbeit wurde wahrscheinlich Mitte 2019 beendet. Zieht man die heute vorhandenen Informationen zum Thema heran, wird man in manchem Punkten wohl zu einem anderen Ergebnis als die Autorin kommen. Dennoch ist die Arbeit aus Sicht der Datenökonomie eine interessante Arbeit, zeigt sie doch an einigen Stellen auf, dass die Datenwirtschaft Anforderungen erhebt, die mit den europarechtlichen Vorgaben hinsichtlich Einwilligung nur schwierig oder gar nicht vereinbar sind. Für an einer juristischen Diskussion Interessierte ist die Arbeit daher empfehlenswert, für die tägliche Praxis eines DSB hingegen nur eingeschränkt.

Rezension von

**Dr. Bernd Schütze**

beschäftigt sich seit 1995 mit den datenschutzrechtlichen Aspekten innerhalb der Gesundheitsversorgung. Nach gut dreißigjähriger beruflicher Tätigkeit in verschiedenen Krankenhäusern arbeitet Dr. Schütze seit 2014 als „Senior Experte Medical Data Security“ bei der Deutschen Telekom Healthcare and Security Solutions GmbH. Als Lehrbeauftragter ist er zudem an verschiedenen Hochschulen tätig und veröffentlicht regelmäßig Beiträge in Büchern und Fachzeitschriften.

# DATENSCHUTZBEAUFTRAGTE - EINSTEIGERLEKTÜRE FÜR ANFÄNGER

Stephan Hansen-Oest

Stephan Hansen-Oest
**»Datenschutzbeauftragte - Einsteigerlektüre für Anfänger«**

**dfv Deutscher Fachverlag**

1. Auflage 2020
316 Seiten, Broschur
39,90 Euro
ISBN 978-3-8005-0013-0

Wer sich in Deutschland mit dem Thema Datenschutz befasst oder die Entwicklung mit einem Ohr auf der Schiene verfolgt, der wird am „Datenschutz-Guru" kaum vorbeikommen. Stephan Hansen-Oest, der nicht häufig genug betonen kann, nach eigener Ansicht gar kein Guru zu sein, ist nicht nur mit seinem Datenschutz-Coaching Startpunkt und Mentor für viele interne sowie externe Datenschutzbeauftragte, man landet auch häufig auf der Suche nach Details zu einem Thema oder Inspiration für einen Text oder ein Formular auf seiner Homepage.

Mit „Datenschutzbeauftragte – Einsteigerlektüre für Anfänger" haben die geneigte Podcast-Hörerin und der Newsletter-Abonnent das Gefühl, einen Sammelband, mitunter ein Best of in Händen zu halten. Wer ohne Vorerfahrungen in diese Lektüre schaut, findet in gut 40 einzelnen Kapiteln mal mehr, mal weniger umfangreich, aber immer passend pragmatisch, verschiedene Aspekte beleuchtet, die Verantwortliche und Datenschutzbeauftragte zu regeln haben. An vielen Stellen werden Vorlagen, Muster sowie Formulierungsvorschläge geliefert. Insgesamt ergibt sich eine Einsteigerlektüre, die nicht nur authentisch bleibt, sondern auch Mut macht. Auch wenn die oder der neu gekürte Datenschutzbeauftragte vor einem großen Berg steht, es ist zu schaffen. Dabei ist auch hilfreich, dass das Werk für Neulinge die eine oder andere Klippe durch weitgehende Auslassung umschifft. Die Ausführungen zu Bußgeldern und zum Drittlandtransfer sind z.B. nicht mehr als ein Ausblick, aber eben auch nicht mehr als jemand ganz frisch im Thema benötigt.

Nur gelegentlich setzen die Inhalte ungewollt Erfahrungen voraus, die nicht jede Leserin und jeder Leser haben wird, z.B. beim Umgang mit IT-Risiken. Zwar wird auch hier das eine oder andere erläutert, ad-hoc wird jedoch die un-

erfahrene Leserin oder der unerfahrene Leser den Unterschied zwischen Risikoreduktion und -vermeidung vielleicht nicht kennen. Allein aufgrund der Ausführungen im Buch würde auch der BSI Grundschutz falsch eingeschätzt werden. Neben einer gut gelungenen Einsteigerlektüre für Datenschützerinnen und Datenschützer auch noch en passant Einsteigerinnen und Einsteiger umfassend im Bereich Informations- bzw. IT-Sicherheit zu qualifizieren, wäre allerdings auch zu viel des Guten gewesen.

Der Autor ist selbst Anwalt, hat das Buch jedoch in einem erfrischend von Fachsprache befreiten Stil verfasst. Noch leichter würde der Einstieg ggf. mit mehr Flow Charts oder grafische Darstellungen fallen. Lediglich zu Beginn des Buches gibt es einige Grafiken zur Benennung, Stellung und den Aufgaben des Datenschutzbeauftragten sowie zur Struktur sowie zum Anwendungsbereich der DSGVO. Im Anschluss wirkt es so, als hätten Zeit oder Muße für solche Aufbereitungen gefehlt. Da wird das Buch leider ein wenig zur Textwüste. Hier und da wären weitere Ablaufdiagramme oder auch kapitelübergreifende tabellarische Darstellung nützlich gewesen, z.B. bei der Abgrenzung von eigener Verantwortung, gemeinsamer Verantwortung und Datenverarbeitung im Auftrag. Was dem Buch leider ebenfalls fehlt, ist ein Stichwortverzeichnis.

Die lockere norddeutsche Schreibe macht von dieser Monotonie viel wieder wett. Etwas störend sind jedoch die zahlreichen Mustertexte, die jeweils in den Fließtext eingebaut werden und in manchen Kapiteln als Unterbrechung wirken, ganz besonders, wenn die Texte wie z.B. bei Richtlinienvorschlägen oder der Mustervereinbarung über Datenverarbeitung im Auftrag mehrere Seiten umfassen. Die Muster in einen Anhang zu verlagern und lediglich den Inhalt kurz zu umreißen würden dem Lesefluss hier helfen. Ganz davon abgesehen wird hoffentlich niemand diese Texte abtippen, sondern über die Datenschutz-Guru-Homepage beziehen.

Auch wenn das Buch für Beginnerinnen und Beginner geschrieben wurde, ist es nicht nur für solche lohnenswert. Der Rezensent muss gestehen, dass er auch nach mehrjähriger Anwendung der DSGVO immer noch einen Spickzettel brauchte, ohne den die fehlerfreie Zuordnung von Rechtsgrundlagen und Buchstaben im Art. 6 Abs. 1 DSGVO nicht gelang. Seitdem jedoch hier die Rechtsgrundlagen als **A**lternative, dickes **B**, **C**aesar, **D**ead, **E**cht jetzt sowie **F**ETT eingeführt und humorvoll erläutert wurden, konnte der Spickzettel in den Mülleimer wandern. Auch gestandene Datenschutzbeauftragte können das Buch als kurzweiliges Roundup und Grundlagen-Repetitorium genießen und sei es nur, um neue Ideen für eine an Zielgruppen angepasste Vermittlungsweise zu bekommen. Das Buch ist daher nicht nur ein gelungener Einstieg, sondern sollte als wohltuender Kontrast zur Kommentarliteratur Eingang in die heimischen Datenschutz-Bibliothek finden.

# DSGVO IM PRAXISTEST – ERMITTLUNGEN BUSSGELDER VERFAHREN

Niko Härting, Lasse Konrad

Niko Härting, Lasse Konrad
**»DSGVO im Praxistest - Ermittlungen Bußgelder Verfahren«**

**Verlag Dr. Otto Schmidt**

1. Auflage 2020
152 Seiten Lexikonformat, Broschur
39,80 Euro
ISBN 978-3-504-56078-2

Das vorliegende Buch möchte 249 Fragen (und Antworten) für die „DSGVO im Praxistest" liefern. Ohne den Untertitel zu lesen, erwartet man eine Einführung für Praktiker und Evergreens zur Abgrenzung personenbezogener Daten, zu nötigen Inhalten des Verzeichnisses der Verarbeitungstätigkeiten usw., eine klassische Sammlung häufig gestellter Fragen eben. Diese Einschätzung liegt allerdings gänzlich daneben, wie der Untertitel „Ermittlungen – Bußgelder – Verfahren" zeigt, der hätte vorangestellt werden können.

Diese neudeutsch Frequently Asked Questions sind nämlich mitnichten Frequently. Das dürfte seitens der meisten Verantwortlichen und Datenschutzbeauftragten auch gewollt sein. Sich mit diesen Inhalten beschäftigen „zu müssen", heißt letztlich nichts anderes, als in eine Auseinandersetzung mit der Datenschutzaufsicht zu gehen und mit fortschreitender Eskalation ferner, dass etwas nicht optimal abgelaufen ist. Entsprechend werden Verantwortliche und Datenschutzbeauftragte so planen wollen, dass dieses Buch nicht gebraucht wird. Ab einer gewissen Größe des Verantwortlichen sowie mit fortschreitender Zeit wird der Kontakt mit den Behörden jedoch immer wahrscheinlicher. Sich darauf vorzubereiten ist entsprechend ratsam. Dafür kann das vorgelegte Buch eine sehr gute Hilfe sein. Auch bei einer versäumten Vorbereitung ist der Frage-Antwort-Stil geeignet eine Art Erstberatung und schnelle Orientierung zu bieten, wenn das Thema schlagend wird, um (weitere) Fehler zu vermeiden.

Als Zielpublikum des Buches kommen vor allem Anwälte im Datenschutzrecht und Konzerndatenschutzbeauftragte in Betracht, die noch nicht die sprichwörtlichen alten Hasen im Bußgeldverfahren sind. Die Autoren, ihres Zeichens beide Anwälte, geben sich aber auch Mühe, auf angemessenem juristischen Niveau, jedoch für den Nicht-Juristen verständlich zu schreiben. Die fachliche Sicherheit ist gleichwohl ebenso zwingend wie ein grundsätzliches Verständnis von Rechtsbehelfen, Haftung und Sanktionen im Datenschutzrecht. Wer bisher nur in Zeitungsartikeln über angedrohte Höhen von Strafzahlungen las, jedoch Schadenersatz, Bußgelder und Anordnungen im Verwaltungsrecht nicht unterscheiden kann, wird mit diesem Buch überfordert sein, sollte dann aber sowieso tunlichst professionelle Hilfe im Fall des Falles in Anspruch

nehmen. Für den internen Datenschutzbeauftragten, der die Aufgabe als Zusatztätigkeit neben operativen Aufgaben erledigt, ist das Buch weniger notwendig und geeignet.

Schlägt man diese Fragensammlung auf, überrascht ein wenig die wie ein Theaterstück angelegte Struktur. In drei Akten mit zehn Aufzügen, Verzeihung, zehn Teilen, wird eine eskalierende Auseinandersetzung mit der Aufsicht nach anfänglicher Auskunft bzw. Ermittlung (Akt 1) über Maßnahmen samt möglicher Gegenwehr (Akt 2) bis zu deren Prüfung vor Gericht (Akt 3) durchgespielt. Die Dramatis Personae sind hier der Beschwerdeführer, Verantwortliche, die zuständige Aufsicht und das Gericht, während die Dämonen der herrschenden Meinung im Untergrund lauern.

Die Struktur wirkt auf den ersten Blick gekünstelt oder verspielt, insbesondere der Mitautor Nico Härting ist auch durchaus für pointierte Auftritte bekannt, mit denen er sich im Rahmen der Corona-Pandemie meinungsstark hervortut. Auf den zweiten Blick gibt es jedoch keine Theatralik um ihrer selbst willen, sondern die gewählte chronologische Struktur ist hilfreich, wenn nicht zwingend, da sie ermöglicht, sich im Prozess wiederzufinden und die ansonsten inhaltlich losgelösten einzelnen Fragen samt Antworten zu verbinden.

Das Buch ist recht dünn, auf etwas mehr als 120 Seiten bleibt für jede Antwort im Schnitt nur eine halbe Seite Platz. Es handelt sich auch nicht um einen Almanach der Rechtsbehelfe, da sich das Werk konkret mit Aufsichtsbehörden und deren Anordnungen sowie Bußgeldern beschäftigt. Um den Umgang mit Betroffenen, deren Auskunftsrechten oder Auseinandersetzungen im Kontext des Schadenersatzes geht es nicht. Auch das Stichwortverzeichnis ist enttäuschend schmal, aber der Nachschlagecharakter ergibt sich aus der Strukturierung entlang der Fragen, auch das Inhaltsverzeichnis leistet hier gute Dienste.

Zahlreiche Fragen könnten exakt so für andere Rechtsgebiete oder die dortigen Aufsichtsbehörden gestellt werden oder in einem allgemeinen Werk über die Hintergründe von Verwaltungsgerichtsprozessen. Nicht wenige der Antworten würden dort genau gleich lauten.

Die Ausführungen sind gelungen, schön geschrieben und durchgehend hilfreich. Gelegentlich ist die eine oder andere Antwort inhaltlich nicht unstrittig, das wird aber durch die Betrachtung der Rechtsprechung einzelner Gerichte dem Leser durchaus klar. Da sich das Buch auch wie geschildert an eine kundige Leserschaft richtet, soll das kein Makel sein.

Wenn man ein Haar in der Suppe finden will, dann ggf., dass der Titel den Mund etwas voll nimmt. Eine klare Praxis zum Umgang mit Bußgeldverfahren hat sich noch nicht so entwickelt, als dass dagegen getestet werden könnte. Noch wird grundlegend über das Verhältnis zum Ordnungswidrigkeitenrecht diskutiert. Entsprechend wartet man am Ende des Werkes vergeblich auf den auslaufenden Spannungsbogen, den fallenden Vorhang und das sich aufhellende Saallicht. Das Ende ist hier noch offen. Es steht zu befürchten, dass sich die Beteiligten am Ende nicht an den Händen nehmen, um sich gemeinsam vor dem Publikum verbeugen. Anders als das Programmheft aus der Theatervorstellung wird dieses Werk aber – einmal zur Hand genommen – nicht achtlos im Regal verstauben.

Rezensionen von

**Markus Steinkamp**
ist Konzerndatenschutzbeauftragter bei Hellmann Worldwide Logistics in Osnabrück. Der studierte Wirtschaftswissenschaftler erlangte einen Master in angewandter IT-Sicherheit an der Ruhr-Universität und arbeitet seit mehr als zehn Jahren in den Bereichen Datenschutz und Informationssicherheit. Markus Steinkamp ist zertifizierter Datenschutzbeauftragter (TÜV) und nach Verbandskriterien des BvD verpflichtet.

# DATENVERARBEITUNG IN DRITTSTAATEN - KOMPLEXE REGELUNGEN EINFACH ERKLÄRT

## Dr. Jens Eckhardt, Bernd Fuhlert

Datenübermittlung in Drittstaaten war 2020 eines der zentralen Themen und wird es 2021 weiterhin sein: das EuGH-Urteil „Schrems II" und gegebenenfalls der Brexit. Der Drittlandtransfer ist kein neues Thema, aber er wird durch die technischen Entwicklungen wie Digitalisierung, KI und Blockchain immer komplexer und stellt Unternehmen immer wieder vor neue Herausforderungen – auch ohne EuGH-Urteile und nicht nur aus Datenschutzsicht.

Dr. Jens Eckhardt, Bernd Fuhlert
**»Datenverarbeitung in Drittstaaten Komplexe Regelungen einfach erklärt.«**

**PrivacyXperts, ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG**

1. Auflage 2020
56 Seiten, DIN A4
129,95 Euro
ISBN 978-3-8125-2900-6

Die Datenschutz-Grundverordnung (DSGVO) lässt einen freien Datenverkehr nur innerhalb der Europäischen Union (EU)/EWR zu, denn nur innerhalb dieser ist ein einheitliches Datenschutzniveau gewährleistet. Der Datentransfer endet aber nicht an den europäischen Grenzen. Der Datentransfer in Drittländer ist nur unter bestimmten Voraussetzungen möglich und folglich nur bei Einhaltung der DSGVO auch zulässig.

Kapitel 2 von insgesamt fünf gibt, nach einer allgemeinen Einführung, einen umfassenden Überblick über die jeweilige Regelung der Artt. 44 bis 49 DSGVO. Inbesondere Art. 44 DSGVO, der Dreh- und Angelpunkt bei der Bewertung einer Datenübermittlung in Drittländer oder an internationale Organisationen. Schicht für Schicht werden die VO-Artikel erläutert und mit Beispielen ergänzt, bis hin zu Checklisten.

In Kapitel 3 werden die einzelnen Garantien für eine Datenübermittlung in Drittländer durchleuchtet: die Anwendungsvoraussetzungen, die Nutzungsmöglichkeiten und die Fallstricke.

Kapitel 4 widmet sich ausführlich Praxisbeispielen und Sonderthemen: Prüfungsvorgehen, Cloud-Computing und Cookies und rundet den Leitfaden ab. Die beiden Autoren, Dr. Jens Eckhardt und Bernd Fuhlert, erläutern kurz und prägnant und dennoch umfassend die Regelungen und Anforderungen, die es zu beachten gilt. Sie führen kompetent durch das Thema „Drittstaat" und erläutern die Rahmenbedingungen für Datenübermittlungen. Randthemen wie Beschäftigtendatenschutz oder Sonderthemen wie der Datenaustausch mit Kanada, werden ebenso erläutert wie die Hintergründe zum EU-US Privacy Shield. Der einheitliche Aufbau und die Gliederung der einzelnen Kapitel macht das Handbuch zum Nachschlagewerk. Es ist inhaltlich verständlich und stringent strukturiert: Schilderung des Sachverhalts und was dieser für die Praxis bedeutet, ergänzt mit Checklisten und teils auch den entsprechenden Fallstricken. Hilfreich sind auch die diversen tabellarischen Abbildungen, Gegenüberstellungen von Gesetzespassagen und Auswirkungen sowie Workflows und Prüfschemata.Der Leitfaden ist ideal und besonders geeignet für Einsteiger und diejenigen, die sich bis dato noch nicht intensiv mit Drittlandübertragungen befassen „mussten". Der praktische Ansatz des gut handhabbaren und verständlich geschriebenen Handbuchs ist, ob der Aktualität für Datenschutzbeauftragte und Datenschutzberater, von hoher Relevanz. Es hilft datenschutzrechtliche Fragen zu beleuchten und schafft einen guten Überblick, ohne dabei alles zu verkomplizieren.

**Fazit:**

Der Titel des Handbuchs ist Programm: Komplexe Regelungen einfach erklärt. Empfehlenswert für einen schnellen und umfassenden Einstieg in das Thema „Drittstaaten" sowie als Nachschlagewerk nach dem Motto „habe ich bei der Bewertung alles berücksichtigt". Und wie es schon im Vorwort heißt: der Praxisleitfaden ist ein Kompass - und hilfreich.

Rezension von

**Regina Mühlich**
ist Geschäftsführerin der AdOrga Solutions GmbH, Datenschutzbeauftragte, Datenschutz-Auditorin, Compliance Officer, anerk. Sachverständige für Informationsverarbeitung und Datenschutz, zert. Informationssicherheitsbeauftragte ISO/IEC 27001 (ISMS), BvD-Vorstandsmitglied.

▶ www.AdOrgaSolutions.de

# 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
▶ www.bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

| | | | |
|---|---|---|---|
| **19.03.2021** | RG Ulm | **16.09.2021** | AK Sozial |
| **25.03.2021** | RG Mitte | **23.09.2021** | RG Gütersloh |
| **16.04.2021** | RG Stuttgart | **23.09.2021** | RG Ost |
| **26.04.2021** | AK Sozial | **01.10.2021** | RG Karlsruhe |
| **26.04.2021** | RG Ost | **15.10.2021** | RG Ulm |
| **06.05.2021** | RG Gütersloh | **22.10.2021** | RG Nürnberg |
| **18.06.2021** | RG Karlsruhe | **22.10.2021** | RG Stuttgart |
| **25.06.2021** | RG Ulm | **29.10.2021** | RG München |
| **25.06.2021** | RG Nürnberg | **23.11.2021** | RG Ost |
| **25.06.2021** | RG München | **25.11.2021** | RG Gütersloh |
| **02.07.2021** | RG Stuttgart | | |

## Bitte beachten Sie:

Aufgrund anhaltender Corona-Beschränkungen bitten wir Sie sich vorab zu informieren, welche der Termine als Präsenztreffen und welche online stattfinden.

**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:** www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

**TWITTER:** www.twitter.com/bvd_datenschutz

**LinkedIn:** www.linkedin.com/company/berufsverband-der-datenschutzbeauftragten

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

**RSS-Feed:** 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

# Jetzt 3 Monate ZD kostenlos testen und Geschenk sichern!

**IHR GESCHENK**

**SONDERAUSGABE DER AUSKUNFTS-ANSPRUCH NACH ART. 15 DS-GVO**

## 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. ‣ 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.

**ZD – Zeitschrift für Datenschutz**

11. Jahrgang. 2021. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

**Jahresabonnement € 279,–**
**Vorzugspreis für BvD-Mitglieder,**
**für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS**
**sowie für ausgewählte Kooperationspartner € 219,–**

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 15,– jährlich.

**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
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK