Ausgabe 01/2023

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Seite 20

DAS NEUE FERN-MELDEGEHEIMNIS

Dürfen Arbeitgeber auf dienstliche E-Mail-Postfächer trotz erlaubter Privatnutzung zugreifen?
Stefan Sander, LL.M., B.Sc.

Seite 10

WENN AUTOS OHNE DATEN NICHT MEHR ROLLEN

Der Verbraucherzentrale Bundesverband (vzbv) schlägt einen Mobilitätsdatenwächter vor, um die Akzeptanz einer digitalisierten Verkehrswende zu erhöhen.
Marion Jungbluth

Seite 48

"WIR SEHEN NACH WIE VOR EINEN GROSSEN BERATUNGSBEDARF."

Interview mit der Berliner Datenschutzbeauftragten Meike Kamp

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

https://mastodon.social/@bvd@privacyofficers.social

www.linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BvD e.V.
DATENSCHUTZ GESTALTEN

Jetzt anmelden: **www.bvdnet.de/datenschutztag**

Jetzt anmelden!

2023

2. Datenschutztag Hessen & Rheinland-Pfalz

für behördliche, kommunale und betriebliche Datenschutzbeauftragte

05.07.2023 | Metropolitan Hotel by Flemings Frankfurt/Main

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

ONLINE-ANMELDUNG:
www.bvdnet.de/datenschutztag

Eine gemeinsame Veranstaltung von BvD e.V. und dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) und dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

DER HESSISCHE BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

BvD e.V. DATENSCHUTZ GESTALTEN

Liebe Leserinnen und Leser,

am 25. Mai feiert die DSGVO ihren 5. Geburtstag. Ich erinnere mich noch lebhaft daran, wie wir als Verband der Datenschutzbeauftragten die Einführung dieses regulatorischen Meilensteins sowohl im Vorfeld als auch nach Inkrafttreten intensiv begleitet haben. Das geschah auf mehreren Ebenen, sowohl in Form von politischer Interessenvertretung als auch in Form von Informationen und Qualifizierungsmaßnahmen für die BvD-Mitglieder.

Mittlerweile sind wir im Großen und Ganzen auf einem guten Niveau angekommen, was die Auslegung der DSGVO und deren Implementierung angeht – auch wenn der Aufbau eines Datenschutzmanagements, wie wir alle wissen, nie ganz abgeschlossen, sondern ein stetiger Prozess ist. Das ist allerdings kein Grund, sich zurückzulehnen, denn Brüssel beschert uns eine ganze Batterie neuer Regularien, mit denen sich Datenschutzprofis nun inhaltlich auseinanderzusetzen haben. Vieles davon hängt mit der im Februar 2020 veröffentlichten europäischen Datenstrategie zusammen – beispielhaft seien der Data Governance Act, der Digital Services Act, der Data Act oder der AI Act genannt. Die Wechselwirkungen dieser Rechtsakte mit der DSGVO zu verstehen, wird uns Datenschutzbeauftragten, aber auch den Aufsichtsbehörden in der nahen Zukunft einiges abverlangen. Das sehen auch die Aufsichtsbehörden so, wie Sie im Interview mit Meike Kamp, der neuen Berliner Beauftragten für Datenschutz und Informationsfreiheit auf Seite 48 lesen können.

Die neuen Rechtsakte bedeuten aber nicht nur einen zusätzlichen Aufwand für Datenschutzbeauftragte und einen gestiegenen Anspruch an ihre Qualifikation, sie bieten auch Chancen für unseren Berufsstand. Und genau aus diesem Blickwinkel nimmt derzeit eine Arbeitsgruppe im Vorstand die aktuellen Entwicklungen in den Blick.

Die Fragen, mit denen sich die Arbeitsgruppe befasst, sind beispielsweise: Inwiefern wird sich das Berufsbild beziehungsweise das Betätigungsfeld von Datenschutzbeauftragten in den kommenden Jahren voraussichtlich wandeln? Und inwieweit muss die Rolle der DSB weiterentwickelt werden, um diese an die im Wandel befindliche Rahmenbedingungen anzupassen? Das Projekt ist längerfristig angelegt, und es ist geplant, neben verbandsinternen Gremien auch geeignete externe Kooperationspartner einzubinden. Neben der politischen Begleitung dieser Entwicklungen geht es dabei auch um das Thema der vorausschauenden Qualifizierung.

Der Arbeitstitel für das Projekt lautet „Next Level DPO“ und wir werden es auf der Mitgliedversammlung am 09. Mai vorstellen. Ich würde mich sehr freuen, Sie dort oder bei den anschließenden Verbandstagen zu treffen. Denn der BvD lebt vom Austausch und vom Einsatz seiner Mitglieder für die gemeinsamen Ziele, wie beispielsweise der Weiterentwicklung des Berufes und die Festigung des Images der Datenschutzbeauftragten als kompetente Lotsen der Digitalisierung.

Doch nun wünsche ich Ihnen zunächst eine anregende Lektüre Ihrer aktuellen Ausgabe der BvD-News.

Ihr

Thomas Spaeing

INHALTSVERZEICHNIS

IM FOKUS

DATENSCHUTZRECHT

DATENSCHUTZPRAXIS

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
https://mastodon.social/@bvd@privacyofficers.social
www.linkedin.com/company/berufsverband-der-datenschutzbeauftragten
www.bvdnet.de/feed/

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

Fotos (sofern nicht anderweitig ausgewiesen):
Fotos: 123RF, Adobe Stock

Lektorat:
Frank Spaeing, Regina Mühlich

Anzeigen:
Christina Denz
Kooperationen:
Nadja Bunk, Karsten Füllhaase
(bvd-news@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.

AUFSICHTSBEHÖRDEN

GESELLSCHAFT

AUS DEM VERBAND

REZENSIONEN

TERMINE / SERVICE UND ONLINE-SEMINARE

© Bundesverfassungsgericht | foto USW. Uwe Stohrer, Freiburg

GESETZLICHE GRUNDLAGEN ZUR AUTOMATISIERTEN DATENANALYSE TEILWEISE VERFASSUNGSWIDRIG

Maria Christina Rost, Ines Walburg LL.M.

Der Erste Senat des Bundesverfassungsgerichts hat mit Urteil vom 16. Februar 2023[1] entschieden, dass § 25a Abs. 1 Alt. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) und § 49 Abs. 1 Alt. 1 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei (HmbPolDVG) verfassungswidrig sind. Beide Vorschriften verstoßen gegen die informationelle Selbstbestimmung aus Artikel 2 Abs. 1 in Verbindung mit Art. 1 Absatz 1 Grundgesetz (GG), soweit sie sich auf die vorbeugende Bekämpfung von Straftaten beziehen.

Die Verfassungsbeschwerden betrafen die landesrechtlichen Ermächtigungen der Polizei zur automatisierten Datenanalyse oder -auswertung. Mit dieser Entscheidung hat das Bundesverfassungsgericht sich mit der Frage auseinandergesetzt, welche Anforderungen an Rechtsgrundlagen zu stellen sind, die die Polizei ermächtigen, gespeicherte personenbezogene Daten mittels automatisierter Anwendung im Rahmen einer Datenanalyse (§ 25a HSOG) oder einer Datenauswertung (§ 49 HmbPolDVG) weiter zu verarbeiten. Allerdings hat das Bundesverfassungsgericht die Verfassungsbeschwerden nur insoweit für zulässig erklärt, soweit sie gegen die Eingriffsschwelle in § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG – Datenanalyse oder -auswertung zur vorbeugenden Bekämpfung von Straftaten – gerichtet sind; die Befugnis zur Abwehr von Gefahren nach § 25a Abs. 1 Alt. 2 HSOG und § 49 Abs. 1 Alt. 2 HmbPolDVG bleibt ausdrücklich unberührt.[2]

In Hessen kommt seit 2018 die Auswertungs-Software Gotham der US-Firma Palantir zum Einsatz. Das auf hessische Verhältnisse angepasste Analyse-Tool trägt in Hessen die Bezeichnung hessenDATA. Mit diesem kann die hessische Polizei alle bei ihr zu unterschiedlichen Zwecken gespeicherten Daten zusammenführen und nach vielfältigen Kriterien auswerten. Zugegriffen wird dabei auch auf polizeiliche Datenbanken wie POLAS (Polizeiauskunftssystem) und ComVor (Vorgangsbearbeitungssystem für sämtliche Verfahren).

Mit dem Einsatz einer automatisierten Anwendung zur Datenanalyse oder -auswertung wie hessenDATA sind viele datenschutzrechtliche Fragen verbunden. Daher waren unter anderem der Bundesbeauftragte für den Datenschutz, Prof. Ulrich Kelber, der Hamburgische Datenschutzbeauftragte Thomas Fuchs sowie der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Prof. Dr. Alexander Roßnagel, vom Bundesverfassungsgericht als sachkundige Dritte zur mündlichen Verhandlung am 20. Dezember 2022 geladen worden und konnten dort ihre datenschutzrechtliche Expertise einbringen. Neben rechtlichen Fragen wurden überdies Fragen im Zusammenhang mit der Funktionsweise des Analyse-Tools, zu dessen Einsatz und zu seiner technischen Gestaltung erörtert.

Das Gericht hat nun mit seinem Urteil die dort vom Bundes- und den Landesbeauftragten vorgetragenen Bedenken bestätigt. Diese Entscheidung hat bundesweite Tragweite, weil viele andere Polizeibehörden diese Software ebenfalls nutzen wollen und hierfür teilweise schon Vorbereitungen getroffen haben. Nun müssen dafür gesetzliche Grundlagen geschaffen werden, die den Anforderungen des Gerichts genügen.

[1] Urteil des BVerfG vom 16.02.2023, Az. 1 BvR 1547/19 und 1 BvR 2634/20.

[2] Urteil des BVerfG vom 16.02.2023 Rn. 47 und 49.

BfDI Ulrich Kelber sagte zur Entscheidung:

„Das Bundesverfassungsgericht hat jetzt Kriterien formuliert, unter denen die Polizeibehörden Analysesysteme für polizeiliche Datenbestände einsetzen dürfen. Das betrifft auch den Einsatz von Künstlicher Intelligenz. Dieses Grundsatzurteil wird sich bundesweit auswirken. Ich begrüße diese Entscheidung, denn sie schafft sowohl für die Bürgerinnen und Bürger, als auch für die Polizei Rechtssicherheit." (Pressemitteilung 4/23[3])

Thomas Fuchs, der Landesdatenschutzbeauftragte für Hamburg begrüßte ebenfalls das Urteil:

„Das Gericht ist im Wesentlichen unserer Argumentation gefolgt, dass die durch neue Datenauswertungstechnologien möglichen schweren Grundrechtseingriffe nur aufgrund eindeutiger rechtlicher Grundlagen erfolgen können. Dies war durch das sehr unbestimmte Hamburgische Gesetz nicht gegeben. Darüber hinaus gibt das Urteil wichtige Hinweise für die Möglichkeiten und Grenzen beim Einsatz automatisierter Systeme. Die Hamburgische Bürgerschaft ist nun aufgefordert, dies neu und grundrechtskonform zu regeln. Bei der Gelegenheit sollten auch andere polizeiliche Eingriffsnormen nachgeschärft und mit der aktuellen Rechtsprechung des BVerfG in Einklang gebracht werden".[4]

Auch der Hessische Datenschutzbeauftragte Alexander Roßnagel begrüßte die Entscheidung des Bundesverfassungsgerichts.

„Es zeigt, wie wichtig es ist, dass der Gesetzgeber den geeigneten gesetzlichen Rahmen für den Einsatz moderner Analysesoftware in der Polizeiarbeit und verhältnismäßige Grenzen zum Schutz der Grundrechte schafft." Aus seiner Sicht schließen sich Datenschutz und Digitalisierung nicht aus, sie gehen Hand in Hand, wenn diese Fragen von Anfang an gemeinsam beantwortet werden. Dies gilt auch für das Gesetzgebungsverfahren, dass jetzt bis zum 30. September 2023 abgeschlossen sein muss.[5]

Die Kernaussagen des Urteils hat das Bundesverfassungsgericht in fünf Leitsätzen zur Verfassungskonformität der automatisierten Datenanalyse zusammengefasst.

1. Eingriff in die informationelle Selbstbestimmung

Der erste Leitsatz des Urteils lautet: *„Werden gespeicherte Datenbestände mittels einer automatisierten Anwendung zur Datenanalyse oder -auswertung verarbeitet, greift dies in die informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) aller ein, deren Daten bei diesem Vorgang personenbezogen Verwendung finden."*

Das Bundesverfassungsgericht führt hierzu in den Urteilsgründen aus, dass der Gesetzgeber mit der automatisierten Auswertung gespeicherter Daten eine weitere Nutzung früher erhobener Daten über den ursprünglichen Anlass hinaus erlaubt und dadurch ein neuer Grundrechtseingriff begründet wird, der verfassungsrechtlich nach dem Grundsatz der Zweckbindung gerechtfertigt werden muss.[6]

Mit dieser Feststellung hat sich das Bundesverfassungsgericht eindeutig zugunsten eines erneuten Grundrechtseingriffs durch die Datenanalyse oder -auswertung bereits bei der Polizei gespeicherter personenbezogener Daten positioniert.

2. Eingriffsgewicht und Anforderung an verfassungsrechtliche Rechtfertigung

Im zweiten Leitsatz werden das Eingriffsgewicht und die Anforderungen an die verfassungsrechtliche Rechtfertigung betrachtet: *„Das Eingriffsgewicht einer automatisierten Datenanalyse oder -auswertung und die Anforderungen an deren verfassungsrechtliche Rechtfertigung ergeben sich zum einen aus dem Gewicht der vorausgegangenen Datenerhebungseingriffe; insoweit gelten die Grundsätze der Zweckbindung und Zweckänderung. Zum andern hat die automatisierte Datenanalyse oder -auswertung ein Eigengewicht, weil die weitere Verarbeitung durch eine automatisierte Datenanalyse oder -auswertung spezifische Belastungseffekte haben kann, die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen; insoweit ergeben sich aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne weitergehende Rechtfertigungsanforderungen."*

Der 1. Senat setzt sich im Urteil intensiv mit der Bedeutung und der Reichweite der Zweckbindung und Zweckänderung von erhobenen personenbezogenen Daten auseinander. Dabei stellt das Gericht fest, dass diese Auswertungen einen eigenen und tiefen Eingriff in die Grundrechte der betroffenen Personen darstellen können, weil sie neues Wissen über diese generieren.

Das Bundesverfassungsgericht verweist zudem darauf, dass, sofern der Gesetzgeber die Nutzung von Daten über den konkreten Anlass und rechtfertigenden Grund einer Datenerhebung hinaus erlaubt, er hierfür eine eigene Rechtsgrundlage schaffen muss.[7] Folglich stellt das Gericht explizit fest, dass für die Datenanalyse oder -auswertung eine Rechtsgrundlage erforderlich ist.

[3] https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2023/04_BVerfG-Urteil-Datenanalyse.html?nn=251944

[4] https://datenschutz-hamburg.de/pressemitteilungen/2023/02/2023-02-16-bverfg

[5] https://datenschutz.hessen.de/presse/urteil-des-bundesverfassungsgerichts-rechtsgrundlage-fuer-hessendata-verfassungswidrig

[6] Urteil des BVerfG vom 16.02.2023, Rn. 50.

[7] Urteil des BVerfG vom 16.02.2023, Rn. 55.

© Bundesverfassungsgericht | lorenz.fotodesign, Karlsruhe

3. Steuerung der Eingriffsintensität durch den Gesetzgeber

Die dritte Kernaussage des Urteils betrifft die Eingriffsintensität. *„Diese weitergehenden Anforderungen an die Rechtfertigung einer automatisierten Datenanalyse oder -auswertung variieren, da deren eigene Eingriffsintensität je nach gesetzlicher Ausgestaltung ganz unterschiedlich sein kann. Das Eingriffsgewicht wird insbesondere durch Art und Umfang der verarbeitbaren Daten und die zugelassene Methode der Datenanalyse oder -auswertung bestimmt. Der Gesetzgeber kann die Eingriffsintensität durch Regelungen zu Art und Umfang der Daten und zur Begrenzung der Auswertungsmethode steuern."*

Die Anforderungen an eine automatisierte Datenanalyse oder -auswertung und deren gesetzliche Regelung bestimmen sich somit auch nach Art und Umfang der Daten, auf die mit der Maßnahme zugegriffen werden soll. Die Spanne kann hierbei von einer sehr schlichten Form des Abgleichs einer überschaubaren Zahl von Daten näher eingegrenzter Herkunft bis hin etwa zur Erstellung von genaueren Bewegungs-, Verhaltens- oder Beziehungsprofilen reichen – letzteres würde einen schweren Eingriff in die informationelle Selbstbestimmung darstellen.[8]

4. Normenklar und hinreichend bestimmt

Leitsatz 4 befasst sich mit der Voraussetzung der Rechtfertigung von schwerwiegenden Eingriffen durch die automatisierte Datenanalyse. *„Ermöglicht die automatisierte Datenanalyse oder -auswertung einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung, ist dies nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten, also nur zum Schutz besonders gewichtiger Rechtsgüter, sofern für diese eine zumindest hinreichend konkretisierte Gefahr besteht. Das Erfordernis einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter ist nur dann verfassungsrechtlich verzichtbar, wenn die zugelassenen Analyse- und Auswertungsmöglichkeiten durch Regelungen insbesondere zur Begrenzung von Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden normenklar und hinreichend bestimmt in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahmen erheblich gemindert ist."*

Das Bundesverfassungsgericht führt hierzu in den Urteilsgründen unter anderem aus, dass, soweit sich Maßgaben zur Eingrenzung zulässiger Datenverarbeitung bereits aus den Vorschriften des allgemeinen oder des polizeilichen Datenschutzrechts ergeben, deren Anwendbarkeit auf die Befugnis zur Datenanalyse oder -auswertung sowohl für die jeweilige Behörde als auch für die Bevölkerung hinreichend deutlich erkennbar sein muss.[9] Will der jeweilige Gesetzgeber die Eingriffsintensität der automatisierten Datenanalyse oder -auswertung verringern, um diese auch im Vorfeld zu einer konkretisierten Gefahr einzusetzen, muss er dafür grundlegende Vorgaben zur Art und Umfang der in der automatisierten Datenanalyse oder -auswertung verwendbaren Daten selbst regeln.[10]

[8] Urteil des BVerfG vom 16.02.2023, Rn. 72 und 73.

[9] Urteil des BVerfG vom 16.02.2023 Rn. 114.

[10] Urteil des BVerfG vom 16.02.2023, Rn. 115.

5. Aufgaben an Gesetzgeber und Verwaltung

Das Bundesverfassungsgericht definiert im 5. Leitsatz die Anforderungen an die gesetzliche Grundlage zur Anwendung von Analyse-Software der Polizei wie folgt: *„Grundsätzlich kann der Gesetzgeber den Erlass der erforderlichen Regelungen zu Art und Umfang verarbeitbarer Daten und zu den zulässigen Datenverarbeitungsmethoden zwischen sich und der Verwaltung aufteilen. Er muss aber sicherstellen, dass unter Wahrung des Gesetzesvorbehalts insgesamt ausreichende Regelungen getroffen werden.*

a) Der Gesetzgeber muss die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben.

b) Soweit er die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigt, hat der Gesetzgeber zu gewährleisten, dass die Verwaltung die für die Durchführung einer automatisierten Datenanalyse oder -auswertung im Einzelfall maßgeblichen Vorgaben und Kriterien in abstrakt-genereller Form festlegt, verlässlich dokumentiert und in einer vom Gesetzgeber näher zu bestimmenden Weise veröffentlicht. Das sichert auch die verfassungsrechtlich gebotene Kontrolle, die insbesondere durch Datenschutzbeauftragte erfolgen kann.“

Was kommt nun auf die beiden Bundesländer zu? § 49 Abs. 1 Alt. 1 HmbPolDVG ist nichtig und § 25a Abs. 1 Alt. 1 HSOG ist mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG unvereinbar. Der Hessische Gesetzgeber hat jedoch die Möglichkeit, § 25a HSOG spätestens bis zum 30. September 2023 zu überarbeiten. Bis zu einer Neuregelung oder längstens bis zu diesem Datum gilt die Norm fort. Die befristete Anordnung der Fortgeltung wurde allerdings mit Blick auf die betroffenen Grundrechte eingeschränkt.

Auch Hamburg muss sich mit seiner Landesvorschrift auseinandersetzen und sie an die Anforderungen der Entscheidung angepasst neu erlassen.

Diese Entscheidung entfaltet aber nicht nur für die beiden Bundesländer Hessen und Hamburg Relevanz, sondern auch etwa in Nordrhein-Westfalen und in Bayern. So hat Bayern im Frühjahr 2022 einen Rahmenvertrag mit Palantir zur Nutzung von VeRA (= Verfahrensübergreifende Recherche und Analyse) unterschrieben, der auch anderen Polizeibehörden von Bund und Ländern eine Anwendung ermöglichen würde.

Das Urteil ist auch insoweit zukunftsweisend, als es sowohl die verfassungsrechtlichen Kriterien für die Zusammenführung und Auswertung von Polizeidaten aus unterschiedlichen Quellen als auch den Einsatz von Big Data und Künstlicher Intelligenz formuliert.

WAS KOMMT AUF HESSEN UND HAMBURG ZU

„Unter Zugrundelegung des in der Hessischen Praxis gewählten Konzepts wird angeordnet, dass der von der Befugnis des § 25a Abs. 1 Alt. 1 HSOG nur Gebrauch gemacht werden darf, wenn bestimmte, genügend konkretisierte Tatsachen den Verdacht begründen (vgl. BVerfGE 154, 152 <286 Rn. 2019>; 156, <56 Rn. 120>), dass eine besonders schwere Straftat im Sinne von § 100b Abs. 2 StPO begangen wurde und aufgrund der konkreten Umstände eines solchen Einzelfall bestehenden Tatverdachts für die Zukunft mit weiteren gleichgelagerten Straftaten zu rechnen ist, die Leib, Leben oder den Bestand oder die Sicherheit des Bundes oder eines Landes gefährden, wenn das Vorliegen dieser Voraussetzungen und die konkrete Eignung der verwendeten Daten nach § 25a Abs. 1 Alt. 1 HSOG zur Verhütung der zu erwartenden Straftat durch eigenständig auszuformulierende Erläuterung begründet wird und wenn sichergestellt ist, dass keine Informationen in die Datenanalyse einbezogen werden, die aus Wohnraumüberwachung, Online-Durchsuchung, Telekommunikationsüberwachung, Verkehrdatenabfrage, länger andauernde Observation, unter Einsatz von verdeckt ermittelten Personen oder Vertrauenspersonen oder aus vergleichbar schwierigen Eingriffen in die informationelle Selbstbestimmung gewonnen wurden.“[11]

Über die Autorinnen

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

Ines Walburg LL.M.
ist Referatsleiterin, Referat Polizei, Justiz, Rechtsanwälte, Verfassungsschutz beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit

▶ https://datenschutz.hessen.de/

[11] Urteil des BVerfG vom 16.02.2023, Rn. 176.

MARION JUNGBLUTH

WENN AUTOS OHNE DATEN NICHT MEHR ROLLEN

Der zunehmenden Digitalisierung des Mobilitätsektors sowie der damit einhergehenden Vernetzung der Verkehrsteilnehmer:innen fehlt es an Akzeptanz. Um diese Akzeptanz zu schaffen, braucht es einen datenschutzrechtlichen und gesellschaftlichen Dialog sowie eine rechtskonforme technische Umsetzung. Nur so kann der Erfolg der notwendigen Mobilitätswende sichergestellt werden.

Es liegt auf der Hand, dass für eine erfolgreiche Mobilitätswende alle Verkehrsteilnehmer:innen eingebunden werden müssen. Eine Umfrage ergab jedoch, dass Verbraucher:innen nur bedingt oder gar nicht bereit sind, die eigenen Daten freizugeben. Lediglich 17 Prozent der Befragten waren bedingungslos zu einer Datenfreigabe bereit.[1] Die Fahrzeughersteller, die faktisch die Hoheit über alle Fahrzeugdaten haben, tun sich ebenso schwer damit, ihre Daten zu teilen. Das ist ein Problem für den Wettbewerb, für Innovationen und für den Erfolg der Verkehrswende.

Doch was sind **Mobilitätsdaten?** Als Mobilitätsdaten werden alle Daten mit und ohne Personenbezug bezeichnet, die bei der Teilnahme am Verkehr auf öffentlichen Straßen entstehen.[2] Das sind Daten, die sowohl durch das eigene Fahrzeuge als auch durch Fahrzeuge anderer Verkehrsteilnehmer:innen generiert werden. Hinzu kommen alle durch die Verkehrsinfrastruktur erfassten Daten zu einem Fahrzeug oder einer Person – erfasst durch intelligente Lichtzeichenanlagen wie Ampeln, Baustellenblinklichter oder intelligente Schilder. Nicht zuletzt fallen auch Daten von Radfahrenden und Fußgänger:innen darunter, die über entsprechend eingestellte Smartdevices eigene und fremde Mobilitätsdaten verarbeiten.[3]

Bei Mobilitätsdaten handelt es sich also um eine sehr dynamische, vielfältige und umfassende Datenmenge. Die Problematiken, die daraus entstehen, werden in einem Gutachten von Baum, Reiter & Collegen[4] zum Positionspapier „Mobilitätsdatenwächter – digitale Privatheit bei vernetzten Fahrzeugen für alle Verbraucher:innen gewährleisten“[5] des Verbraucherzentrale Bundesverbands (vzbv) dargestellt: Unter anderem hat die Beschaffenheit der Daten zur Folge, dass Ansprüche aus der Datenschutz-Grundverordnung (DSGVO) zu keiner angemessenen Lösung der Bedarfe des Mobilitätssektors führen. Denn die in der DSGVO beschriebenen Betroffenenansprüche beschreiben punktuelle Ansprüche, das heißt Momentaufnahmen. Bei vernetzten Fahrzeugen, die beispielsweise im Verkehr Kollisionen vermeiden sollen, wäre aber eine kontinuierliche Datenauskunft in Echtzeit notwendig. Wie diese kontinuierlichen Abfragen geregelt werden können, wird mit den Auskunfts- und Datenübertragungsansprüchen aus der DSGVO jedoch nicht beantwortet.

Dazu kommt, dass automatisierte Fahrzeuge für ihre Funktion umfangreiche Daten benötigen. Bis zur Markteinführung muss man etwa davon ausgehen, dass mindestens zwei Millionen Einzelbilder aufbereitet und ausgewertet werden müssen, um einen brauchbaren Code zur Steuerung eines Fahrzeuges zu schreiben. Zur Steigerung der Sicherheit müssen ungefähr 20 Millionen weitere Bilder ausgewertet werden. Dazu kommen die Bilder oder Daten, die unvermeidbar im laufenden Betrieb der Fahrzeuge verarbeitet werden müssen sowie die Daten aus weiteren Systemen – beispielsweise Sensoren und Radaren.

Darüber hinaus werden auch für andere Verkehrsoptimierungen Daten benötigt – beispielsweise für eine durch künstliche Intelligenz gesteuerte Verkehrslenkung, eine dynamische (stauvermeidende) Navigation, einen bedarfsgesteuerten ÖPNV und so weiter.

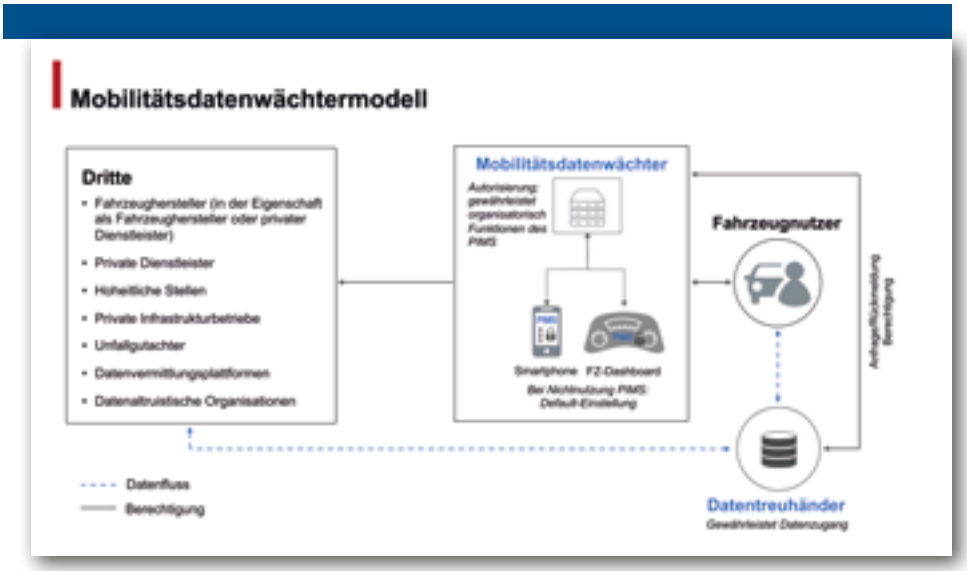
[1] Kantar Public Germany: Verbraucherbefragung zu den Themen Schuhe und Autonomes Fahren, 2021, Basis: 1033 Personen.

[2] Die Straßengesetze in den Bundesländern definieren dabei regelmäßig und in der Hauptsache „Straßen, Wege und Plätze, die dem öffentlichen Verkehr gewidmet sind“ als öffentliche Straße. Siehe z. B. § 2 Berliner Straßengesetz (BerlStrG) und § 2 Straßengesetz Baden-Württemberg.

[3] Unter Verarbeitung versteht man: „…jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“, vgl. Art. 4 Ziffer 2 DSGVO.

[4] https://www.vzbv.de/sites/default/files/2022-11/22-11-15_Gutachten_Mobilit%C3%A4tsdatenw%C3%A4chter_BRC_2022-15-11_Clean_Finalversion.pdf

[5] https://www.vzbv.de/sites/default/files/2022-11/22-11-18-MR_vzbv_Positionspapier%20Mobilit%C3%A4tsdatenw%C3%A4chter_clean_Finalversion_PDF_0.pdf



Grafik: Reiter, Julius; Methner, Olaf; Schenkel, Bénédict in Kooperation mit Bönninger, Jürgen: Einführung eines „Mobilitätsdatenwächters" für eine verbrauchergerechte Datennutzung, 2022, Düsseldorf.

Ein so dynamisches Umfeld bedarf flexibler und rechtskonformer Lösungen. Die Regelungen der DSGVO sind dabei keine Bedrohung. Vielmehr sollten sie als Leitplanken der Digitalisierung und Vernetzung gesehen werden. Ursprünglich war geplant, dass im Jahr 2023 der legislative Prozess für den motorisierten Verkehr begonnen wird. Ziel war es, auf europäischer Ebene eine sektorspezifische Regelung für Fahrzeugdaten zu kodifizieren. Diese sollte den EU Data Act ergänzen. Unverständlicher Weise kommt es jetzt bei der sektorspezifischen Regelung zu Verzögerungen.[6]

Eine solche Verzögerung ist mit Blick auf die sich dynamisch entwickelnde Lage nicht nachvollziehbar. Statt auf die Entscheidung auf EU-Ebene zu warten, sollte dringend eine hilfsweise, nationale Lösung gesucht werden. Für eine solche nationale Lösung bietet sich das von der deutschen Regierungskoalition angestrebte Mobilitätsdatengesetz[7] an. Dabei plant die Regierung, im Verkehrssektor Datentreuhänder zu schaffen und Datentreuhändermodelle zu etablieren.[8] Als Ergänzung zum Datentreuhändermodell schlägt der vzbv im Zuge dessen das **Modell eines Mobilitätsdatenwächters** vor.

Das Modell des vzbv besteht im Wesentlichen aus der Trias von den Betroffenen – Verkehrsteilnehmer:innen bzw. Verbraucher:innen – sowie einem jeweils neutralen Mobilitätsdatenwächter und dem Datentreuhänder. Der Mobilitätsdatenwächter wird vom Betroffenen über eine Eingabemaske in einer App oder im Display des Fahrzeugs individuell eingestellt. Diese Einstellung kann jederzeit neu vorgenommen werden und bildet alle Rechtmäßigkeitsgründe einer Datenverarbeitung ab. Über die Einstellungen ist der Wächter in der Lage, Datenbedarfe von Dritten beim Datentreuhänder nach den Vorgaben der Verbraucher:innen freizugeben oder abzuweisen. Zu den Dritten gehören im Übrigen auch die Hersteller selbst. Die Eingabemaske basiert auf dem System eines PIMS ("personal information management system"). Das PIMS ist gewissermaßen das Steuerungswerkzeug. Eine Datenfreigabe kann nach den Vorgaben der jeweiligen Betroffenen auch anonymisiert oder pseudonymisiert erfolgen. Über das PIMS erhält man auch jederzeit den jeweiligen Status quo seiner datenschutzrechtlichen Einstellungen, Auskunft über Datenanfragen sowie eine Übersicht, welche Daten wann an Dritte gegeben oder angefragt wurden. Das PIMS ist also zusätzlich eine Informationsquelle und soll den Auskunftsrechten von Betroffenen gerecht werden. Das Mobilitätsdatenwächtermodell stellt eine weitere Möglichkeit dar, die uneingeschränkt bestehenden Rechte nach der DSGVO geltend zu machen. Eine Umsetzung des Mobilitätsdatenwächtermodells würde die Datenhoheit der Fahrzeughersteller durchbrechen. Zudem ist durch die Kontrollverlagerung zu den Verbraucher:innen und die permanent gegebene Transparenz und Kommunikation der Datenverarbeitungsvorgänge mit einer sehr hohen Akzeptanz der Verbraucher:innen zu rechnen.

Für das Mobilitätsdatengesetz werden derzeit die Positionen der Stakeholderbeteiligungen ausgewertet. Die Erkenntnisse sollen Ende März 2023 vorliegen. Bis Referentenentwurf und Kodifizierung vorliegen, wird man sich bereits im Jahr 2024 befinden. Nichtsdestotrotz hat die Bundesregierung es jetzt in der Hand, die dringend benötigte sektorspezifische Zugangsregulierung zu den Fahrzeugdaten zu forcieren. Das Mobilitätsdatengesetz muss dabei ein Katalysator der Digitalisierung sein und darf nicht zu einem Prellbock werden. Damit würde die Mobilitätswende eine wichtige Hürde nehmen und die Akzeptanz der Verarbeitung von Mobilitätsdaten gestärkt werden.

Über die Autorin

Marion Jungbluth
leitet das Team Mobilität und Reisen beim Verbraucherzentrale Bundesverband (vzbv) und ist seit 2013 Mitglied im Runden Tisch automatisiertes Fahren des Bundesministeriums für Digitales und Verkehr (BMDV)

[7] SPD, BÜNDNIS 90/DIE GRÜNEN, FDP: Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021-2025, S. 52, https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1, 10.02.2023.

[8] Siehe Fußnote 7, dort S. 17.

WAS DAS GEPLANTE HINWEISGEBERSCHUTZ-GESETZ LEISTEN MUSS

Lea Vietze, Vincent Stöber

Der Milliarden-Skandal um Wirecard ist nur eines von vielen Beispielen, das zeigt, wie wichtig Meldungen von Hinweisgebenden sein können, um Missstände, Korruptions- und Betrugsfälle frühzeitig aufzudecken. Viele dieser Missstände bleiben lange unentdeckt, aus Angst vor Repressalien für die hinweisgebende Person. Die neue EU-Whistleblower-Richtlinie soll helfen, Hinweisgebende in Zukunft vor diesen Folgen zu schützen. Außerdem trägt sie dazu bei, dass hinweisgebende Personen nicht als Unruhestifter wahrgenommen werden, sondern vielmehr als diejenigen, die dazu beitragen, Probleme im Frühstadium zu erkennen und ihnen entgegenzuwirken. Dabei werden viele personen- und unternehmensbezogene Daten offengelegt. Daher ist es essentiell, dass diese Daten mit den Standards der DSGVO-Richtlinie konform sind. Die Bundesregierung ringt derzeit mit den Bundesländern um einen Kompromiss, wie die EU-Wisthleblower-Richtlinie in deutsches Recht zu fassen ist.

1. Überblick Hinweisgeberschutzgesetz

Das geplante Hinweisgeberschutzgesetz (HinSchG), will hinweisgebende Personen schützen. Diese sind laut Entwurf der Bundesregierung nach § 1 Abs. 1 Personen, "die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen". Des Weiteren werden nach § 1 Abs. 2 "Personen geschützt, die Gegenstand einer Meldung oder Offenlegung sind, sowie sonstige Personen, die von einer Meldung oder Offenlegung betroffen sind".[1]

In der Vergangenheit wurden hinweisgebende Personen oft infolge einer Meldung von Missständen benachteiligt. Damit dies in Zukunft nicht mehr geschieht, ist das Ziel des neuen HinSchG diesen Personen eine Rechtssicherheit zu geben und sie vor diesen negativen Folgen zu schützen. Im Dezember 2019 wurde die EU-Whistleblower-Richtlinie verabschiedet. Die Richtlinie 2019/1937 "zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden", verpflichtet alle Unternehmen mit mehr als 50 Mitarbeitenden ein Verfahren einzurichten, welches sicherstellt, dass Angestellte auf geschützte Weise jede Art von Verdacht, Vorfall und Verstoß melden können, die sie im Unternehmen beobachtet haben.[2]

Anders als die EU-Whistleblower-Richtlinie vorgibt, erweitert das geplante deutsche HinSchG den sachlichen Anwendungsbereich nach § 2 Abs. 1 auf deutsche Vorschriften. Der sachliche Anwendungsbereich umfasst damit nicht nur Verstöße ge-

[1] Gesetzesentwurf der Bundesregierung für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden Abgerufen unter: https://dserver.bundestag.de/btd/20/034/2003442.pdf

[2] EU-Richtlinie 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden. Abgerufen unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L1937&from=de

gen das Unionsrecht, sondern auch nach § 2 Abs. 1 Verstöße, die straf- oder bußgeldbewehrt sind und Verstöße gegen Rechtsvorschriften.[1] Im Dezember 2022 nahm der Bundestag den Entwurf für das HinSchG an und setzte mit der Verabschiedung den weiteren Gesetzgebungsprozess in Gang. Am 10. Februar 2023 wurde das neue HinSchG im Bundesrat besprochen und die Zustimmung verweigert. Dieser Konflikt zwischen dem Bundestag und dem Bundesrat bedeutet, dass das Gesetz voraussichtlich in den Vermittlungsausschuss geht, um einen Kompromiss zu finden. Dies kann allerdings mehrere Monate dauern. Damit verzögert sich das ohnehin schon über ein Jahr zu spät umgesetzte und nun für April geplante HinSchG noch einmal.

2. DPOs als Ombudspersonen für Whistleblowing

Nach § 14 Abs. 1 im bislang vorliegenden Entwurf des HinSchG dürfen Unternehmen Dritte mit der Betreuung der internen Meldestelle beauftragen. Dies bedeutet, dass beispielsweise Datenschutzbeauftragte und / oder Anwaltskanzleien als Ombudspersonen den Kanal betreuen dürfen. Sie gelten nach der EU-Richtlinie als interne Meldestelle. Dabei müssen sie nach § 15 Abs. 1 unabhängig handeln.[3] Entscheidet sich ein Unternehmen dazu, die interne Meldestelle auf eine Ombudsperson auszulagern, bedeutet dies, dass alle Verpflichtungen aus dem HinSchG in den Aufgabenbereich dieser dritten Person fallen. Dies sind alle Verfahren und Folgemaßnahmen nach § 17 und § 18 HinSchG.[3] Dazu gehören unter anderem die Entgegennahme der Fälle, diese zu prüfen und zu untersuchen, Kommunikation mit dem Hinweisgebenden und Berichterstattung an das Unternehmen. Im Zusammenhang mit der praktischen Umsetzung kann dies bedeuten, dass Anwälte und Datenschutzberater:innen alle Hinweisgeber-Kanäle ihrer Mandanten gesammelt betreuen könnten. In Deutschland fallen ca. 89.700 Unternehmen[4] mit mehr als 50 Mitarbeitenden unter die EU-Whistleblower-Richtlinie. Sie sind dazu verpflichtet, sobald das neue HinSchG in Kraft tritt, ihren Mitarbeitenden eine Möglichkeit für das sichere Melden von Verstößen zu bieten und diese vor Repressalien zu schützen.

Um den Schutz personenbezogener Daten während der Übertragung sicherzustellen, können Unternehmen verschiedene Methoden nutzen:

Standardvertragsklauseln (SCC):[*]
Dies sind vorformulierte Klauseln, die in Verträge zwischen Unternehmen mit aufgenommen werden können. Sie dienen dem Schutz von personenbezogener Daten bei der Übermittlung in Drittländer. Dabei kann es sich beispielsweise um Verträge zwischen Softwareunternehmen und deren Cloud-Anbieter handeln, die gewährleisten, dass die personenbezogenen Daten nicht an Drittländer übertragen werden.

Verbindliche Unternehmensregeln (BCR):[**]
Dies sind interne Unternehmensrichtlinien, welche die Übermittlung personenbezogener Daten innerhalb eines Unternehmens regeln und zum Nachweis für einen angemessenen Schutz herangezogen werden können.

Datenschutz-Folgenabschätzung (DPIA):[***]
Der DPIA ist ein Prozess bei der Implementierung einer neuen Software, welcher den Schutz von personenbezogenen Daten prüft. Dabei werden potentielle Auswirkungen auf den Datenschutz geprüft und deren Auswirkungen identifiziert.

Umsetzung technischer Maßnahmen:
Die Sicherheit von personenbezogenen Daten kann zusätzlich durch technische Maßnahmen gestärkt werden. Durch eine (Ende-zu-Ende) Verschlüsselung werden die Daten verschlüsselt, sodass nur Personen mit einer Zugriffsberechtigung diese auslesen können.

[3] Gesetzesentwurf der Bundesregierung für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden; Abgerufen unter: https://dserver.bundestag.de/btd/20/034/2003442.pdf

[4] „Unternehmen in Deutschland: Anzahl der rechtlichen Einheiten in Deutschland nach Beschäftigtengrößenklassen im Jahr 2021", Abgerufen unter: https://de.statista.com/statistik/daten/studie/1929/umfrage/unternehmen-nach-beschaeftigtengroessenklassen/

[*] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates; Abgerufen unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914&from=DE

[**] Binding Corporate Rules (BCR); https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

[***] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung); Abgerufen unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

3. DSGVO trifft Whistleblowing

Besonders bei einem sensiblen Thema wie Whistleblowing ergeben sich viele Fragen und Zweifel hinsichtlich Datenschutz und Datensicherheit. Whistleblower-Systeme befassen sich mit einer großen Menge an kritischen personen- und unternehmensbezogenen Daten. Daher ist es von zentraler Bedeutung, dass alle Daten im System mit der allgemeinen DSGVO-Richtlinie konform sind.

Diese regelt den "Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr", die Verarbeitung von personenbezogenen Daten sowie die Übertragung dieser Daten in Drittländer.[5] Unternehmen, die Daten von Personen speichern, verarbeiten oder übertragen, müssen der DSGVO entsprechen. Um Daten in Drittländer wie die USA zu übertragen, verlangt die DSGVO, dass personenbezogene Daten mit einer ausreichenden Garantie geschützt werden.

4. Auswahl eines geeigneten Meldekanals

Um der neuen EU-Whistleblower-Richtlinie gerecht zu werden, muss eine geeignete Meldestelle eingerichtet werden, dabei dürfte es auch im auszuhandelnden Kompromiss zwischen Bundestag und Bundesrat bleiben. In der Vergangenheit haben Unternehmen physische Briefkästen, Telefon-Hotlines oder E-Mail-Dienste genutzt, um Meldungen von Hinweisgebenden zu erfassen. Viele dieser Methoden sind nicht mit den Vorschriften zum Schutz von hinweisgebenden Personen oder der DSGVO vereinbar.

Eine Softwarelösung ist gerade mit Hinblick auf das anonyme Melden und die anonyme Kommunikation zwischen der/dem Hinweisgebenden und dem/der Fallbearbeiter:in die bestgeeignete Lösung für einen Whistleblowing-Kanal.

4.1 Anonymes Whistleblowing?

Beim anonymen Whistleblowing handelt es sich um das Melden möglicher Missstände an eine/n Arbeitgeber:in oder eine/n externe/n Vertreter:in, ohne persönliche Informationen preiszugeben.

Da ein Whistleblower immer noch als Unruhestifter:in wahrgenommen wird und nicht als der-/diejenige, der/die dazu beitragen kann ein Problem im Frühstadium zu erkennen, zögern viele Mitarbeitende aus Angst vor Konsequenzen, eine Meldung abzugeben. Die Möglichkeit anonym zu bleiben sorgt dafür, dass sich die Mitarbeitenden wohler fühlen, wenn sie Missstände melden, anstatt zu schweigen und die Angelegenheit eskalieren zu lassen. Um jedoch sicherzustellen, dass die Kommunikation in einem anonymen Hinweisgebersystem richtig abläuft, benötigt ein Unternehmen ein spezielles Whistleblowing-System.

	Physischer Briefkasten	Telefon - Dienst	Email - Dienst	Whistleblower Software
Sicherheitsstufe	✗	✗	?	✓
Der Whistleblower kann entscheiden ob er/sie vertraulich oder anonym melden möchte	✓	✗	✗	✓
Gespräch mit Hinweisgebenden kann nach Meldung fortgesetzt werden	✗	✓	✓	✓
Ist das System konform mit der DSGVO, der EU-Richtlinie und Schrems II?	✗	✗	?	✓

Eine Softwarelösung ist gerade mit Hinblick auf das anonyme Melden und die anonyme Kommunikation zwischen der/dem Hinweisgebenden und dem/der Fallbearbeiter:in die bestgeeignete Lösung für einen Whistleblowing-Kanal.

[5] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung); Abgerufen unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

[6] Gesetzesentwurf der Bundesregierung für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden; Abgerufen unter: https://dserver.bundestag.de/btd/20/034/2003442.pdf

4.2 Schutz von Whistleblowern

Der Schutz der Anonymität des Whistleblowers wird durch die Nichtaufbewahrung der IP-Adresse oder Rechner-ID des Hinweisgebenden und durch die Entfernung von Metadaten von Whistleblower-Software garantiert. Das System stellt sicher, dass keine Informationen gespeichert werden, die nicht ausdrücklich von der hinweisgebenden Person angegeben wurden. Auf der Meldeseite werden keine Cookies und kein Tracking verwendet. Zusätzlich kann das System alle Metadaten aus allen in das System hochgeladenen Dateien entfernen. Metadaten können Informationen über die Identität des Whistleblowers preisgeben. Dies können Informationen sein, die zum Beispiel ein Foto transportiert, darunter Daten zum Standort, wo das Foto aufgenommen wurde, die Uhrzeit und der/die Eigentümer:in des Smartphones. Das System löscht diese Informationen, bevor die Dateien an den/die Sachbearbeiter:in übermittelt werden. Um die Anonymität auch bei mündlichen Meldungen zu gewährleisten, kann das System die Stimme des Hinweisgebenden automatisch verzerren. Somit ist neben dem schriftlich anonymen Melden auch das mündlich anonyme Melden möglich. Bei der Erstellung eines Falles kann sich die hinweisgebende Person entscheiden, ob sie den Fall vertraulich oder anonym melden möchte. Sobald ein neuer Fall in das System eingeht, werden die jeweiligen Fallbearbeiter:innen informiert. Nach § 17 und § 18 des geplanten HinSchG muss die Möglichkeit für die weitere Kommunikation mit dem Hinweisgebenden bestehen.[6] Den Fallbearbeiter:innen ist es bei der Fallbearbeitung möglich, über eine Chat-Funktion mit dem Hinweisgebenden vertraulich oder anonym zu kommunizieren. Die hinweisgebende Person kann sich dafür mit einem zufällig generierten Passwort (welches er/sie nach Einreichung eines Falles erhält) erneut in den Fall einloggen. Über diese Chatfunktion kann dem Hinweisgebenden mitgeteilt werden, sobald der Fall bei einem/r Fallbearbeiter:in eingegangen, in Bearbeitung oder geschlossen ist. Ebenfalls kann nach weiteren Beweisen wie Fotos oder Dokumenten gefragt werden.

Über die Autoren

Lea Vietze
ist Solution Specialist bei Whistleblower Software. Sie ist Expertin im Datenschutzbereich und zum Hinweisgeberschutzgesetz und verantwortet die Kommunikation im deutschsprachigen Raum.

Vincent Stöber
ist Partner Manager DACH bei Whistleblower Software. Er ist Experte für digitale Meldekanäle zum Hinweisgeberschutz. Zudem verantwortet er Partnerschaften mit Unternehmen im deutschsprachigen Raum.

▶ https://whistleblowersoftware.com

Whistleblower Software

Die Whistleblower Software wird auf den BvD-Verbandstagen in Berlin vertreten sein.

DER ZUGANG VON E-MAILS IM RAHMEN DER GELTENDMACHUNG VON BETROFFENENRECHTEN

Nicole Schmidt, Lilly Steinbrecher, LL.B., Laura Toska Genkinger

E-Mails haben in der heutigen Geschäftswelt einen hohen Stellenwert erlangt. Sie ermöglichen eine schnelle und unkomplizierte Kommunikation und sind daher ein wichtiges Instrument für Unternehmen und Privatpersonen. Ein zentraler Aspekt bei der Verwendung von E-Mails ist der Zustellzeitpunkt. Dieser kann, wenn es um die Bestimmung des Fristbeginns geht, im Zusammenhang mit der Ausübung von datenschutzrechtlichen Betroffenenrechten von großer Bedeutung sein.

Nachfolgend wird sich deshalb zunächst mit der Frage auseinandergesetzt, wann eine E-Mail zugegangen ist und wer dabei das Risiko der Beweislast trägt. Gleichzeitig werden die verschiedenen Aspekte der Zustellung von E-Mails betrachtet und die Rechtsprechung von verschiedenen Gerichten in Deutschland und Österreich beleuchtet. Schließlich wird erörtert, ob sich diese Ausführungen auf den Fristbeginn bei der Geltendmachung von Betroffenenrechten nach der DSGVO übertragen lassen.

Der E-Mail-Zugang nach dem BGB

Die Wirksamkeit einer Willenserklärung unter Abwesenden bestimmt sich nach § 130 Abs.1 BGB. Die Willenserklärung wird in dem Zeitpunkt wirksam, in welchem sie dem Abwesenden zugeht. Von der ständigen Rechtsprechung wurde die Zugangsformel entwickelt, dass die Willenserklärung so in den Machtbereich des Empfängers gelangen muss, dass dieser unter normalen Umständen die Möglichkeit hat, vom Inhalt der Erklärung Kenntnis zu nehmen.

Für elektronische Willenserklärungen im Unternehmensverkehr drängt sich die Frage auf, wann eine E-Mail in den Geschäfts- oder Machtbereich gelangt und wann mit der Kenntnisnahme gerechnet werden kann. In diesem Zusammenhang sind mehrere Urteile von großer Bedeutung.

Vergangenen Jahres erließ der BGH ein Urteil[1], welches sich zentral mit dem E-Mail-Zugang beschäftigt. Die Karlsurher Richter entschieden, dass eine E-Mail im geschäftlichen Verkehr jedenfalls dann zugehe, wenn sie auf dem **Mailserver des Empfängers abrufbereit zur Verfügung gestellt** wird und der **Eingang der Nachricht innerhalb der üblichen Geschäftszeiten erfolgt.** Es komme gerade nicht auf die tatsächliche Kenntnisnahme durch den Empfänger an. Die Möglichkeit der Kenntnisnahme werde danach unmittelbar nach Eingang der E-Mail angenommen, sofern dieser innerhalb der Geschäftszeiten erfolgt.

[1] BGH, Urteil vom 06.10.2022, Az. VII ZR 895/21.

Als Machtbereich definiert der BGH den für den Empfang von E-Mail-Nachrichten genutzten Mailserver dann, wenn der Empfänger zum Ausdruck bringt, mittels E-Mail-Kommunikation rechtsgeschäftliche Erklärungen abgeben zu wollen. Dies kann in Form von einer Veröffentlichung der E-Mail-Adresse oder einer sonstigen Handlung im Rechtsverkehr zum Ausdruck kommen. So entschied auch der OGH Österreich, der den E-Mail-Server jedenfalls dann als Machtbereich ansah, wenn vom Empfänger ein Vertrauenstatbestand gesetzt wird, dass er über die E-Mail-Adresse erreichbar ist.[2] Es müsse hinreichend zum Ausdruck kommen, dass mit der Kenntnisnahme elektronischer Post durch den Empfänger gerechnet werden kann. Beispielhaft wird die Übergabe einer Visitenkarte oder das Herantreten einer Person per E-Mail angeführt. Da im österreichischen Recht entsprechende Anforderungen an den Zugang einer Willenserklärung gestellt werden, kann diese Entscheidung durchaus als Vorbild für das deutsche Recht dienen. Die beiden Gerichte stimmen insoweit hinsichtlich der **Bewertung des E-Mail-Postfachs als Machtbereich** überein, jeweils unter der Bedingung, dass ein **zurechenbares Verhalten** für die Erreichbarkeit unter der E-Mail-Adresse gesetzt wird.

Mit seiner Entscheidung hat der BGH an der klassischen Zugangsdefinition festgehalten und die bisher in der Literatur und Rechtsprechung vertretenen Auffassungen zum E-Mail-Zugang teilweise miteinander verknüpft. Offen gelassen wird hingegen die Rechtsfrage, wann eine E-Mail **außerhalb der gewöhnlichen Geschäftszeiten** zugeht. Interessengerecht erscheint einstweilen der herrschenden Ansicht[3] zu folgen und den Zugang der E-Mail am folgenden Geschäftstag anzunehmen.

Zugang eines Schreibens mit Dateianhang

Die bisher erörterte Problematik des Zugangs einer E-Mail wird umso relevanter, wenn das maßgebliche Schreiben im E-Mail-Anhang „versteckt" ist. Das OLG Hamm befasste sich mit dem Zugang einer Abmahnung, welche im Dateianhang versendet wurde, und führte in seinem Urteil aus, dass der Zugang erst erfolgt, wenn der Empfänger den Dateianhang tatsächlich geöffnet hat,[4] mit der Begründung des allgemeinen Virenrisikos in E-Mail-Anhängen und damit verbundener Warnungen könne von dem Empfänger nicht erwartet werden, den Dateianhang zu öffnen. Dies überzeugt nur bedingt, da eine Abkehr von dem allgemeinen Zugangserfordernis stattfindet.[5] Nur wenn der Absender unter einer gänzlich unbekannten E-Mail-Adresse auftritt und die E-Mail einen unseriösen Anschein vermittelt, vermag die Ansicht des Gerichts zu überzeugen.

Wer trägt die Beweislast?

Der **Absender trägt grundsätzlich das Zugangsrisiko und somit die Darlegungs- und Beweislast.**[6] Zur Begründung stellte das Gericht auf das Risiko der Zustellung im Vergleich zur einfachen Post ab und kam zu dem Entschluss, dass das Risiko nicht dem Empfänger der Nachricht aufgebürdet werden kann, weil gerade der Absender die Art der Übermittlung wählt und Möglichkeiten zur Vorbeugung hat.

Diese Ausführungen lassen sich auch auf die Geltendmachung von Betroffenenrechten übertragen. Einerseits ist dies relevant für den Zeitpunkt des Fristbeginns. Im Zweifel muss der Betroffene, der etwa Auskunft möchte, beweisen, dass seine E-Mail zur Geltendmachung seines Betroffenenrechts zugegangen ist. Andererseits kommt die Frage der Beweislast zum Tragen, wenn der Verantwortliche kurz vor Ende der Monatsfrist auf die Betroffenenanfrage reagieren möchte. Der Verantwortliche trägt dann die Beweislast dafür, fristgemäß zu antworten.

Im Sinne der Rechtssicherheit sollte demnach hinreichend dokumentiert werden, dass die E-Mail versendet worden ist. Zu denken wäre an die Anforderung einer Lesebestätigung beim Empfänger. Nach dem oben genannten BGH-Urteil müsste aber der Absender beweisen, dass die E-Mail auf dem fremden E-Mail-Server gespeichert wurde. Eine Übermittlungsbestätigung könnte diesem Erfordernis wohl eher genügen.

In Anlehnung daran ist das Urteil des VG Gelsenkirchen[7] zu nennen, welches sich mit der Fristwahrung bei der elektronischen Versendung von Schriftsätzen gemäß § 55a VwGO auseinandersetzte. Das Gericht führte an, dass das Zugangsrisiko beim Absender liegt und daher gewöhnliche Verzögerungen einzukalkulieren sind. Bedeutung erlangt dies bei der Ergreifung von Sicherheitsmaßnahmen, denn laut dem Gericht müsse zur Einhaltung der Sorgfaltspflicht ein zeitlicher Sicherheitszuschlag bis zum Ablauf der Frist einberechnet werden. Dieser Sicherheitszuschlag müsse mögliche Störungen mitberücksichtigen.

[2] Vgl. OGH Österreich, Entscheidung vom 19.05.2022, Az.9 Ob 86/21v.

[3] Spindler, in: Spindler/Schuster, Recht der elektronischen Medien, 4.Aufl.2019, § 130 Rn.8; OLG Düsseldorf, Urteil vom 19.07.2011, Az.24 U 186/10; Ultsch, NJW 1997, 3007, 3008.

[4] Vgl. OLG Hamm, Urteil vom 09.02.2022, Az.4W 119.

[5] Vgl. auch: Gramespacher, MIR 2022, Dok.027.

[6] Vgl. LAG Köln, Urteil vom 11.01.2022, Az.4 Sa 315.

[7] VG Gelsenkirchen, Urteil vom 07.12.2021, Az.18 K 3240/20.

Betroffenenrechte

Betroffenen stehen nach Art. 15 bis 22 DSGVO bestimmte Rechte zu, wodurch sie die Möglichkeit haben, sich über die Datenverarbeitungen zu informieren. Besonders praxisrelevant ist das Auskunftsrecht nach Art. 15 DSGVO. Laut der LfD Niedersachsen[8] stellt die Nichtbeachtung des Auskunftsrechts im nicht-öffentlichen Bereich den häufigsten Beschwerdegrund dar. Ein Auskunftsantrag per E-Mail ist ein formeller Antrag auf die Übermittlung von bestimmten Informationen, der vom Verantwortlichen innerhalb einer Frist beantwortet werden muss. Nach Art. 12 DSGVO bestimmen sich die Modalitäten für die Ausübung der Betroffenenrechte. **Art. 12 Abs. 3 S. 1 DSGVO definiert die Frist** und setzt die unverzügliche Zurverfügungstellung von Informationen über die Befriedigung der Rechte voraus. Die Mitteilung muss nach Antragseingang also unverzüglich, d.h. ohne schuldhaftes Zögern, erfolgen. Spätestens sollen die Informationen jedoch **innerhalb eines Monats nach Eingang des Antrags** mitgeteilt werden.

Im Unternehmensalltag besteht ein immer größeres Bewusstsein für Datenschutz und somit auch das Interesse an der Einhaltung datenschutzrechtlicher Fristen, um Bußgelder zu vermeiden. Betroffene wenden sich meist mit einer E-Mail-Anfrage an das Unternehmen, das ihre Daten verarbeitet. Die zentrale Frage lautet mithin: Wann ist der Antrag eingegangen?

Antragseingang nach Art. 12 Abs. 3 S. 1 DSGVO

Art. 12 Abs. 3 S. 1 DSGVO setzt den Eingang des Antrags voraus, während § 130 BGB von dem Zugang einer Willenserklärung spricht. Die angeführten Urteile gehen allerdings nur auf den Zugang von elektronischen Willenserklärungen unter der Heranziehung der allgemeinen Zugangsdefinition ein.

Sie helfen nur bedingt weiter, zumal sie sich gerade nicht mit dem fristauslösenden Ereignis bei Betroffenenrechten befassen. Ausgehend von dem Wortlaut könnte der Unterschied darin liegen, dass ein Antragseingang nur das Gelangen in den Machtbereich voraussetzt, wohingegen ein Zugang zusätzlich die Möglichkeit der Kenntnisnahme unter gewöhnlichen Umständen erfordert. Daraus folgt, dass die Begriffe entweder unterschiedlich auszulegen sind oder der Eingang mangels anderweitiger Definition wie der Zugang nach deutschem Recht zu bewerten ist.

Für ein Gleichsetzen der Begriffe spricht, dass die DSGVO keine speziellen Zugangsvoraussetzungen geregelt hat. Möglicherweise hat der europäische Gesetzgeber die Problematik des Zugangs nicht erkannt und den Wortlaut rein zufällig gewählt. Diese Annahme wird dadurch gestützt, dass die Erwägungsgründe keine Hinweise zur Norminterpretation geben. In der DSGVO lässt sich zudem keine weitere Norm finden, die sich mit dem Eingang beschäftigt.

Für eine Eigenständigkeit des Begriffs „Antragseingang" können die Ausführungen des Europäischen Datenschutzausschusses[9] herangezogen werden. Zwar wird die Problematik hier nicht näher vertieft, und das Papier enthält die klare Aussage, dass alleine der Eingang des Antrags entscheidend ist, ohne dass der Verantwortliche vom Inhalt Kenntnis nehmen muss. Auch könnte die Intention des Europäischen Gesetzgebers nicht unbedingt in der Heranziehung der deutschen Zugangsdefinition liegen. Der Art. 12 Abs. 3 DSGVO spricht eindeutig von Antragseingang. Ein weiterer Aspekt ist die Tatsache, dass ein Eingang geringere Voraussetzungen als ein Zugang hat. Dies könnte hinsichtlich des Schutzzwecks von Belang sein, da die Norm dem Verantwortlichen Pflichten auferlegt, welcher im Vergleich zum Betroffenen eine Art Machtposition innehat. Der Betroffene erlangt nur Informationen, wenn der Verantwortliche aktiv wird.

[8] Die Landesbeauftragte für den Datenschutz Niedersachsen, 25. Tätigkeitsbericht 2019, S. 88.

[9] Leitlinie zu Betroffenenrechte – Auskunftsrecht 01/2022, Rdnr. 157.

Andererseits könnte der Normtelos darin bestehen, den Verantwortlichen vor einer unzureichenden Antwortfrist zu schützen. Unsachgemäß wäre es danach, lediglich das Gelangen in den Machtbereich genügen zu lassen, mit der Folge, dass die Frist ohne Kenntnisnahme des Verantwortlichen zu laufen beginnen würde. Im Ergebnis soll durch die Norm aber ein gerechter Interessenausgleich vorgenommen werden.

Schließlich spielt auch die Beweislast eine große Rolle für den Betroffenen, der den Zugang der E-Mail im Zweifel beweisen muss. Nimmt man die etablierte Zugangsdefinition als unverzichtbar an, muss der Betroffene auch die Möglichkeit der Kenntnisnahme beweisen. Der BGH urteilte jedoch, dass jedenfalls im Geschäftsverkehr der Zugang einer E-Mail bereits erfolgt, wenn die E-Mail innerhalb der üblichen Geschäftszeiten im Postfach abrufbereit zur Verfügung gestellt wird. Ein Unterschied zu einem einfachen Eingang ergibt sich in diesem Fall damit gerade nicht.

Die hier thematisierte Frage, wann eine E-Mail bei der Geltendmachung von Betroffenenrechten zugeht, hat zumindest nach deutschem Recht kaum Auswirkungen. Stellt man auf den Eingang nach der DSGVO ab, erfolgt dieser bereits mit Abrufbereitschaft im E-Mail-Postfach. Zieht man die deutsche Zugangsregelung heran, geht die E-Mail, die innerhalb gewöhnlicher Geschäftszeiten gesendet wird, sogar gleichzeitig zu. Ein Absenden außerhalb der Geschäftszeiten führt dann zu dem Unterschied, dass die E-Mail erst am nächsten Geschäftstag zugeht. Dennoch erscheint es naheliegend, die DSGVO-Norm, unter Zuhilfenahme der zuvor dargestellten deutschen Zugangsformel, auszulegen. Es kann nicht gewollt sein, dass die Frist bereits ausgelöst wird, wenn eine Betroffenenanfrage per E-Mail an einem Freitagabend eingeht, während das Unternehmen regelmäßig erst montags davon Kenntnis erlangt. Zufällige Ergebnisse sollen gerade vermieden werden. In jedem Fall unbestritten ist, dass es auf eine tatsächliche Kenntnisnahme nicht ankommt. Eine Lesebestätigung ist damit gerade nicht erforderlich.

Die Fristenberechnung nach Unionsrecht

Nach Bestimmung des fristauslösenden Ereignisses sollte nicht unerwähnt bleiben, dass die Fristenberechnung unterschiedlich gehandhabt wird. Die DSGVO enthält dazu keine Regelungen. Vorzugswürdig erscheint aufgrund des Anwendungsvorrangs des Unionsrechts die **Heranziehung der einschlägigen Fristenverordnung vom 3. Juni 1971**[10] und nicht die Fristenbestimmung nach den §§ 186 ff. BGB. Die FristenVO ist gem. Art. 1 auf Rechtsakte der Europäischen Union anwendbar, worunter die DSGVO fällt. Das fristauslösende Ereignis i.S.d. Art. 3 Abs. 2 lit. c FristenVO bestimmt den Tag des Fristbeginns, die Frist beginnt dann nach Art. 3 Abs. 1 2. Unterabs. FristenVO am nächsten Tag zu laufen. Fristauslösendes Ereignis ist der Eingang des Antrags auf Auskunftserteilung.

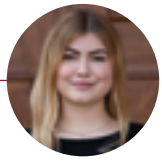
AUSBLICK

Festzuhalten bleibt, dass der E-Mail-Zugang gem. § 130 Abs. 1 BGB im Unternehmensbereich inzwischen fast allumfänglich höchstrichterlich geklärt ist. Unsicherheiten bleiben wiederum bezüglich der Auslegung des Antragseingangs nach der DSGVO. Um diese Frage eindeutig beantworten zu können, bleibt eine klärende Rechtsprechung abzuwarten. Relevant wird dies im Hinblick auf die Wahrung der einheitlichen Anwendung der Datenschutz-Grundverordnung sowie der Funktionsfähigkeit des Unionsrechts.

Über die Autorinnen

Nicole Schmidt, LL.M.
Rechtsanwältin, Geschäftsführerin SüdWest Datenschutz Rechtsanwaltsgesellschaft mbH

Lilly Steinbrecher, LL.B.
studierte Rechtswissenschaften mit dem Schwerpunkt Geistiges Eigentum an der Universität Mannheim und tritt als Nächstes den juristischen Vorbereitungsdienst an. Sie arbeitet als Werkstudentin bei der SüdWest Datenschutz Rechtsanwaltsgesellschaft mbH.



Laura Toska Genkinger
ist Studentin der Rechtswissenschaften an der Universität Mannheim mit dem Schwerpunkt Internationales Wirtschaftsrecht. Sie arbeitet als Werkstudentin bei der SüdWest Datenschutz Rechtsanwaltsgesellschaft mbH.

▶ https://www.suedwest-datenschutz.com

swds
DATENSCHUTZRECHT FÜR UNTERNEHMEN

[10] 1. Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine.

DAS NEUE FERNMELDE-GEHEIMNIS

Dürfen Arbeitgeber auf dienstliche E-Mail-Postfächer trotz erlaubter Privatnutzung zugreifen?

Ein Update zum neuen Recht

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

Im Beitrag wird die Zulässigkeit der Kenntnisnahme von Kommunikationsinhalten (E-Mails) durch Arbeitgeber untersucht. Dabei stellt sich heraus, dass das mit Wirkung zum 01.12.2021 neu geregelte Fernmeldegeheimnis durch den Gesetzgeber eine Ausgestaltung erfahren hat, welche mit höherrangigem Recht nicht vereinbar ist, so dass der Beitrag mit einem Lösungsvorschlag für die zukünftige Rechtsanwendung schließt.[*]

1. Sachverhalt

Ein Arbeitgeber entscheidet, zur Unterstützung der Arbeitsabläufe, eine Kommunikation via E-Mail einzusetzen. Er betreibt daraufhin mittels seiner eigenen IT einen E-Mail-Server oder lässt auf fremder IT für sich einen E-Mail-Server betreiben. Dort sind Postfächer eingerichtet, die den Arbeitnehmern einzeln zugeteilt und in der Regel auf diese personalisiert sind, so dass sich den Postfächern zugeordnete E-Mail-Adressen unter der auf den Arbeitgeber registrierten Domain gemäß folgendem Schema ergeben:

Vorname.Nachname@Name-der-Organisation.de.

Der E-Mail-Server hat als Betriebsmittel den Zweck, von den Arbeitnehmern im Rahmen ihrer Tätigkeit eingesetzt zu werden und damit der Verwirklichung der unternehmerisch verfolgten Ziele zu dienen. Neben der vom Arbeitgeber im Wesentlichen intendierten Nutzung der Postfächer zu „dienstlichen" Zwecken und damit abweichend von der gesetzlichen Ausgangslage für die Nutzung von Betriebsmitteln kommt jedoch auch eine Nutzung derselben zu „privaten" Zwecken durch die Arbeitnehmer im Alltag vor. Diese vollzieht sich entweder aufgrund ausdrücklicher Erlaubnis des Arbeitgebers oder zumindest mit Kenntnis des Arbeitgebers und seiner Duldung.

Fällt ein Arbeitnehmer beispielsweise wegen Krankheit unvorhergesehen aus, besteht ein Interesse des Arbeitsgebers daran, auf jenes individuell zugeordnete Postfach zuzugreifen und dessen Inhalte zur Kenntnis zu nehmen, um die weitere Bearbeitung der dort gespeicherten und weite eingehenden E-Mails zu ermöglichen. Im Falle von Stetigkeiten mit einem Arbeitnehmer sowie im Falle vorgelagerter, interner Ermittlungen besteht ebenfalls ein Interesse des Arbeitsgebers daran, auf jenes individuell zugeordnete Postfach zuzugreifen und dessen Inhalte zur Kenntnis zu nehmen, insbesondere um Beweismittel zu erlangen.

2. Rechtliche Würdigung

2.1 Personenbezogene Daten und betroffene Person(en)

Im Hinblick auf die Person des Arbeitnehmers sind als personenbezogene Daten i. S. v. Art. 4 Nr. 1 DS-GVO „alle" Informationen zu werten, welche sich dieser Person zuordnen lassen, so dass ausnahmslos der gesamte Inhalt des ausweislich des Sachverhalts „personalisierten" Postfachs von dieser Bewertung erfasst ist. Der Personenbezug ergibt sich bereits aus der Information, dass das personalisierte Postfach und damit der Arbeitnehmer als Sender oder Empfänger an dem einzelnen Nachrich-

[*] Der Beitrag ist eine gekürzte Fassung des Vortrags des Verfassers bei der DSRI-Herbstakademie 2022, welcher im Tagungsband von Heinze „Daten, Plattformen und KI als Dreiklang unserer Zeit", DSRI Herbstakademie, 2022, S. 277 ff. veröffentlicht wurde.

[1] BGH, Urt. v. 15.06.2021 – VI ZR 576/19, Rn. 28 ff. (33).

tenaustausch beteiligt war.[1]

Eine Kenntnisnahme von den Inhalten eines dem einzelnen Arbeitnehmer zugeordneten E-Mail-Postfachs durch den Arbeitgeber geht zwingend mit einer Verarbeitung i. S. v. Art. 4 Nr. 2 DS-GVO bezüglich der im Postfach gespeicherten personenbezogenen Daten einher. Ob es sich insoweit um ein „Auslesen", „Erfassen" oder „Verwenden" handelt, bedarf keiner Entscheidung, weil alle solche Verarbeitungen vorliegend denselben Regelungen unterliegen. Dass diese Vorgänge im Zusammenhang mit personenbezogenen Daten in den sachlichen Anwendungsbereich des Datenschutzrechts gem. Art. 2 Abs. 1 DS-GVO fallen, ist offenkundig.

Mit Blick auf den Umstand, dass es in Bezug auf eine jede E-Mail (abgesehen von etwaig zwischengespeicherten Entwürfen zukünftiger E-Mails) einen Sender und mindestens einen Empfänger gibt, weisen die in Rede stehenden personenbezogenen Daten häufig einen mehrfachen Personenbezug auf, das heißt, die Informationen beziehen sich häufig zeitgleich auf mehr als eine betroffene Person.[2] Aufgrund der Zuordnung des „personalisierten" Postfachs ist davon auszugehen, dass jedenfalls der jeweilige Arbeitnehmer eine betroffene Person ist.

2.2 Verantwortlichkeit i. S. v. Art. 4 Nr. 7 DS-GVO

Der Arbeitgeber, welcher die im Sachverhalt angegebene Anwendungssoftware entweder selbst betreibt oder betreiben lässt, ist vorliegend derjenige Rechtsträger, welcher die Entscheidung über die Zwecke und Mittel der Verarbeitung personenbezogener Daten getroffen hat und damit als Verantwortlicher i. S. v. Art. 4 Nr. 7 DS-GVO anzusehen ist. Die anteilige Nutzung des Postfachs zur Abwicklung von Kommunikation mit privaten Inhalten gegenüber Sendern oder Empfängern dieser privaten Kommunikation ist keine eigene „Entscheidung" der Arbeitnehmer i. S. v. Art. 4 Nr. 7 DS-GVO, sondern findet aufgrund der ausdrücklich erteilten oder aus der in Kenntnis der Umstände erfolgten Duldung abgeleiteten Erlaubnis seitens des Arbeitgebers statt. Er hat damit diese Form der Nutzung in seine Entscheidung über Zwecke und Mittel der Verarbeitung personenbezogener Daten i. S. v. Art. 4 Nr. 7 DS-GVO aufgenommen. An dieser die Erlaubnis und ihre Folgen umfassenden Entscheidung waren die einzelnen Arbeitnehmer nicht beteiligt, so dass keine „gemeinsame", sondern eine „alleinige" Entscheidung i. S. v. Art. 4 Nr. 7 DS-GVO durch den Arbeitgeber vorliegt und damit allein dieser als Verantwortlicher anzusehen ist.[3]

2.3 Rechtsrahmen zur Prüfung der Zulässigkeit einer Kenntnisnahme

2.3.1 Telekommunikationsrecht und Datenschutz in der elektronischen Kommunikation

Den maßgeblichen Rechtsrahmen für die Bewertung der Zulässigkeit der mit der Kenntnisnahme einhergehenden Verarbeitungen bestimmt die DS-GVO nicht allein. Aufgrund von Art. 95 DS-GVO sind zusätzlich die Inhalte der Richtlinie 2002/58/EG („ePrivacy") beziehungsweise die Inhalte der Richtlinie umsetzenden, nationalen Vorschriften maßgeblich.

Ausweislich von ErwG 2 Richtlinie (EU) 2018/1972 („TK-Kodex") ist die Richtlinie 2002/58/EG Bestandteil des geltenden europäischen Rechtsrahmens für elektronische Kommunikationsnetze und -dienste und zugleich der einzige der dort genannten fünf Bestandteile, welcher durch Art. 125 Richtlinie (EU) 2018/1972 nicht aufgehoben wurde. In Übereinstimmung damit wurde auch hinsichtlich des Anwendungsbereichs des neuen Telekommunikationsrechts in Art. 1 Abs. 3 Richtlinie (EU) 2018/1972 festgelegt, dass das Datenschutzrecht unberührt bleibt. Folglich werden die Inhalte der DS-GVO sowie der Richtlinie 2002/58/EG durch die Richtlinie (EU) 2018/1972 weder verdrängt noch modifiziert.

Soweit jedoch andersherum aus dem Datenschutzrecht, insbesondere aus der Richtlinie 2002/58/EG beziehungsweise den diese Richtlinie umsetzenden nationalen Vorschriften heraus auf das Telekommunikationsrecht (also die Richtlinie EU 2018/1972 beziehungsweise die diese Richtlinie umsetzenden, nationalen Vorschriften) Bezug genommen wird, hat die Neufassung des Telekommunikationsrechts Auswirkungen auf die Anwendung des Datenschutzrechts. Dies gilt mit Blick auf den umfangreich veränderten § 3 TKG insbesondere für diejenigen datenschutzrechtlichen Regelungen, die an die im Telekommunikationsrecht definierten Begriffe anknüpfen.

Aufgrund der Richtlinie (EU) 2018/1972 wurde das deutsche Telekommunikationsrecht grundlegend überarbeitet und im Zuge dessen ein neues Telekommunikationsgesetz (TKG) mit Wirkung zum 01.12.2021 in Kraft gesetzt.

2.3.2 Folgen der möglichen Anwendbarkeit des Fernmeldegeheimnisses

Vor diesem Hintergrund ist auf eine i. S. v. Art. 95 DS-GVO vorrangige Sonderregelung hinzuweisen, die eine gegenüber Art. 6 Abs. 1 DS-GVO – dem allgemeinen Verbot mit Erlaubnisvorbehalt – strengere Regelung enthält:

Gestützt auf Art. 5 Richtlinie 2002/58/EG, welcher mit Vertraulichkeit der Kommunikation betitelt ist, ist in § 3 TTDSG der Schutz des Fernmeldegeheimnisses geregelt. Der Kern der Regelung findet sich in § 3 Abs. 3 S. 1, 2 TTDSG, wonach es den auf das Fernmeldegeheimnis Verpflichteten einerseits verboten ist, sich über das zur Erbringung der Telekommunikationsdienste […] [*einschließlich des Schutzes ihrer technischen Systeme*] erforderliche Maß hinaus Kenntnis vom Inhalt oder von den näheren

[2] Grundlegend zum mehrfachen Personenbezug: EuGH, Urt. v. 20.12.2017 - C-434/16 (Nowak).

[3] Der abweichende Sachverhalt, in dem sich die Erlaubnis zur Privatnutzung aus einer Kollektivvereinbarung ergibt, bedarf im Hinblick auf die Frage nach einer „gemeinsamen" Entscheidung i. S. v. Art. 4 Nr. 7 DS-GVO hier keiner Betrachtung.

Umständen der Telekommunikation zu verschaffen und es ihnen andererseits vorgegeben wird, dass sie die Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur zur Erbringung der Telekommunikationsdienste […] [*einschließlich des Schutzes ihrer technischen Systeme*] verwenden dürfen. Soweit das explizite Verbot der Kenntnisnahme nicht entgegensteht, das heißt wenn zulässigerweise Kenntnis genommen werden durfte, ist gem. § 3 Abs. 3 S. 3 TTDSG eine Verwendung dieser Kenntnisse für „andere Zwecke" [*als die Erbringung des Dienstes*], insbesondere die Weitergabe an andere, nur zulässig, soweit das TTDSG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.

Dem Verbot der Kenntnisnahme des § 3 Abs. 3 S. 1 TTDSG ist im Gesetz kein allgemeiner Erlaubnistatbestand gegenübergestellt, welcher – wie Art. 6 Abs. 1 S. 1 lit f) DS-GVO – auf der Grundlage von „berechtigten Interessen", die im Sachverhalt verschiedentlich erkennbar sind, derartige Kenntnisnahmen oder Weiterverwendungen der Kenntnisse erlauben würden.

Die Anwendbarkeit des Fernmeldegeheimnisses und damit des strengen Verbotes gem. Art. 5 Richtlinie 2002/58/EG i. V. m. § 3 Abs. 3 TTDSG setzt, wie nachfolgend dargestellt, die Eröffnung des sachlichen sowie des persönlichen Anwendungsbereiches voraus. Selbst wenn eine Kenntnis vorhanden wäre, dürften die dem Anwendungsbereich des Fernmeldegeheimnis unterliegenden personenbezogenen Daten nicht zu den im Sachverhalt erkennbaren, berechtigten Interessen aufgrund von Art. 6 Abs. 1 S. 1 lit f) DS-GVO weiterverarbeitet werden, weil diese Norm keine „andere gesetzliche Vorschrift, die sich ausdrücklich auf Telekommunikationsvorgänge bezieht" i. S. d. vorrangingen Regelung gem. Art. 5 Richtlinie 2002/58/EG i. V. m. § 3 Abs. 3 S. 3 TTDSG darstellt.

Daher ist es besonders bedeutsam, dass in tatsächlicher Hinsicht ein Mangel an Trennbarkeit vorliegt, so dass die Zulässigkeitsregeln sowohl die private als auch die dienstliche Kommunikation gleichermaßen erfassen könnten.[4]

2.3.3 Sachlicher Anwendungsbereich des Fernmeldegeheimnisses Der Begriff Telekommunikation - Änderung der Rechtslage

Gem. § 3 Abs. 1 TTDSG unterliegen dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Diese Regelung beruht dabei auf der – durch die Reform nicht veränderten – Begriffsdefinition der Telekommunikation (§ 3 Nr. 59 TKG). Bis zu diesem Punkt entspricht die Rechtslage, jedenfalls dem Wortlaut nach, der alten Rechtslage, d. h. jener, die vor dem 01.12.2021 galt. Vorgenannte Regelung des § 3 Abs. 1 TTDSG war zuvor in § 88 Abs. 1 TKG (a .F.) und die Begriffsbestimmung zu „Telekommunikation" in § 3 Nr. 22 TKG (a. F.) enthalten.

Anzumerken ist insoweit, dass es durch zwei streitige Verfahren zu Entscheidungen des EuGH im Jahr 2019 kam, die sich mit der Abgrenzung des Begriffs der Telekommunikation befassten: E-Mail-Dienste wurden damals mit der Begründung nicht als Telekommunikationsdienste eingestuft, dass diese durch Software realisierten Funktionen zwar „Telekommunikation" voraussetzten, ihre Implementierung jedoch über die technischen Vorgänge des Sendens und Empfangens von Signalen abstrahiert.[5] E-Mail-Dienste würden vielmehr auf einer höheren Abstraktionsschicht über die von anderen erbrachten Telekommunikationsdienste hinweg („over the top", OTT) arbeiten und von den technischen Vorgängen des Sendens und Empfangens von Signalen losgelöst sein. Im Gegensatz dazu befand der EuGH in der zweiten Entscheidung für VoIP-Diente, also für durch Software realisierte Funktionen, welche eine Sprachübertragung unmittelbar ins oder vom klassischen Telefonnetz (PSTN) ermöglichten, dass diese bei wertender Betrachtung der „Telekommunikation",

[4] Voigt, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 668.

[5] EuGH, Urt. v. 13.06.2019 – C-193/18 (Gmail).

[6] EuGH, Urt. v. 05.06.2019 – C-142/18 (SkypeOut).

also den technischen Vorgängen des Sendens und Empfangens von Signalen, zugerechnet werden müssten.[6]

Der europäische Gesetzgeber hat jedoch mit der Richtlinie (EU) 2018/1972 die Rechtslage grundlegend verändert und diese Rechtsprechung des EuGH damit überholt. Ganz bewusst ist der Gesetzgeber von der stark technikbezogenen Betrachtungsweise abgerückt und hat nunmehr eine funktionsbezogene Betrachtung in den Mittelpunkt gestellt.[7] Ganz bewusst wollte er, wie nachfolgend anhand der Erwägungsgründe aufgezeigt werden wird, OTT-Dienste von der Regelung erfasst sehen. Der deutsche Gesetzgeber hat diese Änderung in Umsetzung der Richtlinie in der Neufassung des TKG mit Wirkung zum 01.12.2021 dahingehend berücksichtigt, dass sich die Änderungen in den sich an die Begriffsdefinition der Telekommunikation anschließenden Begriffsdefinitionen wiederfinden (siehe dazu § 3 Nr. 60, 61 und Nr. 24 TKG).

Die Begriffsdefinition des § 3 Nr. 24 TKG („Interpersonelle Telekommunikationsdienste") ist inhaltlich deckungsgleich mit der Begriffsbestimmung in Art. 2 Nr. 5 Richtlinie (EU) 2018/1972. Der europäische Gesetzgeber hat indes sein Regelungsziel weiter konkretisiert, mit dem auf diese Begriffsbestimmung bezogenen ErwG 17 Richtlinie (EU) 2018/1972 und dem dortigen Regelbeispiel „E-Mails". Dieses Begriffsverständnis, wonach ausdrücklich OTT-Dienste in den Anwendungsbereich der Regelungen zu Telekommunikationsdiensten einzubeziehen sind, ist für die deutsche Rechtslage zwingend zu übernehmen, jedenfalls aufgrund der gebotenen richtlinienkonformen Auslegung des deutschen Rechts.

Zwischenergebnis

Als Zwischenergebnis ist festzuhalten, dass jedenfalls der Betrieb der Anwendungssoftware, welche die Funktionen des E-Mail-Servers realisiert, als Betrieb eines interpersonellen Kommunikationsdienstes und damit eines Telekommunikationsdienstes zu werten ist. Die Kenntnisnahme vom Inhalt eines E-Mail-Postfachs stellt mithin, vom sachlichen Anwendungsbereich her beurteilt, einen Eingriff in einen Telekommunikationsdienst und damit den Schutzbereich des Fernmeldegeheimnisses dar.

2.3.4 Persönlicher Anwendungsbereich des Fernmeldegeheimnisses. Der Begriff Diensteanbieter - Änderung der Rechtslage

Nach der Vorgängerregelung des § 3 TTDSG, dem § 88 TKG (a. F.), war zur Wahrung des Fernmeldegeheimnisses jeder „Diensteanbieter" verpflichtet. Früher war gem. § 3 Nr. 6 TKG (a. F.) jeder ein „Diensteanbieter", der ganz oder teilweise geschäftsmäßig (a) Telekommunikationsdienste erbringt oder (b) an der Erbringung solcher Dienste mitwirkt. Diese Regelung wurde aufgehoben und der Begriff „Diensteanbieter" entfiel ersatzlos. Heute ist gem. § 3 Nr. 1 TKG nur noch derjenige „Anbieter von Telekommunikationsdiensten", der Telekommunikationsdienste erbringt. Soweit der Gesetzgeber auch einer mitwirkenden Person Pflichten auferlegen wollte, erfolgt dies nicht mehr über den Weg, den Mitwirkenden zum „(Dienste-)Anbieter" zu erklären, sondern indem in der jeweiligen Norm explizit festgeschrieben ist, dass die Pflichten für den Anbieter von Telekommunikationsdiensten sowie für jede Person gelten, die an der Erbringung des Dienstes mitwirkt. Ob der Arbeitgeber in Bezug darauf, dass er mittels seiner eigenen IT einen E-Mail-Server betreibt bzw. auf fremder IT für sich einen E-Mail-Server betreiben lässt, selber ein „Anbieter von Telekommunikationsdiensten" ist oder ob er nur an der Erbringung eines Dienstes mitwirkt, ist eine neue Rechtsfrage, die sich in der Vergangenheit aus vorgenanntem Grund (siehe § 3 Nr. 6 TKG (a. F.)) nie stellte. Inwieweit sie relevant ist, zeigt der Blick auf den Kreis der auf das Fernmeldegeheimnis Verpflichteten nach § 3 Abs. 2 S. 1 Nr. 1 bis Nr. 4 TTDSG.

Die Regelungen der Nr. 1 und Nr. 3 adressieren öffentlich zugängliche Dienste bzw. Infrastruktur, so dass diese Regelungen für vorliegenden Sachzusammenhang nicht relevant sind.

Bislang wurde der Arbeitgeber von der Rechtsprechung nicht als zur Wahrung des Fernmeldegeheimnisses verpflichtet angesehen. Dabei ist die Rechtsprechungshistorie wechselvoll. Vor 17 Jahren wurde unter den Umständen eines Einzelfalls – einer gestatteten Privatnutzung des E-Mail-Postfachs – das Vorliegen eines gem. § 206 StGB strafbaren Eingriffs in das Fernmeldegeheimnis aufgrund des Herausfilterns bestimmter E-Mails erblickt.[8] Demgegenüber wurde der Arbeitgeber später regelmäßig, sogar dann, wenn er gegenüber seinen Arbeitnehmern die Privatnutzung der E-Mail-Postfächer ausdrücklich zugelassen hatte, nicht als Diensteanbieter qualifiziert.[9] Zur Begründung führten die Gerichte aus, dass die Qualifizierung als „Diensteanbieter" davon abhänge, ob ein Erbringen von Telekommunikationsdiensten in Rede stünde, woran es in den damaligen Fällen fehlte. Denn die alte Rechtslage enthielt in § 3 Nr. 10 TKG (a. F.) die Begriffsbestimmung für das „geschäftsmäßige Erbringen von Telekommunikationsdiensten", welches das nachhaltige Angebot von Telekommunikation *für Dritte* mit oder ohne Gewinnerzielungsabsicht war. Das Vorliegen dieses Tatbestands wurde von der Rechtsprechung abgelehnt.Besondere Beachtung verdient insoweit, dass diese Regelung aufgehoben wurde und die Begriffsbestimmung für das „Erbringen von Telekommunikationsdiensten" ersatzlos entfiel, wenngleich das Gesetz nach wie vor an diesen Wortlaut anknüpft

[7] Tinnefeld/Buchner in: BeckOK Datenschutzrecht, Wolff/Brink, Grundlagen, Syst. I. Datenschutz in Medien und Telekommunikation, D. II. Rn. 109.

[8] OLG Karlsruhe, Beschl. v. 10.01.2005 – 1 Ws 152/04.

[9] LG Erfurt, Urt. v. 28.04.2021 – 1 HK O 43/20; VG Karlsruhe, Urt. v. 27.05.2013 – 2 K 3249/12, Rn. 59; LAG Hamm Urt. v. 10.07.2012 – 14 Sa 1711/10, Rn. 175; LAG Berlin-Brandenburg, Urt. v. 16.02.2011 – 4 Sa 2132/10, Rn. 38 ff; LAG Niedersachsen, Urt. v. 31.5.2010 – 12 Sa 875/09, Rn. 45; VGH Kassel, Beschl. v. 19.5.2009 - 6 A 2672/08.Z, Rn.11 ff..

(§ 3 Nr. 1 TKG (Definition des Anbieters) und § 3 Abs. 2 S. 1 TTDSG (Kreis der Verpflichteten)).

Telekommunikationsdienste, Drittbezogenheit (§ 3 Abs. 2 S. 1 Nr. 2 TTDSG)

Diese gesetzliche Begriffsbestimmung entfiel nicht nur innerhalb des TKG, sondern erfuhr auch keine Fortsetzung im TTDSG. Dieser Umstand ist deshalb von herausgehobener Bedeutung, weil die Rechtsprechung früher maßgeblich damit argumentierte, dass sich aus der Begriffsbestimmung für das Erbringen von Telekommunikationsdiensten in § 3 Nr. 10 TKG (a. F.) die sogenannte Drittbezogenheit dieser Tätigkeit als Merkmal ergab („für Dritte"). Es lässt sich also argumentieren, dass der Gesetzgeber das Merkmal der Drittbezogenheit bewusst zum 01.12.2021 aufgegeben hat.

Während die zitierte Rechtsprechung dieses Merkmal „für Dritte" stets verneinte, wenn der Arbeitgeber seinen Arbeitnehmern – wie in vorliegendem Sachverhalt dargestellt – die Nutzung des Betriebsmittels „E-Mail-Server" überließ, differenzierte die rechtswissenschaftliche Literatur danach, ob die Nutzung zu dienstlichen oder privaten Zwecken erfolgte, insbesondere sofern letztgenannte eine erlaubte Nutzung war. Für die Fälle der erlaubten Privatnutzung wurde die Drittbezogenheit bejaht, weil der Arbeitnehmer insoweit dem Arbeitgeber als „Dritter" i. S. v. § 3 Nr. 10 TKG (a. F.) gegenüberstehe. Auch nach bisheriger Auffassung der Aufsichtsbehörden wurde die private Kommunikationsdienstleistung im Betrieb miterfasst und damit der Arbeitgeber als ein auf das Fernmeldegeheimnis Verpflichteter angesehen.[10]

Selbst wenn demnach die zukünftige Rechtsprechung im Wege der Auslegung von § 3 Abs. 2 S. 1 TTDSG weiterhin eine Drittbezogenheit als Voraussetzung für die Verpflichtung auf das Fernmeldegeheimnis annehmen wollen würde, ist Folgendes zu prognostizieren: Jedenfalls diejenigen Arbeitgeber, die nach dem 01.12.2021 immer noch eine Privatnutzung des – wie oben im sachlichen Anwendungsbereich dargestellt, im Unterschied zu früher nunmehr der Sache nach gegebenen – Telekommunikationsdienstes gem. § 3 Nr. 61 TKG erlauben, laufen Gefahr, ein Erbringen des bzw. Mitwirken am Dienst mit Drittbezogenheit attestiert zu bekommen und damit zum Kreise der Verpflichteten gem. § 3 Abs. 2 S. 1 Nr. 2 TTDSG zu zählen.

Falls die Rechtsprechung einen Drittbezug voraussetzen wollen würde, könnte eine solche Voraussetzung im Wort „angebotene" i. S. v. § 3 Abs. 2 S. 1 Nr. 2 TTDSG gesehen werden. Das notwendige „Anbieten" des Telekommunikationsdienstes könnte ein Auseinanderfallen von Anbieter und Nutzer erfordern, worin sich wiederum die Voraussetzungen der Drittbezogenheit ausdrücken könnte. Ob ein solches Auseinanderfallen erforderlich ist, könnte jedoch abzulehnen sein, weil das Gesetz auch die „Eigenerbringung" kennt (z. B. in § 3 Nr. 77 TKG).

In aktueller Literatur wird in Bezug auf die Definition des Telekommunikationsdienstes gem. § 3 Nr. 61 TKG das Merkmal „in der Regel gegen Entgelt" hervorgehoben, verbunden mit dem Hinweis darauf, dass eine Entgeltlichkeit in Bezug auf die private Nutzung des dienstlichen E-Mail-Postfachs im Verhältnis von Arbeitgeber zum Arbeitnehmer nicht vorliegt und deshalb eine Verpflichtung auf § 3 TTDSG nicht in Betracht käme.[11] Dies vermag nicht zu überzeugen. Das Tatbestandsmerkmal „in der Regel gegen Entgelt" ist entweder dahingehend zu verstehen, dass es belanglos ist – weil es eben nur in der Regel und nicht immer vorliegt. Oder diese Formulierung des Gesetzgebers ist dahingehend zu verstehen, was vorzugswürdiger erscheint, dass der Dienst typisierend zu betrachten ist. Insoweit ist jedoch zu konstatieren, dass die Nutzungsmöglichkeit „eines" E-Mail-Postfachs zu privaten Zwecken gerade etwas ist, was einen Marktwert hat, eben weil es „in der Regel" gegen Entgelt angeboten wird. Die sog. „Freemail"-Angebote, wie sie z. B. Gegenstand der „Inbox-Advertising" Rechtsprechung sind[12], sind auch nicht unentgeltlich – dort ist das Entgelt lediglich nicht in Geld bemessen (vgl. dazu auch § 327 Abs. 3 BGB).

Betreiben einer Telekommunikationsanlage (§ 3 Abs. 2 S. 1 Nr. 4 TTDSG)

Zu prognostizieren ist, dass es zur Beurteilung der vorliegend betrachteten Rechtsfrage möglicherweise auf die Auslegung des Wortes „angebotene" i. S. v. § 3 Abs. 2 S. 1 Nr. 2 TTDSG und damit eine etwaig immer noch zu fordernde Drittbezogenheit gar nicht ankommen wird. Denn der Arbeitgeber kann jedenfalls unter § 3 Abs. 2 S. 1 Nr. 4 TTDSG fallen, weil der von ihm oder für ihn betriebene E-Mail-Server eine Telekommunikationsanlage i. S. d. oben wörtlich zitierten Begriffsbestimmung des § 3 Nr. 60 TKG ist. Für den Arbeitgeber wäre es günstig, wenn es hier auf die sich erstmals stellende Rechtsfrage – nach Fortfall der alten Begriffsbestimmung des „Diensteanbieters" i. S. v. § 3 Nr. 6 TKG (a. F.), welche die Person des Mitwirkenden mit einbezog – ankommen würde, wie die Erbringung des Telekommunikationsdienstes von der der Mitwirkung an der Erbringung abzugrenzen ist (und er lediglich als Mitwirkender eingestuft würde, was auch schon an sich unwahrscheinlich erscheint).

Denn § 3 Abs. 2 S. 1 Nr. 4 TTDSG verpflichtet – anders als § 3 Abs. 2 S. 1 Nr. 2 TTDSG – die bloß mitwirkende Person gerade nicht.

In der Literatur wurde bislang vorgeschlagen, dass durch den Tatbestand des Mitwirkens sämtliche an der Diensteerbringung tatsächlich beteiligten Personen in den Kreis der nach dem TTDSG

[10] „Die meisten Datenschutzbehörden scheinen dem zu folgen", so Thüsing, Beschäftigtendatenschutz, § 3 Rn. 74 unter Verweis auf die Auffassung des LfDI BW, Brink/Schwab ArbRAktuell 2018, 111 (112).

[11] Rossow, DuD 2022, 93 (95)

[12] EuGH, Urt. v. 25.11.2021 - C-102/20; BGH, Urt. v. 13.01.2022 – I ZR 25/19.

Verpflichteten einbezogen werden sollen. Dazu gehören nicht nur die Mitarbeiter des diensteerbringenden Unternehmens, sondern auch alle sonstigen „Erfüllungsgehilfen", derer sich der Anbieter zur Erbringung des Dienstes bedient. Mitwirkende sind so insbesondere die „Betreiber" eines Telekommunikationsnetzes, etwa im Rahmen eines Outsourcings von Telekommunikationsdiensten, soweit sie nicht ohnehin den Dienst selbst erbringen. In den Kreis der Verpflichteten sind allerdings nur solche Mitarbeiter einzubeziehen, die tatsächlich mit dem Betrieb des Telekommunikationsnetzes betraut sind, also z. B. das technische Personal.[13]

Mutmaßlich wird es jedoch nicht darauf ankommen, weil § 3 Abs. 2 S. 1 Nr. 4 TTDSG nur indirekt an die Erbringung eines Telekommunikationsdienstes, nämlich über die Begriffsbestimmung in § 3 Nr. 60 TKG, dem Wortlaut nach jedoch an das „Betreiben" der Telekommunikationsanlage anknüpft. Was darunter zu verstehen ist, ist zwar im Detail offen, jedoch dürfte im vorliegenden Sachverhalt, in dem der Arbeitgeber mittels seiner eigenen IT einen E-Mail-Server betriebt bzw. auf fremder IT für sich einen E-Mail-Server betreiben lässt, das Vorliegen des Tatbestands „Betreiber einer Telekommunikationsanlage" i. S. v. § 3 Abs. 2 S. 1 Nr. 4 TTDSG schlechterdings nicht zu verneinen sein.

Bewusste Regelung für nicht öffentlich Zugängliches (§ 3 Abs. 2 S. 1 Nr. 2 und Nr. 4 TTDSG)

Dass der Arbeitgeber – im Ergebnis – zum Kreise der Verpflichteten gem. § 3 Abs. 2 S. 1 TTDSG zu zählen sein wird, wird ferner durch einen weiteren Umstand verstärkt: Im ursprünglichen Referentenentwurf des Bundesministeriums für Wirtschaft und Energie vom 12.01.2021 für das neue TTDSG, mit dem das Gesetzgebungsverfahren begonnen wurde, hatte § 3 Abs. 2 S. 1 TTDSG einen ganz anderen Wortlaut und umfasste insbesondere nicht die Aufzählung in Nr. 1 bis Nr. 4. Dieser § 3 Abs. 2 S. 1 TTDSG-RefE lautete: „Anbieter öffentlicher Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze sind zur Wahrung des Fernmeldegeheimnisses verpflichtet."

Hiernach wäre der Kreis der Verpflichteten erheblich kleiner gewesen. Wie es sich aus dem Vergleich mit dem oben zitierten Wortlaut der in Kraft getretenen Regelung des § 3 Abs. 2 S. 1 TTDSG ergibt, wurden im Gesetzgebungsverfahren bewusst die Anbieter von Telekommunikationsdiensten und Betreiber von Telekommunikationsanlagen, die gerade nicht öffentlich zugänglich sind, in den Kreis der Verpflichteten gem. § 3 Abs. 2 S. 1 TTDSG aufgenommen. Der Gesetzgeber war der Auffassung, dass der Kreis der Verpflichteten gegenüber dem RefE erweitert werden müsse, damit sich der Anwendungsbereich des Fernmeldegeheimnis „weiterhin" auf Betreiber nicht-öffentlicher TK-Netze und Erbringer nicht-öffentlich zugänglicher TK-Dienste erstrecke.[14] Hierdurch soll gewährleistet werden, dass „*wie bisher schon*" Anbieter geschlossener Benutzergruppen und Hotel- und Cafébetriebe und Arbeitgeber, die Arbeitnehmer die private Nutzung der betrieblichen TK-Mittel gestatten, unter das Fernmeldegeheimnis fallen.[15]

Zusätzlich zu diesem „historischen" Argument zur Auslegung von § 3 Abs. 2 S. 1 TTDSG spricht auch die Norm aus sich heraus dafür, dass es – jedenfalls für die Auslegung von § 3 Abs. 2 S. 1 Nr. 4 TTDSG – nicht darauf ankommt, ob die Telekommunikationsanlage, mit einen öffentlich zugänglichen oder einem bloß nicht öffentlich zugänglichen Telekommunikationsdienst in Zusammenhang steht. Denn in § 3 Abs. 2 S. 1 Nr. 3 TTDSG, der ebenfalls „Betreiber" adressiert, ist ausdrücklich das Wort „öffentlicher" hinzugefügt worden, worauf im Kontext des Betriebs der Telekommunikationsanlagen in § 3 Abs. 2 S. 1 Nr. 4 TTDSG verzichtet wurde. Weil das Wort „Betreiber" in den Regelungen des § 3 Abs. 2 S. 1 Nr. 3 und Nr. 4 TTDSG in unterschiedlichen Kontexten steht, wird zugunsten der Arbeitgeber auch nichts aus der Begriffsbestimmung des „Betreibers" in § 3 Nr. 7 TKG abzuleiten sein, welche zwar für sich genommen ein „öffentliches" Telekommunikationsnetz oder eine zugehörige Einrichtung voraussetzt, jedoch diese Voraussetzung der Öffentlichkeit in den Nr. 3 und Nr. 4 von § 3 Abs. 2 S. 1 TTDSG gerade unterschiedlich geregelt ist (und dies die vorrangige Sonderregelung sein dürfte, falls überhaupt ein Rückgriff auf § 3 Nr. 7 TKG möglich wäre).

Abschließend ist darauf hinzuweisen, dass der Gesetzgeber bei Erschaffung des TTDSG, in welches auch die Regelungen zum telemedienrechtlichen Datenschutz der früheren §§ 11 bis 15a TMG (a. F.) aufgenommen wurde, keine dem Gedanken des § 11 Abs. 1 TMG (a. F.) entsprechende Regelung ins TTDSG aufgenommen hat. Dort war damals unter der Überschrift „Anbieter-Nutzer-Verhältnis" unter anderem geregelt, dass die Vorschriften keine Anwendung finden, soweit die Bereitstellung der Dienste im Arbeitsverhältnis zu ausschließlich beruflichen Zwecken erfolgte. Es lässt sich also argumentieren, dass der Gesetzgeber die Differenzierung nach der Privatnutzung oder der ausschließlich dienstlichen Nutzung bewusst zum 01.12.2021 aufgegeben hat.

2.4 Zulässigkeit einer Kenntnisnahme von den Inhalten des Postfachs

2.4.1 Besondere TK-rechtliche Erlaubnisse nicht gegeben

Für die Bewertung der Zulässigkeit der mit der Kenntnisnahme einhergehenden Verarbeitung personenbezogener Daten i. S. v. Art. 4 Nr. 2 DS-GVO kann dann nicht auf Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO zugegriffen werden, wenn das vorrangige Verbot gem. § 3 Abs. 3 TTDSG in sachlicher und zeitlicher

[13] Munz in: Taeger/Gabel, DSGVO - BDSG – TTDSG, TTDSG § 3 Rn. 14.

[14] Kiparski, CR 2021, 482 (485).

[15] Munz in: Taeger/Gabel, DSGVO - BDSG – TTDSG, TTDSG § 3 Rn. 17.

Hinsicht eingreift und nicht durch telekommunikationsrechtliche Erlaubnisse überwunden wird. Ausgehend von dem Befund, dass ein Telekommunikationsdienst in Rede steht, ergibt sich die Schlussfolgerung, dass Daten einer spezifischen Art Bestandteil des Sachverhalts sind, deren zulässige Verarbeitung in den §§ 9 ff. TTDSG gesondert geregelt ist.

„Verkehrsdaten" i. S. v. § 3 Nr. 70 TKG sind Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Die Inhalte der Telekommunikation fallen nicht in die Menge der Verkehrsdaten, so dass sich zur Abgrenzung der früher wie heute nicht gesetzlich definierte Begriff der „Inhaltsdaten" in der Praxis etabliert hat. Dass es an einer gesetzlichen Definition insoweit fehlt, ist ungeachtet des Umstands festzustellen, dass die Begriffsdefinitionen des § 3 TKG, insbesondere die des „Telekommunikationsdienstes" in § 3 Nr. 61 TKG, an verschiedenen Stellen sehr wohl an die „Inhalte" anknüpfen. Besonders darauf hingewiesen sei, dass die Menge der Verkehrsdaten sowohl personenbezogene Daten i. S. v. Art. 4 Nr. 1 DS-GVO als auch darüber hinaus weitere Daten umfasst, die mangels einer „betroffenen Person" (welche qua Definition nur eine natürliche Person sein kann) keine personenbezogenen Daten darstellen. Diese Ausgestaltung des deutschen Gesetzgebers entspricht den Grundgedanken des europäischen Rechts, weil die Richtlinie 2002/58/EG nicht Datenschutzrecht enthält, sondern mit dem „Schutz der Privatsphäre" in der elektronischen Kommunikation auch über dessen sachlichen Anwendungsbereich hinausgehende Regeln.

„Bestandsdaten" i. S. v. § 3 Nr. 6 TKG setzen ein gesondertes Vertragsverhältnis über einen Telekommunikationsdienst voraus und sind daher nicht Bestandteil des Sachverhalts, weil die in Rede stehende Nutzung der E-Mail-Postfächer nur gelegentlich der Überlassung der Nutzungsmöglichkeit des Betriebsmittels im Rahmen des Arbeitsverhältnisses erfolgt. Es sind keine Anhaltspunkte dafür ersichtlich, dass auch die ausdrückliche Erlaubnis zur Privatnutzung mehr als eine schlichte Zustimmung war.

Ebenso enthält der Sachverhalt keine „Standortdaten" i. S. v. § 3 Nr. 56 TKG.

Da eine unmittelbare Kenntnisnahme der Inhalte der Kommunikation ausweislich des Sachverhalts in keinem denkbaren Fall ohne eine Kenntnisnahme der Umstände der Kommunikation auskommt, sind zwingend die Regeln über die Zulässigkeit der Verarbeitung von Verkehrsdaten zu beachten.

Die im Sachverhalt erkennbaren berechtigten Interessen des Arbeitgebers lassen sich jedoch mit den für die Verarbeitung von Verkehrsdaten geltenden Vorschriften der §§ 9, 10, 11 und 12 TTDSG – sowie der Vorschriften für damit zusammenhängende Dienste mit Zusatznutzen der §§ 2 Abs. 2 Nr. 5, 13 Abs. 1, Abs. 4 TTDSG – nicht in Einklang bringen.

2.4.2 Allgemeine TK-rechtliche Erlaubnisse nicht gegeben

Das Verbot der Kenntnisnahme in § 3 Abs. 3 S. 1 TTDSG erstreckt sich über die Verkehrsdaten hinaus auch auf die sogenannten Inhaltsdaten, also auf Inhalte der Kommunikation. Die in § 3 Abs. 3 TTTDSG gewährten Erlaubnisse zur Kenntnisnahme und zur Weiterverwendung decken indes offensichtlich nicht die im Sachverhalt erkennbaren berechtigten Interessen des Arbeitgebers, weil sie begrenzt sind auf Kenntnisnahmen in dem zur „Erbringung des Dienstes" beziehungsweise zum „Betrieb der Telekommunikationsanlagen" erforderlichen Maß. Hieran zeigt sich besonders deutlich, dass § 3 Abs. 3 TTDSG für den Kreis von Verpflichteten gedacht ist, welcher noch im TTDSG-RefE vorgesehen war, nämlich nur die Anbieter öffentlicher Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze. Der Regelung ist eine „Eigenerbringung" durch den Nutzer fremd, der insoweit eben nicht selbst Anbieter von Telekommunikationsdiensten oder Anlagenbetreiber sein sollte. Dieser Fall wurde, wie sich vorliegend zeigt, nicht bedacht.

2.4.3 Zeitliche Dimension des Verbots nach § 3 Abs. 3 TTDSG

Besonders hervorzuheben ist, dass die Regelungen des § 3 TTDSG nicht zeitlich begrenzt sind auf den Vorgang der „Übertragung einer Nachricht" als einzelne Nutzung eines Telekommunikationsdienstes, sondern zeitlich unbegrenzt darüber hinaus gelten sollen. Dies hat der Gesetzgeber des TTDSG durch unreflektierte Übernahme der Vorgängerregelung des § 88 TKG übernommen, soweit es in § 3 Abs. 2 S. 2 TTDSG heißt:

> „Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist."

Auch dies passt konzeptionell zum Kreis von Verpflichteten, welcher noch im TTDSG-RefE vorgesehen war. Im Übrigen sei angemerkt, dass sich die „einfachgesetzliche" Rechtslage des § 3 TTDSG insoweit von der verfassungsrechtlichen Rechtslage, die nach der Auslegung des BVerfG von Art. 10 GG gegeben ist, unterscheidet – was bisweilen von den Instanzgerichten übersehen wird.[16] Der Schutz des Fernmeldegeheimnisses im Sinne von Art. 10 GG ist nur für einen begrenzten Zeitraum gegeben, nämlich kurzgesagt während der Übertragung einer Nachricht. Konkret prüft das BVerfG das Vorliegen einer „grundrechtsspe-

[16] LAG Hessen, Urt. v. 21.09.2018 – 10 Sa 601/18, Rn. 60 (in Verkennung der wortgleichen Vorgängernorm, § 88 Abs. 2 S. 2 TKG (a. F.)).

zifischen Gefährdungslage“ i. S. v. Art. 10 GG und orientiert sich dabei u.a. an dem im Sachverhalt geschilderten, technisch spezifizierten Endpunkt der Übertragung der Nachricht (Mail User Agent) oder Mail Delivery Agent).[17] Nach der Übertragung fallen die Informationen in der Nachricht, die zuvor dem Schutz des Fernmeldegeheimnisses unterstanden, wie auch vor Beginn der Übertragung nur unter das Grundrecht auf informationelle Selbstbestimmung, mithin dem Datenschutz. Vor diesem Hintergrund sind Ansichten in der Literatur abzulehnen, die das grundgesetzliche sowie das einfachgesetzliche Fernmeldegeheimnis undifferenziert behandeln und etwa Formulierungen dieser Art wählen: Das Fernmeldegeheimnis ist ein grundrechtlich verankertes Recht, welches in Art. 10 Abs. 1 GG normiert ist und durch § 3 TTDSG präzisiert wird.[18]

3. Kollision einer Verordnung mit der nationalen Umsetzung einer Richtlinie

Im Regelungsbereich der DS-GVO ist das Verhältnis von DS-GVO, BDSG und TTDSG nach den allgemeinen Regeln über die Normenkollision aufzulösen, das heißt die DS-GVO geht als Verordnung i. S. d. Art. 288 Abs. 2 AEUV mitgliedstaatlichen Vorschriften vor, soweit nicht eine Öffnungsklausel zugunsten nationalen Rechts vorliegt.[19] Soweit die Informationen, die nach § 3 Abs. 1 TTDSG dem Fernmeldegeheimnis unterliegen (S. 1) und auf die sich das Fernmeldegeheimnis erstreckt (S. 2), für den Arbeitgeber als Verantwortlichen personenbezogene Daten gem. Art. 4 Nr. 1 DS-GVO sind, verbietet sich die Anwendbarkeit des einfachgesetzlichen Fernmeldegeheimnisses (konkret: § 3 Abs. 3 TTDSG), um eine i. S. v. Art. 4 Abs. 3 EUV effektive Wirkung der DS-GVO zu ermöglichen. Dies gilt jedenfalls für „*rein innerbetriebliche*“ Kommunikation via E-Mails.[20]

Diese Argumentation, welche insbesondere im Kontext von Art. 6 Abs. 1 S. 1 lit. f) DS-GVO steht, setzt sich zutreffend mit Art. 95 DS-GVO und dem sehr weiten Gestaltungsspielraum der Mitgliedsstaaten auseinander, welcher diesen durch Art. 5 Abs. 1 Richtlinie 2002/58/EG zugebilligt wurde. Der Wortlaut der Richtlinie beschränkt sich auf den Regelungsauftrag, dass die Mitgliedsstaaten die Vertraulichkeit der Kommunikation durch innerstaatliche Vorschriften sicherzustellen haben. Zutreffend wird jedoch hervorgehoben, dass die Richtlinie 2002/58/EG ausweislich ihres Art. 3 Abs. 1 nur für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung „öffentlich zugänglicher“ elektronischer Kommunikationsdienste „in öffentlichen“ Kommunikationsnetzen in der Gemeinschaft gilt und dass es daran bei der rein innerbetrieblichen Kommunikation via E-Mail evident fehle. Insoweit enthält daher § 3 Abs. 3 TTDSG eine überschießende Umsetzung der Richtlinie 2002/58/EG. Überschießende Regelungen sind jedoch ein rein nationales Recht und als solches nicht von der Öffnungsklausel des Art. 95 DS-GVO privilegiert.[21]

Das Nebeneinander von DS-GVO und nationalen datenschutzrechtlichen Vorschriften, welche eine Umsetzung der RL 2002/58/EG darstellen, ist hingegen nicht abschließend geklärt. Virulent wird diese Fragestellung, wenn der Blickwinkel über die zuvor betrachtete, innerbetriebliche Kommunikation via E-Mail hinaus erweitert wird und „das übliche Tagesgeschäft“, namentlich eingehende und ausgehende Handelsbriefe i. S. v. § 257 Abs. 1 Nr. 2, 3 HGB in Gestalt von E-Mails, in den Blick genommen werden. Das in der Literatur formulierte Argument, „*ein pauschales Verbot der Datenverarbeitung im Telekommunikationskontext ohne die Möglichkeit der Verarbeitung aufgrund eines erheblichen Interesses* [wie in § 3 Abs. 3 TTDSG vorgesehen] *sei eine unzulässige Beschränkung des unionalen Datenschutzniveaus*“[22], trägt die dort gewünschte Schlussfolgerung nicht, dass das Fernmeldegeheimnis nach § 3 Abs. 3 TTDSG vollständig von der DS-GVO verdrängt wird. Denn die DS-GVO ist nur auf die Verarbeitung von Daten in Bezug auf natürliche Personen, mithin personenbezogene Daten, anwendbar.

Die anhand der rein innerbetrieblichen Kommunikation via E-Mail entwickelte, zutreffende Argumentation greift jedoch auch hier durch. Die in Abweichung zum Ref-E hinzugefügten Nr. 2 und Nr. 4 in § 3 Abs. 2 S. 1 TTDSG finden keine Grundlage in der Richtlinie 2002/58/EG, aufgrund deren Geltungsbereichs. Folglich wird § 3 Abs. 3 TTDSG insoweit durch Art. 6 Abs. 1 DS-GVO verdrängt.

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 mbB in Duisburg.

▶ www.sds.ruhr

SDS Rechtsanwälte

[17] BVerfG, Urt. v. 16.6.2009 - 2 BvR 902/06 Rn. 48 (dort: IMAP).

[18] Diel/Selzer, CR 2022, 119 (119).

[19] Golland, NJW 2021, 2238 (2238).

[20] Wünschelbaum, NJW 2022, 1561 (1563).

[21] Golland in: Taeger/Gabel, DSGVO – BDSG – TTDSG, DSGVO Art. 95 Rn. 17.

[22] Wünschelbaum, NJW 2022, 1561 (1564)

Microsoft 365

So erfüllen Verantwortliche ihre Rechenschaftspflicht.

Kristin Benedikt

Die deutschen Datenschutzaufsichtsbehörden veröffentlichten im November 2022 eine weitere Stellungnahme zum Einsatz von Microsoft 365. Die Meinung der Datenschützer überrascht wenig. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) kommt nach einer Prüfung zu dem Ergebnis, dass der rechtmäßige Einsatz von Microsoft 365 nicht nachgewiesen werden kann. Die Veröffentlichung der DSK ist Anlass genug, um zu prüfen, was sich in den letzten Monaten in punkto Microsoft 365 getan hat und wie Verantwortliche ihre Rechenschaftspflicht erfüllen können.

1. Stellungnahme der DSK

Die DSK veröffentlichte am 25.11.2022 eine „Festlegung“[3] zu Microsoft-Onlinediensten. Nach der Geschäftsordnung[1] der DSK handelt es sich bei den Festlegungen um Positionen zu internen inhaltlichen, technischen und organisatorischen Fragen einschließlich der Gremienarbeit. Die DSK kann gemeinsame Positionen unter den deutschen Datenschutzaufsichtsbehörden auch in Form von Erschließungen, Beschlüssen oder Orientierungshilfen veröffentlichen. Diese Unterscheidung ist für Verantwortliche eher nebensächlich. Denn egal wie die DSK ihre Veröffentlichungen nennt, jede Veröffentlichung ist für Verantwortliche und Auftragsverarbeiter von Bedeutung. Immerhin erklären die Aufsichtsbehörden in diesen Veröffentlichungen, wie sie datenschutzrechtliche Regelungen auslegen und welche Anforderungen bei der Datenverarbeitung zu beachten sind. Doch sind die Veröffentlichungen der DSK für Unternehmen keinesfalls verbindlich. Sie binden noch nicht einmal die einzelnen Aufsichtsbehörden, die Teil der DSK sind.[2]

Die Veröffentlichung der DSK zu Microsoft 365 verweist auf einen achtseitigen Bericht, in dem das Verfahren zur Prüfung und die wesentlichen Ergebnisse zusammengefasst werden. Grundlage für die Prüfung der DSK war der „Datenschutznachtrag“ in der Fassung vom 15. September 2022, den Microsoft zur Verfügung stellt. Die DSK betont, dass weder tatsächlich stattfindende Datenflüsse noch einzelne Verarbeitungstätigkeiten überprüft wurden. Ebenso wenig wurden die Vertragsunterlagen von Microsoft vollumfänglich berücksichtigt. Auch Fragen zum TTDSG, insbesondere zum Telekommunikationsrecht, blieben außen vor. Dabei wirft gerade das TTDSG und seine Regelung zum Fernmeldegeheimnis viele Fragen auf, insbesondere bei Videokonferenzsystemen. Die DSK kommt zu dem Ergebnis, dass die Vertragsunterlagen von Microsoft nach wie vor unzureichend sind. Verarbeitungszwecke und Arten der verarbeiteten personenbezogenen Daten werden nicht hinreichend bestimmt. Weiterhin bleibt unklar, für welche eigenen Zwecke Microsoft

[1] Geschäftsordnung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz), Stand: 21.9.2022, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_09-2021.pdf [17.2.2023].

[2] Auswertungsbericht des AK Medien, Konsultation zur Orientierungshilfe für Anbieter von Telemedien, Stand: 19.10.2022, S. 5, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Auswertung_Konsultation_zur_Orientierungshilfe_fuer_Anbieter_von_Telemedien_final.pdf [17.2.2023].

[3] Festlegung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Stand: 24.11.2022, abrufbar unter: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf

die personenbezogenen Daten verarbeitet. Außerdem würden konkrete Angaben zu den technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO sowie zu den eingesetzten fehlen. Ungelöst ist nach wie vor das Problem hinsichtlich der Datenübermittlung in Drittstaaten. Dies betrifft nach der „Schrems II"-Entscheidung des EuGH nicht nur die Datenübermittlung in die USA, sondern auch in andere Drittländer.

Aus Sicht der DSK ist die Datenverarbeitung beim Einsatz von Microsoft 365 nicht hinreichend transparent. Da liegt die Schlussfolgerung nahe: Wenn der Verantwortliche die Datenverarbeitung nicht im Detail kennt, kann er auch nicht nachweisen, dass er die Grundsätze der Verarbeitung einhält. Der Verantwortliche kann somit seine Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nicht erfüllen. Konsequenterweise hätte die DSK die Schlussfolgerung treffen müssen, dass bei einem Verstoß gegen die Rechenschaftspflicht die Datenverarbeitung nicht stattfinden darf. Ein solches Fazit fehlt jedoch und bleibt den Verantwortlichen sowie Microsoft überlassen.

2. Reichweite der Rechenschaftspflicht

Microsoft hat ebenfalls am 25.11.2022 eine Gegendarstellung veröffentlicht und findet deutliche Worte zur Meinung der DSK. Microsoft wirft den deutschen Aufsichtsbehörden vor, übermäßig risikoscheu zu sein und die Pflichten der DSGVO ausufernd auszulegen, was im Ergebnis dazu führt, dass die Digitalisierung in Deutschland ausgebremst wird.[3] Eine der zentralen Fragen ist, wie die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO zu verstehen ist. Aus Sicht von Microsoft muss die technische Funktionsweise von Microsoft 365 nicht vollständig verstanden werden. Die Kunden würden von Microsoft eine umfangreiche Dokumentation erhalten, um ihre Rechenschaftspflicht erfüllen zu können.

Tatsächlich ist höchst umstritten, wie weit die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO reicht und wie der Verantwortliche seine Verarbeitungstätigkeiten dokumentieren soll. Zwar enthält die DSGVO einige explizite Dokumentationspflichten, wie zum Beispiel das Verzeichnis über Verarbeitungstätigkeiten, die Datenschutz-Folgenabschätzung, Hinweise zum Datenschutz gemäß Art. 13, 14 DSGVO sowie die inhaltlichen Vorgaben zum Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DSGVO. Verantwortliche, die ausschließlich die Mindestangaben im Verzeichnis nach Art. 30 DSGVO aufnehmen, kommen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO nicht ansatzweise nach. Empfehlenswert ist es, die Dokumentation um folgende Nachweise zu ergänzen:

- Konzepte für Gewährleistung der Betroffenenrechte
- Prozesse der Datenschutzorganisation
- Interne oder externe Audits
- Mitarbeiterschulungen
- Rechtsgutachten
- Berichte, Vermerke oder Protokolle

Auch der EuGH hat sich bisher nicht abschließend zur Frage geäußert, wie die Rechenschaftspflicht zu verstehen ist und wie detailliert der Verantwortliche den Nachweis über eine rechtmäßige Datenverarbeitung erbringen muss. Der EuGH hat lediglich in einem Vorabentscheidungsverfahren beiläufig erwähnt, dass die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO dahingehend zu verstehen sei, dass der Verantwortliche die Beweislast dafür trägt, dass er Daten rechtmäßig verarbeitet.[4] Das Bundesverwaltungsgericht griff diesen Gedanken auf und entschied in einem Verfahren zum Recht auf Berichtigung, dass es sich bei Art. 5 Abs. 2 DSGVO um eine Beweislastregel handelt, die den nationalen Beweisregeln vorgeht.[5]

TIPP ZUR RECHENSCHAFTSPFLICHT

Verantwortliche sollten ihre Dokumentation in jedem Fall ergänzen. Zusätzlich zum aktuellen „Datenschutznachtrag" sollten Verantwortliche weitere Informationen zur Datenverarbeitung von Microsoft prüfen. Zahlreiche Erläuterungen, Muster und sonstige Hilfestellungen finden Kunden im Trust-Center von Microsoft und in den zahlreichen frei zugänglichen Online-Beiträgen. Kleiner Wermutstropfen: Bei der Vielzahl an Veröffentlichungen kann man schnell den Überblick für das Wesentliche verlieren. Microsoft hat in seiner Stellungnahme vom 25.11.2022[6] die wichtigsten Fundstellen verlinkt. Verantwortliche finden dort neben den Angaben zum Speicherort oder zu den verarbeiteten Datenkategorien auch Hinweise zum Umgang mit Betroffenenanfragen und zur Datenschutz-Folgenabschätzung.

[4] Microsoft, Stellungnahme von Microsoft Deutschland zur datenschutzrechtlichen Bewertung von Microsoft 365 durch die DSK, 25.11.2022, abrufbar unter: https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/2022.11_Stellungnahme-MS-zu-DSK_25NOV2022_FINAL.pdf [17.2.2023].

[5] EuGH, Urteil vom 24.2.2022 - C 175/20, Rn. 81.

[6] Microsoft, Stellungnahme von Microsoft Deutschland zur datenschutzrechtlichen Bewertung von Microsoft 365 durch die DSK, 25.11.2022, abrufbar unter: https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/2022.11_Stellungnahme-MS-zu-DSK_25NOV2022_FINAL.pdf [17.2.2023].

3. Neuer Vertrag zur Auftragsverarbeitung

Nur wenige Wochen nach der Veröffentlichung der DSK hat Microsoft einen neuen „Datenschutznachtrag“ veröffentlicht.[7] Diesen sollten Verantwortliche unbedingt kennen und archivieren. Das gilt für sämtliche Dienstleister, die Verträge zur Auftragsverarbeitung bereitstellen. Es sollten stets die aktuellen Versionen geprüft und zu Nachweiszwecken gespeichert werden. Im aktuellen Datenschutznachtrag hat Microsoft die Kritikpunkte der DSK nur geringfügig aufgegriffen. Die Details zur Verarbeitung, wie beispielsweise Art und Zweck der Verarbeitung oder die Kategorien von Daten, wurden nicht aktualisiert. Neu sind Angaben zu Weisungsrechten und zum Ort der Datenspeicherung. Außerdem wird klargestellt, dass Microsoft ein Anbieter von Telekommunikationsdiensten ist und somit das Telekommunikationsrecht beachten muss. Diese Klarstellung bezieht sich vor allem auf die Dienste „Teams“ und „Skype“ und hat weitreichende Folgen für Anwender von Videokonferenzsystemen.

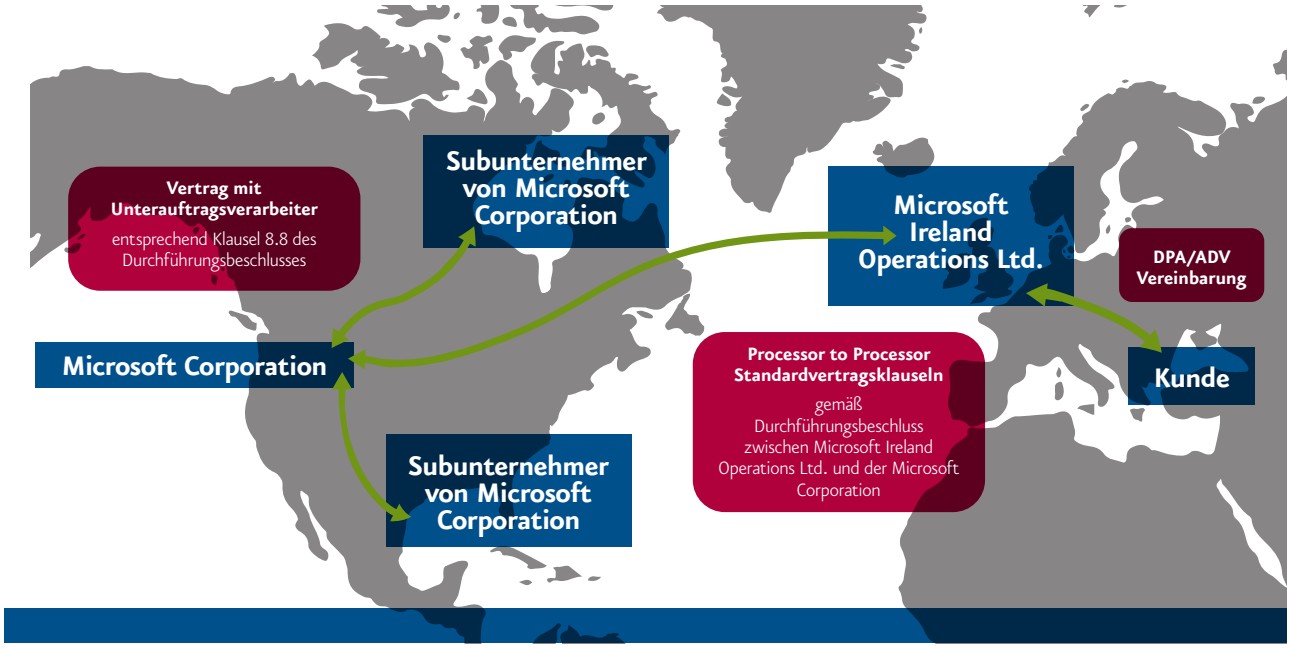
4. Telekommunikationsrecht

Als Anbieter eines Telekommunikationsdienstes ist Microsoft verpflichtet, das Fernmeldegeheimnis gem. § 3 TTDSG zu beachten. Dem Fernmeldegeheimnis unterliegen nicht nur die Inhalte der Telekommunikation, d.h. die Nachrichteninhalte wie Text-, Bild- oder Sprachnachrichten, sondern auch die näheren Umstände der Telekommunikation. Mit letzterem sind die sog. Metadaten gemeint wie z.B. Telefonnummern oder Nutzerkennungen sowie Dauer und Umfang der Telekommunikation. Unerheblich ist, ob es sich aus Sicht der Nutzer um eine private, dienstliche der geschäftliche Kommunikation handelt. Die Vertraulichkeit der Kommunikation umfasst auch juristische Personen. Ebenso wenig spielt es keine Rolle, ob es sich um personenbezogene Daten handelt oder nicht.[8] Grundsätzlich keine Verpflichteten im Sinne des Telekommunikationsrechts sind somit die Unternehmen oder die öffentlichen Stellen, die Microsoft Teams für die interne oder externe Kommunikation nutzen. Sie gehören stattdessen zum geschützten Personenkreis.[9] Folglich ist Microsoft auch kein Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO, soweit es um die Durchführung von Videokonferenzen geht, sondern der Verpflichtete nach dem Telekommunikationsrecht.[10]

5. Drittstaatentransfer

Die EU-Kommission hat im Dezember 2022 offiziell das Verfahren zur Annahme des neuen Angemessenheitsbeschlusses zwischen der EU und den USA, das sogenannte „Trans-Atlantic Data Privacy Framework“ (TADPF), aufgenommen.

Der Angemessenheitsbeschluss ist noch lange nicht verabschiedet und schon gibt es heftige Kritik. Unter anderem hat der LIBE-Ausschuss des Europäischen Parlaments Bedenken geäußert



Vertragliche Konstruktion zur Datenübermittlung innerhalb des Microsoft Konzerns

[7] Datenschutznachtrag zu den Produkten und Services von Microsoft, 01.01.2023, abrufbar unter: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

[8] Assion, TTDSG § 3 Rn. 37; Schwartmann/Jaspers/Eckhardt, TTDSG § 3 Rn. 11.

[9] Konkret gehört der Mitarbeiter als Beteiligter an der Telekommunikation zum geschützten Personenkreis.

[10] Vgl. Assion, TTDSG § 3 Rn. 140.

und kommt zu dem Schluss, dass auch das neue EU-USA-Abkommen kein gleichwertiges Schutzniveau schaffen wird.[11] Verantwortliche sollten sich daher nicht allzu große Hoffnung machen, dass das TADPF zum einen frühzeitig beschlossen wird und zum anderen auch lange Bestand hat. Immerhin hat Maximilian Schrems schon mehrfach angekündigt, den erneuten Angemessenheitsbeschluss schnellstmöglich vor den EuGH zu bringen.

Umso mehr lohnt sich ein Blick auf die Standardvertragsklauseln

TIPP ZUR RECHENSCHAFTSPFLICHT

Kunden von Microsoft sollten unbedingt die zwischen der Microsoft Ireland Operations Ltd. und Microsoft Corporation vereinbarten Standardvertragsklauseln kennen. In diesem Vertragsdokument werden zusätzlich zum Vertrag zur Auftragsverarbeitung konkrete Angaben zu den übermittelten Kategorien von Daten und die getroffenen technischen und organisatorischen Maßnahmen aufgelistet. Mithilfe dieser Angaben kann die eigene Dokumentation ergänzt werden, um die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO zu erfüllen.

und die ergänzenden Maßnahmen, die Microsoft trifft. Europäische Kunden von Microsoft schließen mit der Microsoft Ireland Operations Ltd. mit Sitz in Irland den „Datenschutznachtrag", d.h. den Vertrag zur Auftragsverarbeitung ab. Die Standardvertragsklauseln im Modul Auftragsverarbeiter-Auftragsverarbeiter schließt die Microsoft Ireland Operations Ltd. mit der Microsoft Corporation ab.[12] Die ergänzenden Maßnahmen wurden zugleich in Microsofts Vertrag zur Auftragsverarbeitung, konkret in „Anhang C – Nachtrag zu den zusätzlichen Schutzmaßnahmen" aufgenommen. Demzufolge ist Microsoft Ireland Operations Ltd. der Datenexporteur und nicht wie lange Zeit angenommen, der Kunde von Microsoft, der beispielsweise seinen Sitz in Deutschland hat.

6. Handlungsempfehlungen

Verantwortliche sollten anlässlich der Veröffentlichung der DSK zeitnah die vorhandene Dokumentation prüfen, um Handlungsbedarf zu ermitteln. Ausgangspunkt einer jeden datenschutzrechtlichen Prüfung ist das Verzeichnis über Verarbeitungstätigkeiten. Empfehlenswert ist es, das Verzeichnis über Verarbeitungstätigkeiten um die Angaben

- Mittel der Verarbeitung
- Rechtsgrundlagen und
- Risiko der Verarbeitung

zu erweitern.

Unter Mittel der Verarbeitung sind die konkreten Anwendungen und Dienste von Microsoft aufzulisten, z.B. Teams, Word, Access, Sway etc.

Außerdem sollten für jede Verarbeitungstätigkeit die in Betracht kommenden Rechtsgrundlagen angegeben werden. Erfolgt die Datenverarbeitung beispielsweise gem. Art. 6 Abs. 1 lit. f) DSGVO, kann in dieser Stelle auf die detaillierte Interessenabwägung verwiesen werden. Selbst in Fällen, in denen keine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO erforderlich ist, sollte der Verantwortliche das Risiko der Datenverarbeitung ermitteln. Eine Risikoeinschätzung hilft nicht nur dabei, die Anforderungen an die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO zu bestimmen. Die Feststellungen zum Risiko der Verarbeitung können zugleich helfen, die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f) DSGVO zu dokumentieren und den Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO zu ergänzen. Bei all den Dokumentations- und Nachweispflichten sollten Verantwortliche eines nicht vergessen: Die Rechenschaftspflicht ist nicht nur eine bürokratische Bürde, sondern kann den Verantwortlichen in aufsichtlichen oder gerichtlichen Verfahren entlasten. Das gilt vor allem dann, wenn der Verantwortliche substantiiert darlegen kann, welche Maßnahmen er getroffen hat, um aus seiner Sicht Microsoft 365 rechtmäßig einsetzen zu können.

Über die Autorin

Kristin Benedikt

ist Richterin und Datenschutzbeauftragte am Verwaltungsgericht Regensburg. Sie gehört dem Vorstand der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. und des Instituts für Europäisches Medienrecht e.V. (EMR) an.

[11] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2023/2501(RSP), 14.2.2023.

[12] Die aktuell vereinbarten Standardvertragsklauseln mit ergänzenden Maßnahmen zwischen der Microsoft Ireland Operations Ltd. mit der Microsoft Corporation sind im geschützten Kundenbereich abrufbar.

LOTSE DURCH DEN DATENSCHUTZ-DSCHUNGEL: DER DATENSCHUTZ-BEAUFTRAGTE

Andrea Backer-Heuveldop, Bernd Schütze

Compliance benötigt mehr als „nur“ Kenntnis der Vorschriften

Die Kenntnis und Vermittlung der Datenschutzvorschriften an die Beschäftigten alleine versetzt weder Verantwortliche noch Auftragsverarbeiter in die Lage, im Datenschutz rechtliche Compliance zu erreichen. Vielmehr sind strategische Überlegungen anzustellen und Festlegungen zu treffen, um diese gesetzlichen Vorgaben effektiv und rechtssicher in der eigenen Organisation so umzusetzen, dass ein Nutzen für das eigene Unternehmen daraus resultiert. Die Überwachung der Einhaltung der DS-GVO, anderer Datenschutzvorschriften der EU oder ihrer Mitgliedsstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen obliegt gem. Art. 39 Abs. 1 lit. b DS-GVO wiederum dem oder der betrieblichen oder behördlichen Datenschutzbeauftragten (DSB).

Die „Strategien des Verantwortlichen oder Auftragsverarbeiters“ werden in der DS-GVO selbst nicht legal-definiert, aber in Erwägungsgrund (EWG) 78 konkretisiert:

> „Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.“

EWG 78 führt weiter beispielhaft auf, worin entsprechende Maßnahmen bestehen können und nennt Datenminimierung, Pseudonymisierung, Herstellung von Transparenz, Schaffung von Überwachungsmöglichkeiten für die betroffene Person und Verbesserungsmöglichkeiten der Sicherheitsfunktionen für den Verantwortlichen.

Interne Strategien müssen als organisatorische Maßnahmen im Sinne von Art. 24 Abs. 1 DS-GVO verstanden werden.[1] Der Verantwortliche wie auch Auftragsverarbeiter[2] im Sinne des Art. 28 DS-GVO müssen daher entsprechende Maßnahmen vor und während einer Verarbeitung personenbezogener Daten festlegen.

Es obliegt der höchsten Managementebene interne Strategien zu entwickeln und dabei eindeutig zu definieren, wer in der Organisation welche Aufgaben bei der Umsetzung der Datenschutzvorgaben verantwortet. Bei dieser Aufgabe steht der oder die DSB für Beratung zur Verfügung, denn Beratung gehört entsprechend Art. 39 Abs. 1 lit. a DS-GVO zu den originären Aufgaben des oder der DSB. Die Erarbeitung entsprechender Strategien selbst darf jedoch nicht auf den oder die DSB übertragen werden; da Datenschutzbeauftragte gemäß Art. 39 Abs. 1 lit. a DS-GVO die Einhaltung der datenschutzrechtlichen Vorgaben überwachen und bewerten müssen, würde hier ein Interessenskonflikt vorliegen, wenn der oder die DSB die selbst entwickelten Strategien beurteilen muss.

Daher ist eine Übertragung entsprechender Aufgaben von der höchsten Managementebene auf den oder die DSB rechtlich nicht zulässig und würde einen Verstoß gegen die Vorgaben der DS-GVO darstellen. Auch bei der Vereinbarung von Einzelregelungen zum Datenschutz, etwa in Betriebsvereinbarungen, sollte darauf geachtet werden, dass diese nicht Konkretisierungen der gesetzlichen Aufgaben der oder des DSB beinhalten, die nicht mit der Weisungsfreiheit der Rolle oder mit dem Vertrag des externen DSB beziehungsweise der Stellenbeschreibung des internen DSB vereinbar sind. Festlegungen des Verantwortlichen oder Auftragsverarbeiters zum Datenschutz lassen sich an vielen Stellen finden. Es kann sich dabei um spezifische Verfahrens- oder Organisationsanweisungen zum Datenschutz handeln, die im günstigsten Fall unter Einbeziehung des oder der DSB festgelegt werden, aber oftmals finden sich mehr oder weniger detaillierte Vorgaben in Betriebsvereinbarungen, Prozessbeschreibungen, Arbeitsanweisungen oder gar Erläuterungen zur Verwendung von Formblättern oder in der Organisation zu verwendende Muster. Nicht immer stehen diese Elemente zueinander in Beziehung oder berücksichtigen die an anderer Stelle geregelten Vorgaben. Mitunter wurde bei der Festlegung einzelner Regelungen Vorgaben aus dem Datenschutz nicht mit bedacht, obwohl diese Regelungen eine Relevanz für andere Regelungen zum Umsatz der Vorgaben des Datenschutzes beinhalten. So kann beispielsweise in Betriebsvereinbarungen ein so hoher Schutz der Beschäftigtendaten vereinbart worden sein, dass in der Folge notwendige Kontrollen zum Schutz anderer Betroffenenkreise als unzulässig klassifiziert werden.

Es gehört auch zur Beratungsaufgabe des DSB zur Verknüpfung solcher losen Enden im Datenschutz zu beraten. Ob der oder die benannte DSB alle bestehenden Einzelregelungen überhaupt kennen kann, ist dabei maßgeblich davon abhängig, wie konsequent seine oder ihre ordnungsgemäße Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen in der Organisation auch wirklich dort gelebte Praxis ist. Wie kann man als DSB in Wahrnehmung der Beratungsaufgabe zu einer Verringerung loser Enden beitragen? Dabei können beispielsweise die nachfolgend genannten zwei Anknüpfungspunkte helfen:

- Eine gute Zusammenarbeit mit der Personalvertretung ist essentiell. Einerseits bedarf auch die Personalvertretung eine Beratung des DSB, denn entsprechend § 79a BetrVG muss die Personalvertretung bei der Verarbeitung personenbezogener Daten die Vorschriften über den Datenschutz einhalten. Eine Zusammenarbeit ist allein schon aus diesem Grund unab-

[1] Moos F.: Art. 39, Rn. 10. In: Wolff/Brink (Hrsg.) Beck'scher Online-Kommentar. 42. Edition, Stand 2021-11-11

[2] Verantwortliche dürfen nur Auftragsverarbeiter beauftragen, die geeignete technische und organisatorische Maßnahmen umsetzen können, was insbesondere auch bedingt, dass die vom Verantwortlichen festgelegten Vorgaben wie Regelungen eingehalten werden, was wiederum auch entsprechende organisatorische Maßnahmen beinhaltet. So z.B.: Spoerr W.: Art. 28, Rn. 33. In: Wolff/Brink (Hrsg.) Beck'scher Online-Kommentar. 42. Edition, Stand 2021-11-11

dingbar. Aber die Personalvertretung erfährt als Anlaufstelle der Beschäftigten mit an erster Stelle von diesen, wenn betriebsinterne Regelungen nicht zum Arbeitsalltag passen, sodass sie eine wichtige Informationsquelle für Datenschutzbeauftragte darstellt. Zudem gehört gemäß § 80 Abs. 1 Ziff. 1 BetrVG auch die Überwachung der Einhaltung von Datenschutzvorschriften zu den Aufgaben der Personalvertretung. Die ordnungsgemäße Anwendung der DS-GVO ist für eine Personalvertretung verpflichtend, sodass hieraus gegebenenfalls auch eine Informationspflicht erwachsen kann, den DSB bei potentiellen Risiken eines Verstoßes gegen Datenschutzvorschriften zu informieren. Hier ist vom DSB, der ja eine Berichtspflicht gegenüber den Verantwortlichen hat, ein sensibler Umgang mit den Informationen gefordert, insbesondere muss neben der Verschwiegenheitspflicht gem. § 79a S. 4 BetrVG über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen, gegebenenfalls auch die aus Art. 38 Abs. 5 DS-GVO resultierende Pflicht zur Verschwiegenheit zum Schutz von Informanten beachtet werden.

- Die Schulung von Beschäftigten ist nicht nur eine Pflicht, sondern immer auch eine gute Gelegenheit mit Beschäftigten ins Gespräch zu kommen und zu erfahren, wo sie eine Diskrepanz zwischen gesetzlichen und betrieblichen Vorgaben sehen. Vielfach können Beschäftigte dabei Hinweise geben, wie man interne Vorgaben anpassen könnte, damit gesetzliche Vorgaben und betriebliche Erfordernisse in Einklang gebracht werden können. Dabei müssen DSB im Rahmen der Kommunikation beachten, dass sie keine Erwartungen auf Änderungen erwecken: Die Aufgabe der oder des DSB in diesen Punkten ist „Unterrichtung und Beratung", die Entscheidung über Änderungen liegt allein beim Verantwortlichen.

Eine gute Kommunikationsfähigkeit, ausgeprägte soziale Kompetenzen sowie ein zielorientierter Lösungswille sind Grundvoraussetzungen, damit DSB erfolgreich ihre Aufgaben erfüllen können.

Zusammenarbeit höchste Managementebene und DSB

Die DS-GVO differenziert bei den Aufgaben des DSB bezüglich der Strategien des Verantwortlichen. Während die Überwachung der Strategien zu seinen gesetzlichen Aufgaben gem. Art. 39 Abs. 1 lit. b DS-GVO gehört, fordert sie seine Beratung in § 39 Abs. 1 lit. a bei der Festlegung der Strategien zwar nicht ausdrücklich ein, aber sie verlangt Beratung hinsichtlich der Pflichten von Verantwortlichen und Auftragsverarbeiter „nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften", was insbesondere natürlich auch die Vorgaben von Art. 24 DS-GVO einschließt. Jedoch sind weder Verantwortliche noch Auftragsverarbeitender verpflichtet, die Beratung der oder des DSB bei der Festlegung der Strategien einzuholen,[3] obgleich eine Pflicht zur „frühzeitigen Einbindung" zu beachten ist;[4] Verantwortliche dürfen DSB nicht „außen vor lassen". Verantwortliche sind verantwortlich für die Einhaltung aller gesetzlichen Vorgaben zum Datenschutz, auch die in Art. 38 Abs. 1 DS-GVO verankerte Vorgabe zur Einbindung des oder der DSB muss beachtet werden. Im Rahmen seiner Verpflichtung zur Berichterstattung gegenüber der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters muss der DSB zudem auf seiner Einschätzung nach nicht ausreichende oder – wenn notwendig – sogar auf widersprüchliche Strategien hinweisen.[5] Verstöße gegen die gesetzlich vorgegebene Vorgabe zur frühzeitigen Einbindung von DSB unterliegen ebenfalls der Berichtspflicht, auch hierauf muss also hingewiesen sowie hinsichtlich der Möglichkeiten zur Umsetzung der gesetzlichen Umsetzung beraten werden.

Aus EWG 77 ergibt sich, dass der oder die DSB durch Hinweise Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter geeignete Maßnahmen durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist, geben kann, „insbesondere was die Ermittlung des mit der Verarbeitung verbundenen Risikos, dessen Abschätzung in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für dessen Eindämmung betrifft". In entsprechenden Berichten an das höchste Management sollten Hinweise, wo entsprechende Hinweise zu bestimmten Themen zu finden sind, enthalten sein.

[3] Sydow/Marsch DS-GVO/BDSG/Helfrich, 3. Aufl. 2022, DS GVO Art. 39 Rn. 79

[4] Moos F.: Art. 39, Rn. 6. In: Wolff/Brink (Hrsg.) Beck'scher Online-Kommentar. 42. Edition, Stand 2021-11-11

[5] siehe auch Sydow/Marsch DS-GVO/BDSG/Helfrich, 3. Aufl. 2022, DS GVO Art. 39 Rn. 80 zum Hinweis im Rahmen der Überwachungsaufgabe

Bin ich mir als DSB darüber bewusst, dass ich beim Management die Bedeutung dieser festzulegenden Datenschutzstrategien schärfen muss?

Um das Management von der Umsetzung von Best Practices im Datenschutz zu überzeugen, ist zunächst die Grundlage dafür zu schaffen, dass ein Bewusstsein bei der Geschäftsführung oder Leitung der Behörde, Einrichtung oder anderer Stelle dafür entsteht, dass sich Compliance im Datenschutz nur durch eine gute Datenschutzstrategie und nicht etwa durch die Schaffung von Papiertigern erzielen lässt. Dazu bedarf es der Veranschaulichung der Risiken wie möglichen Sanktionen der Aufsichtsbehörden und Schadenersatzansprüche der betroffenen Personen als auch Imageschäden, wenn Datenschutzvorgaben nur auf dem Papier, aber nicht in der täglichen Arbeitswelt eingehalten werden. Hier kann der Hinweis hilfreich sein, dass in der Arbeitswelt gelebte Praxis gegebenenfalls und somit auch rechtlich zugeordnet werden kann. Das heißt, dass der Verantwortliche für ein entsprechendes Verhalten dann auch haftet. Ein DSB sollte also Verantwortliche darauf aufmerksam machen, dass Vorgaben, die nur auf dem Papier existieren, aber bekanntermaßen nicht gelebt werden, nicht immer vor unangenehmen Folgen schützen.

Weiterhin kann bei einer Festlegung von unkoordinierten Einzelregelungen zum Datenschutz ohne übergeordnete Strategie ein Dschungel an Regelungen entstehen, der sich im besten Fall durch mangelnde Effizienz für den Datenschutz auswirkt, aufgrund von Widersprüchlichkeiten die Organisation in ihren Abläufen behindert und lähmt oder im schlimmsten Fall sogar in bester Absicht zu dokumentierten Verstößen gegen das Datenschutzrecht führt. Zudem sind durch die Anordnung durch betriebsbedingte Regelungen entstandene Verstöße gegebenenfalls sogar als Vorsatz zu bewerten, wenn Verantwortliche von DSB im Rahmen der Erfüllung ihrer Pflicht zur Unterrichtung auf die den Datenschutzvorschriften widersprechenden internen Regelungen hingewiesen wurden.

Bezüglich der Vorteile, die sich im Gegensatz dazu aus einem gut etablierten Datenschutz-Management-Verständnis ergeben, kann zunächst damit argumentiert werden, dass sich dadurch das Vertrauen der betroffenen Personen in die Datenverarbeitung der Organisation erhöht. Dies gilt gleichermaßen für die eigenen Beschäftigten als betroffene Personen der Datenverarbeitung im Personalumfeld, was in einem immer stärker umkämpften Arbeitsmarkt einen Vorteil bei der Suche nach Fachkräften darstellen kann. Aber dies gilt natürlich auch gleichermaßen für die Betroffenenkreise, deren Daten von den eigenen Beschäftigten verarbeitet werden.

Weiterhin können Organisationen mit einer gut etablierter Datenschutzstrategie auch Kosteneinsparungseffekte erwarten, die daraus resultieren, dass die zu erledigenden Tätigkeiten für die Erfüllung der datenschutzrechtlichen Pflichten in der Organisation unter Berücksichtigung der Arbeitsteilung klar zugewiesen und in Datenschutzprozessbeschreibungen beschrieben sind. Kosten für etwaige Orientierungsphasen bezüglich der Ermittlung von Ansprechpartnern und die Prüfung von Tatbestandsvoraussetzungen im Einzelfall ohne die notwendige Expertise können so minimiert werden. Durch die Vermeidung von sich widersprechenden Regelungen durch eine abgestimmte, koordinierte Datenschutzstrategie wird zudem eine Verwirrung bei den Beschäftigten vermieden, sodass sich auch hierdurch eine Effizienzsteigerung ergibt.

Weitere Kostenersparungen können sich zudem durch die Vermeidung von Bußgeldern und Schadensersatzansprüchen durch die Beachtung von Datenschutzprozessvorgaben und Kommunikationsstrategien gegenüber Aufsichtsbehörden und Betroffenenkreisen ergeben. Risi-

ken von nicht oder nur unzureichend umgesetzten gesetzlichen Regelungen, die (auch) zu finanziellen Belastungen führen können, sind gegebenenfalls ungewisse Verbindlichkeiten entsprechend § 249 HGB in der Bilanz über Rückstellungen zu berücksichtigen, was für ein Unternehmen ebenfalls zu einer gewissen finanziellen Belastung führen kann. Um diesbezüglich argumentativ Überzeugungsarbeit leisten zu können, sollte die gesetzlich verpflichtende Möglichkeit der DSB zur Berichterstattung gegenüber der höchsten Managementebene aus Art. 38 Abs. 3 S. 3 DS-GVO regelmäßig wahrgenommen werden. Eine abstrakte Möglichkeit zur Berichterstattung nur im Eskalationsfall oder im Sinne eines reinen rückwärtsgewandten Tätigkeitsberichtes ist dafür bei weitem nicht ausreichend und entspricht auch nicht den gesetzlichen Erfordernissen. Die Beratung des Verantwortlichen resp. des Auftragsverarbeiters sollte bedarfsorientiert und anlassabhängig erfolgen, die Unterrichtung idealerweise proaktiv.[6] Die höchste Managementebene und der oder die DSB sollten idealer Weise in kontinuierlichem Austausch stehen, denn nur so können Verantwortliche den Anforderungen von Art. 38 Abs. 1 DS-GVO genügen.

Bin ich mir darüber im Klaren, dass ich den Beschäftigten bei Verantwortlichen oder Auftragsverarbeitern ein Bewusstsein für ihre Rolle vermitteln muss?

Das Datenschutzrecht unterscheidet bei der Verarbeitung personenbezogener Daten die Rollen der verarbeitenden Akteure in Verantwortliche, zu denen auch gemeinsam Verantwortliche gehören, und Auftragsverarbeiter. Die objektiv vorliegenden Kriterien der tatsächlichen Aktivitäten der Akteure in bestimmten Konstellationen, nicht hingegen eine formale Einordnung bestimmen die von diesen eingenommenen Rollen und die damit einhergehenden Pflichten.[7] Die richtige Einordnung ist insbesondere hinsichtlich des Grads der Verantwortung für die Datenverarbeitung von Bedeutung. Der Auftragsverarbeiter ist Empfänger von Daten gem. Art. 4 Nr. 9 DS-GVO, gilt aber aufgrund der gesetzlichen Privilegierung in Art. 4 Nr. 10 DS-GVO nicht als Dritter.[8] Da das Datenschutzrecht kein Konzernprivileg kennt, gelten diese Rollen auch in der Zusammenarbeit innerhalb einer Unternehmensgruppe.

Voraussetzung für die datenschutzkonforme Verarbeitung personenbezogener Daten durch die verarbeitenden Beschäftigten des Verantwortlichen oder Auftragsverarbeiters in der Praxis ist, dass diese die für ihre spezifische Tätigkeit relevanten Vorgaben kennen und anwenden.

Der oder die DSB berät die Beschäftigten des Verantwortlichen beziehungsweise Auftragsverarbeiters hinsichtlich des Rollenverständnis des Datenschutzrechts und der daraus resultierenden Pflichten und überwacht, dass diese ausreichend geschult und sensibilisiert sind.

Stellt der oder die DSB bei der Wahrnehmung der Überwachungsaufgabe fest, dass sich interne Regelungen in Prozessbeschreibungen, Richtlinien oder Handbüchern zwar finden lassen, diese aber bei den dienstlichen Tätigkeiten mangels Kenntnis nicht beachtet und befolgt werden, muss der DSB reagieren, und dem Verantwortlichen muss die Anordnung entsprechender Schulungen empfohlen werden. Auch wenn festgestellt wird, dass Anweisungen zwar existieren, diese aber nicht zur Aufgabenbeschreibung passen, sodass eine pflichtgemäße Tätigkeitserfüllung eine Anwendung der anderen Regelungen nicht ermöglicht, muss der DSB tätig werden und den Verantwortlichen auf die Widersprüchlichkeit hinweisen, sodass entweder die Regelungen oder die Tätigkeitsbeschreibung angepasst werden.

Es ist hierbei von wesentlicher Bedeutung, dass für die Beschäftigten geltenden Verfahrens- und Arbeitsanweisungen auf die vertraglichen Pflichten angemessen eingehen. Insbesondere müssen im Rahmen einer Auftragsverarbeitung eingegangene vertragliche Verpflichtungen, die Verantwortlicher und Auftragsverarbeiter im entsprechenden Auftragsverarbeitungsvertrag eingegangen sind, beachtet werden. Nur so sind die Beschäftigten in der Lage, den Weisungen und Weisungsbefugnissen aus dem Auftragsverarbeitungsverhältnis zu entsprechen. Gleichermaßen sind die aus der Vereinbarung gemeinsamer Verantwortlichkeiten resultierenden eigenen Pflichten den Beschäftigten zu vermitteln, damit eine diesen Vereinbarungen entsprechende, datenschutzkonforme Verarbeitung umgesetzt werden kann.

Mein Platz im Team – Soft Skills von DSB

Auf die benötigte Sozialkompetenz wurde schon hingewiesen, die der oder die DSB als Teamplayer, als die sich jeder DSB verstehen sollte, innerhalb der Organisation benötigt. Auch wenn die ordnungsgemäße und frühzeitige Einbindung der oder des DSB eine Verpflichtung des Verantwortlichen oder Auftragsverarbeiters darstellt, kann der oder die DSB durch die Art und Weise, wie er sich in die Organisation einbringt, entscheidend dazu beitragen, Rahmenbedingungen dafür zu schaffen, dass die Einbindung des DSB in die Unternehmensprozesse leicht fällt. Dazu gehört, dass das Selbstverständnis von DSB zunächst von der internen Beratung und einem Bewusstsein für die Interaktion mit Teams bei den Verantwortlichen oder Auftragsverarbeitern geprägt ist. Damit DSB ihren gesetzlichen Aufgaben effektiv und für sie zufriedenstellend nachkommen können, ist ihre Kommunikati-

[6] So zu finden z. B. in: Moos F.: Art. 39, Rn. 3, 6. In: Wolff/Brink (Hrsg.) Beck'scher Online-Kommentar. 42. Edition, Stand 2021-11-11

[7] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted 7.7.2020, p. 9 no. 12

[8] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted 7.7.2020, p. 9 no. 12

onsfähigkeit von zunehmender Bedeutung. DSB sollten Defizite und Konflikte im Datenschutz erkennen und lösungsorientiert ansprechen sowie zielgruppenorientiert kommunizieren können. Aufgeschlossen und offen für neue Entwicklungen auf die Fachbereiche zuzugehen, so dass eine nicht erfolgte Einbeziehung schnell nachgeholt werden kann, wird dem oder der DSB helfen, die eigene Stellung im Team zu verfestigen. Ein introvertiertes Warten im „stillen Kämmerlein" mit Blick auf das stumme Telefon oder den leeren E-Mail-Posteingang hingegen weniger.

Wie schon an früherer Stelle angesprochen: Soft Skills sind essenziell für DSB. DSB müssen ausgesprochen gute Kommunikationsfähigkeiten besitzen. Niemand hört gerne von eigenen Fehlern, aber DSB müssen regelmäßig Verantwortliche und auch Beschäftigte nicht nur über datenschutzrechtliche Vorschriften unterrichten, sondern des Öfteren muss auch auf (mögliche) Verstöße gegen Vorschriften hingewiesen werden – keine leichte Aufgabe, viel Fingerspitzgefühl ist hier erforderlich.

Obwohl DSB „nur" überwachen, unterrichten und beraten, sind sie gemäß Art. 39 Abs. 3 lit d DS-GVO zur Zusammenarbeit mit Aufsichtsbehörde verpflichtet. Ob eine Möglichkeit oder sogar Pflicht zur Meldung von schweren Verstößen existiert, wird in der Literatur unterschiedlich bewertet. Aber auf jeden Fall gehört die Bereitstellung von Dokumenten zu den Aufgaben der Zusammenarbeit, inklusive der Berichte des oder der DSB, in dem die Verstöße aufgrund der Unterrichtspflicht ja enthalten sein müssen. Daher sollte ein oder eine DSB gezielt darauf hinarbeiten, dass fortgesetzte Verstöße beim Verantwortlichen abgestellt werden. DSB benötigen daher immer auch eine gut ausgeprägte Durchsetzungsfähigkeit – die auch hilfreich sein kann, wenn einige Beschäftigte einen deutlich höheren Unterrichtungsbedarf zu datenschutzrechtlichen Vorschriften haben.

FAZIT

Das Verkaufstalent des oder der DSB ist gefordert: Denn nur wenn es gelingt, die Bedeutung der Rolle der oder des DSB für die Einhaltung der Rechenschaftspflicht durch den Verantwortlichen oder Auftragsverarbeiter darzustellen, wird die höchste Managementebene bereit sein, den oder die DSB als wertvollen Ratgeber für den Nachweis, die Anforderungen der DS-GVO zu erfüllen, zu empfinden.

Ein DSB sollte von allen an der Verarbeitung Beteiligten – sei es das Management oder die Beschäftigten – als wertvolle Ressource bei der Planung und Umsetzung von unternehmensspezifischen Vorgängen angesehen werden, als ein Partner, auf den man nicht verzichten kann und auch nicht will. Dazu muss der DSB sich in das Team integrieren und als Teammitglied interagieren.

Über die Autoren

Andrea Backer-Heuveldop
ist fachlich geprüfte fachkundige Datenschutzbeauftragte nach dem Ulmer Modell. Sie ist als externe Datenschutzbeauftragte bei ds-quadrat Unternehmensberatung GmbH & Co. KG im Gesundheitswesen tätig und engagiert sich im BvD als Sprecherin des Arbeitskreises der externen Datenschutzbeauftragten und als Mitglied des Ausschusses Recht & Politik.

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.

HARALD TRETTOW

DEN AUFTRAGSVERARBEITUNGSVERTRAG AUSGESTALTEN

Die Auswahl eines geeigneten Auftragsverarbeiters und dessen Überprüfung

Die Auswahl eines geeigneten Auftragsverarbeiters durch den Verantwortlichen nach Art. 28 Abs 3 lit. h der EU Datenschutz-Grundverordnung 2016/679 gehört zu den Grundpflichten eines jeden Verantwortlichen. Verstößt der Verantwortliche gegen diese Pflicht, kann er nach Art. 83 DS-GVO mit einem Bußgeld durch eine Aufsichtsbehörde konfrontiert werden. Gleichwohl kann aber auch eine dokumentierte und nachweisbare sorgfältige Auswahl eines Auftragsverarbeiters als weiterer Nachweis zur Erfüllung seiner Rechenschaftspflicht herangezogen werden und bei einer Bemessung von einem möglichen Bußgeld nach Artikel 83 DS-GVO relevant sein.

Gemäß Artikel 5 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 müssen personenbezogene Daten vom Verantwortlichen und vom Auftragsverarbeiter so verarbeitet werden, dass eine angemessene Sicherheit der personenbezogenen Daten durch geeignete technische oder organisatorische Maßnahmen gewährleistet ist, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Beschädigung.

Zudem ist zu beachten, dass eine regelmäßige Prüfung, Messung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung eine grundlegende Verpflichtung jedes Verantwortlichen und jedes Auftragsverarbeiters ist, die sich aus Artikel 32 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 ergibt.

Bei nachfolgenden Ausführungen wird von einem Vertragsverhältnis zwischen zwei privatwirtschaftlichen Unternehmen ausgegangen.

Rechtliche Vorgaben aus der DS-GVO

Nach Art. 28 Abs. 3 lit. g DS-GVO hat der Verantwortliche vor Beginn einer Auftragsverarbeitung sich von hinreichenden Garantien des Auftragsverarbeiter zu überzeugen, ob dieser insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen die erforderlichen technischen und organisatorischen Maßnahmen implementiert hat und dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Zudem ist der Verantwortliche nicht alleiniger Adressat des Artikel 32 DS-GVO, sondern auch dem Auftragsverarbeiter obliegt selbst und unmittelbar die Pflicht die Sicherheit der personenbezogenen Daten nach Art. 32 Abs. 1 DS-GVO zu gewährleisten.

Risiken und Risikobewertung

Die Risiken bei der Auswahl eines Auftragsverarbeiters bestehen oft darin, dass der Verantwortliche seinen Fokus lediglich auf den Umfang und die Qualität der angebotenen Dienstleistung und die Kosten des potenziellen Dienstleisters richtet und nicht auch einen Blick auf datenschutzrechtliche Vorgaben und deren Umsetzung bei einem potenziellen Auftragsverarbeiter wirft. Datenschutzrechtliche Vorgaben sind

aufgrund einer allgemeinen Compliance-Verpflichtung, von möglichen Datenschutzschutzverletzungen und drohenden Bußgeldern, aber auch in Hinblick auf den Ruf des Unternehmens am Markt von enormer Bedeutung.

Ein Risiko kann auch darin bestehen, dass ein Dienstleiter keine eigenen Zertifikate oder Nachweise über seine Qualifikation besitzt und den Verarbeitungsauftrag nur mit Hilfe von Zertifikaten oder Dokumenten seiner Unterauftragnehmer belegt – und sich selbst damit in trügerischer Sicherheit wähnt. Dies ist leider in der Praxis nicht selten der Fall. Aus diesem Grund sind besonders die weiteren vorgelegten Nachweise des Auftragsverarbeiters maßgeblich und mit entsprechend erhöhter Gewichtung zu bewerten.

Äußerst relevant ist auch die Transparenz über konkrete Verarbeitungsphasen und beim Umfang einer Übertragung einer Verarbeitungstätigkeit auf den Auftragsverarbeiter und mögliche Unterauftragnehmer. Die technischen und organisatorischen Maßnahmen können bei dem Auftragsverarbeiter und bei Unterauftragnehmer unterschiedlicher Art sein, aber im Gesamtergebnis müssen diese die Sicherheit der Daten des Verantwortlichen gewährleisten, da dieser weiterhin die volle Verantwortung der gesamten Verarbeitungstätigkeit trägt.

Bei der erforderlichen Risikobewertung, ob die Garantien des potentzellen Auftragsverarbeiters ausreichend sind, sind auch die Umstände der Verarbeitungstätigkeit zu bewerten. Dies umfasst insbesondere den Sensibilitätsgrad der personenbezogenen Daten, deren Umfang und die Anzahl der betroffenen Personen. Bei der Sensibilität sind die besonderen Kategorien personenbezogener Daten aus Art. 9 DS-GVO und die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten aus Art. 10 DS-GVO zwingend zu berücksichtigen. Die Gefahr des Verlustes der Integrität, der Vertraulichkeit und der Verfügbarkeit zählen sicherlich zu den wichtigen Kriterien, wie hoch das Schutzniveau bei der Verarbeitungstätigkeit sein muss. Alle Kriterien erfordern daher eine intensiven Bewertung um die Risiken sachgerecht und nachvollziehbar entscheiden zu können.

Art und Weise einer Auswahl eines Auftragsverarbeiters

Äußerst wichtig ist zudem der Sitz des Auftragsverarbeiters. Ein Auftragsverarbeiter oder dessen Unterauftragnehmer, der außerhalb der EU oder des EWR seine Dienstleistung erbringt, birgt besonders hohe Risiken, beinhaltet erhöhte Anforderungen und bedarf daher einer intensiven Begutachtung und Abwägung, ob nicht vergleichbare Dienstleister in der EU vorhanden sind.

Ist es im Einzelfall notwendig, einen Dienstleister außerhalb der EU oder dem EWR mit einer Auftragsverarbeitung zu beauftragen, ist sicherzustellen, dass ausreichende Garantien für eine solche Übermittlung nach Kapitel 5 DS-GVO vorliegen und dass das durch die DS-GVO zu gewährleistende Schutzniveau für natürliche Personen nicht untergraben wird. Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 DS-GVO vorliegt, noch geeignete Garantien nach Artikel 46 DS-GVO, einschließlich verbindlicher interner Datenschutzvorschriften bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur noch in Ausnahmefällen und im Rahmen der Bedingungen nach Artikel 49 DS-GVO möglich.

Zu empfehlen ist, die vom Europäischen Datenschutzausschusses veröffentliche Sechs-Punkte-Checkliste[1] als Basisprüfung anzuwenden, da die Beteiligung von Dienstleistern aus Drittstaaten eine fortlaufende Überprüfung notwendig machen, um die Einhaltung der Rechtskonformität, der Datensicherheit und des Datenschutzes sicherzustellen.

Die vorgenannten Garantien sind jedenfalls vor Verarbeitungsbeginn des Auftragsverarbeiters dem Verantwortlichen zur Kenntnis zu bringen, falls ein Auftragsverarbeiter oder Unterauftragnehmer seinen Sitz außerhalb der EU oder dem EWR hat, damit der Verantwortliche unter anderem seiner Informationspflicht nach Art. 13 Abs. lit. f nachkommen kann.

Es sollte zudem vertraglich vereinbart werden, dass ein Wegfall von Garantien dem Verantwortlichen sofort mitzuteilen ist, so dass der Verantwortliche und der Auftragsverarbeiter die Möglichkeit erhalten, unverzüglich eine datenschutzkonforme Übermittlung auf einem anderen Weg herzustellen oder die Auftragsverarbeitungstätigkeit auszusetzen. Als letztes Mittel muss es möglich sein, die gesamte ausgelagerte Auftragsverarbeitung zu beenden.

Auch die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 können als Faktor herangezogen werden, um die Erfüllung der Anforderungen nachzuweisen. Derzeit erfolgt hauptsächlich eine Bewertung, ob die von dem Auftragsverarbeiter vorgeschlagenen Garantien ausreichend sind und zwar fast ausschließlich über die Bereitstellung einer Auflistung der technischen und organisatorischen Maßnahmen, einem Datenschutzkonzepts oder über Zertifikate aus dem Bereich IT-Sicherheit seitens eines Auftragsverarbeiters.

Natürlich kann auch der Ruf des Auftragsverarbeiters ein relevanter Faktor bei der Auswahl eines Auftragsverarbeiter sein. Dies sollte aber nicht überbewertet werden, da in der Praxis

[1] Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten; angenommen am 10. November 2020

der Ruf eines Dienstleisters sich grundsätzlich auf die angebotene Dienstleistung und dessen Qualität bezieht und nicht auf die vom Dienstleister implementierten und angewendeten Verfahren zur Datensicherheit und des Datenschutzes.

In den seltensten Fällen gelangen daher interne Datenschutzverletzungen oder Beeinträchtigung der IT-Infrastruktur eines Auftragsverarbeiters an die Öffentlichkeit. Um dies aber in die Bewertung zur Auswahl eines geeigneten Auftragsverarbeiter einfließen lassen zu können, sollte der Verantwortliche Informationen über in der Vergangenheit möglicherweise aufgetretenen Datenschutzvorfällen und Störungen der IT-Infrastruktur Auskunft beim potenziellen Auftragsverarbeiter anfordern.

Dies erfordert im zweiten Schritt, dass in dem Auftragsverarbeitungsvertrag eine Pflicht zu vereinbaren ist, dass der Auftragsverarbeiter den Verantwortlichen unverzüglich über technische Störungen, Verstöße gegen datenschutzrechtliche Bestimmungen oder den Verdacht auf Datenschutzverletzungen bei der Verarbeitung personenbezogener Daten, unverzüglich zu informieren hat. Gibt der Auftragsverarbeiter an, dass sich solche Vorfälle noch nicht ereigneten, kann dies als (Teil-) Nachweis zur Eignung des Auftragsverarbeiter dienen, weil die vorhandenen Schutzmaßnahmen offensichtlich und mit hoher Wahrscheinlichkeit wirksam sind.

Dokumentennachweise

Seit Inkrafttreten der DS-GVO haben sich verschiedene Lösungswege etabliert, wie der Auftragsverarbeiter den Nachweis von geeigneten Garantien vor Vertragsabschluss vorlegen kann. Diese kann er über Dokumenten wie (ISO-)Zertifikate, Testate, eigene Auditberichte, Datenschutzkonzepte oder einem Datenschutzhandbuch belegen.

Das Instituts der Wirtschaftsprüfer in Deutschland e. V (IDW) verweist in seinen Hinweisen für Wirtschaftsprüfer (IDW PH 9.860.1; „Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz"; S. 47) explizit darauf hin, dass der Verantwortliche Nachweise in Form vongeeigneten Garantien vorzulegen hat. Darin muss der Auftragsverarbeiter zusichern, dass Verfahren, Maßnahmen und Kontrollen den Anforderungen gemäß Artikel 28 Abs. 1 DS-GVO der DS-GVO entsprechen.

ISO Zertifikate

Auftragsverarbeiter legen derzeit üblicherweise ISO-Zertifikaten wie die ISO 27001 aus dem IT-Bereich oder die Qualitätsnorm ISO 9001:2015 vor, um einen Nachweis durch eine unabhängige und kompetente Prüfstelle zu erbringen, dass ausreichende und angemessene technische und organisatorische Maßnahmen vorliegen. Besonders ist daher im ersten Schritt auf den festgelegten Geltungs- und Anwendungsbereich eines Zertifikates zu achten.

Dieses sollte von einer akkreditierten Zertifizierungsgesellschaft ausgestellt sein, die wiederum bei der Deutschen Akkreditierungsstelle (DAkkS) – der nationale Akkreditierungsbehörde der Bundesrepublik Deutschland – akkreditiert ist. Damit ist klar, dass die Zertifizierungsgesellschaft nach den Anforderungen international gültiger Normen, gesetzlicher Grundlagen und relevanter Regeln ihre Bewertungsleistung erbringt. Erkennbar ist eine Akkreditierung an der Angabe der DAkkS-Registrierungsnummer auf der Zertifizierungsurkunde. Die Akkreditierungsurkunde der DAkkS dient den akkreditierten Konformitätsbewertungsstellen (KBS) als Hinweis auf ihre Akkreditierung durch die DAkkS und damit als formales Akkreditierungsdokument nach DIN EN ISO/IEC 17011. Im Zweifel sollte sich der Verantwortliche die Akkreditierungsurkunde der Zertifizierungsgesellschaft vorlegen lassen.

Die Registrierungsnummer einer Zertifizierungsgesellschaft und ihr Format.

D-XX-YYYYY-ZZ-NN.

XX: Akkreditierungsart

yyyyy: fortlaufende Kundennummer.
Sie ist die Identifikation der Rechtsperson.

ZZ: fortlaufende Nummer einer Akkreditierungsaktivität eines Kunden

NN: Identifizierung von Teil-Akkreditierungsurkunden: „00" steht für Akkreditierungen, die den gesamten Umfang umfassen

Bei der Vergabe öffentlicher Aufträge (Vergabeverordnung – VgV) wird die Einhaltung zutreffender Normen im Bereich der Qualitätssicherung durch entsprechende Belege einer akkreditierten Zertifizierungsgesellschaft gefordert (§ 49 VgV).

Nach einer Studie[2] der KPMG aus dem Jahr 2019 wird die hautsächlich angewendete internationale ISO 27001 bei 58 Prozent der zertifizierten teilnehmenden Unternehmen umgesetzt. Aber bei weniger als 50 Prozent der nach ISO 27001 zertifizierten Firmen bezieht sich der Anwendungsbereich nur auf Teilbereiche des Unternehmens. Daher muss sehr genau darauf geachtet werden, welcher Anwendungsbereich auf dem jeweiligen ISO-Zertifikat benannt ist und ob sich dieses tatsächlich auf die Auftragstätigkeit für den Verantwortlichen bezieht. Es wäre zudem fahrlässig, aufgrund eines Zertifikates davon auszugehen, dass dies ein ausreichender Nachweis wäre für die Einhaltung von technischen und organisatorischen Maßnahmen (TOMs) des Auftragsverarbeiters. So betrachtet eine Risikobewertung nach ISO 27001 ausschließlich die Risiken für das zertifizierte Unternehmen oder Teile davon und nicht das Risiko für betroffene Personen und deren Daten. Weiterhin enthält die DS-GVO Forderungen, welche über die Anforderungen der ISO 27001 hinausgehen oder gar nicht Bestandteil der ISO 27001 sind. Deshalb kann das IT-bezogene Zertifikat nur ein Teilbaustein für den Beleg einer effektiven Umsetzung von technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten angesehen werden.

Das alleinige Vorliegen von Zertifikaten entbindet den Verantwortlichen keinesfalls von seinen fortlaufenden Kontroll-, Überwachungs-, und Auswahlpflichten und deren dokumentierten Umsetzung (Rechenschaftspflicht).

Eigene Berichte: Interne Audits des Auftragsverarbeiters

Eine dokumentierte Selbstevaluierung des Auftragsverarbeiters ist nur dann aussagekräftig, wenn die Prüfkriterien, die Prüfsystematik und die Prüfmethoden mit den detaillierten Ergebnisse dem Verantwortlichen offengelegt werden und dieser sich so über die Wirksamkeit der Maßnahmen überzeugen kann. Dazu gehört auch die Eignung und das Fachwissen des mit der Evaluierung beauftragten Prüfers. Der Verantwortliche kann selbst aber auch einen unabhängigen Prüfer beauftragen, um sicher zu gehen, dass die Ergebnisse des internen Audits stimmen. Aufgrund Art. 32 Abs. 1 lit. d DS-GVO hat der Verantwortliche jedenfalls bei Zweifeln an der Aussagekraft eines Evaluierungsberichtes die Möglichkeit, sich selbst von dem Verfahren zur Bewertung und Evaluierung zu überzeugen. Dafür steht ausdrücklich ein Vor-Ort-Audit dem Verantwortlichen zur Verfügung.

Eine fortlaufende Verpflichtung

Der Einsatz von geeigneten Auftragsverarbeitern ist eine ständige Verpflichtung des Verantwortlichen.[3] Daher obliegt es ihm, sich in angemessen Abständen von der Arbeit des Auftragsverarbeiter zu überzeugen. Denn eine Überprüfungspflicht besteht bis zum Ende der Verarbeitungstätigkeit. Das ist auch dadurch begründet, dass sich die Risiken für Betroffene etwa durch die Weiterentwicklung der Digitalisierung und eine neue Bedrohungslage verändern können.

Dies erfordert im Regelfall mindestens eine Anpassung, oft aber eine Erweiterung von Sicherheitsmaßnahmen, um das notwendige Schutzniveau zu halten. Diesen Umstand hat der europäische Gesetzgeber mit Art. 32 Abs. 1 lit. d DS-GVO Rechnung getragen und normiert eine Verpflichtung zur Anwendung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen.

Unter Evaluierung ist eine fachliche und faktenbezogene Bewertung von Prozessen und deren Ergebnissen zu verstehen. Ziel dieser Bewertung ist es, die Wirkung von Maßnahmen und Prozessen entsprechend steuern zu können. Um eine transparente und nachvollziehbare Evaluierung zu belegen, sollte der Auftragsverarbeiter einen detaillierten Evaluierungsbericht erstellen. Dieser sollte die Methoden der Erhebungen, der Aufbereitung, der Datenauswertung und die erfolgten oder geplanten Maßnahmen darlegen.

[2] Cloud-Monitor 2020, Studie von Bitkom Research GmbH im Auftrag von KPMG

[3] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0, 07 July 2021, Rn. 99

Falls die Evaluierung Änderungen beispielsweise bei Verarbeitungsprozessen oder Abweichungen von Datenschutzkonzepten feststellt, muss der Auftragsverarbeiter offenlegen, welche Gründe dafür verantwortlich waren. Zudem muss er dem Verantwortlichen Vorschläge unterbreiten, welche Maßnahmen geeignet sind, ein angemessenes Schutzniveaus wieder herzustellen. Damit liefert er dem Verantwortlichen die Grundlage für eine Entscheidung.

Zudem sollten organisatorische Änderungen beim Auftragsverarbeiter, aber auch aktuelle datenschutzrechtliche Änderungen wie Empfehlungen bzw. Vorgaben z. B. von Datenschutz-Aufsichtsbehörden oder einschlägige Urteile des EuGH bei einer Überprüfung durch den Verantwortlichen oder eines durch diesen beauftragten Dritten berücksichtigt werden. Diesbezüglich sollte der AV-Vertrag eine Klausel beinhalten, welche eine Verpflichtung zur Aktualisierung des Vertrages bei datenschutzrelevanten Änderungen vorsieht.

Eine nur oberflächliche oder lediglich teilweise durchgeführte Überprüfung kann den Wert der Schutzmaßnahmen nicht erfassen, und ein trügerisches Gefühl von Sicherheit vermitteln. Je sensibler die Daten, umso intensiver und häufiger sollte kontrolliert werden.

Häufigkeit einer Überprüfung

Im Regelfall sollte alle ein bis drei Jahre[4] – je nach Umfang, Sensibilität der Daten und Laufzeit des Vertrages, eine Überprüfung des Auftragsverarbeiters durch den Verantwortlichen stattfinden. In einigen Fällen kann es jedoch erforderlich sein, die Auftragsverarbeiter jährlich zu kontrollieren. Nachfolgende Faktoren der dänischen Datenschutzaufsichtsbehörde[5] geben Hinweise, welche Prüffrequenz geboten ist.

Beispiele für Faktoren, die auf die Notwendigkeit einer häufigen Überprüfung hinweisen:

- Der Auftragsverarbeiter hatte in der Vergangenheit Schwierigkeiten mit der Einhaltung von Vereinbarungen (nicht nur der Datenverarbeitungsvereinbarung).
- Der Auftragsverarbeiter hat mehrere schwerwiegende Sicherheitsverletzungen erlitten, darunter Verletzungen des Schutzes personenbezogener Daten. Dies setzt natürlich voraus, dass der Verantwortliche von solchen Verstößen überhaupt Kenntnis erlangt. Bei Verstößen gegen den Schutz personenbezogener Daten ist es gesetzlich vorgeschrieben, dass der Auftragsverarbeiter unverzüglich über derartige Verstöße informiert.
- Unterauftragsverarbeiter werden häufig ausgetauscht.
- Bei Übernahmen, Eigentümerwechseln, Fusionen oder wesentlichen Änderungen in der Geschäftsstrategie des Auftragsverarbeiters.

Beispiele für Faktoren, die auf die Notwendigkeit einer Überprüfung außerhalb der üblichen Häufigkeit hinweisen:

- Wechsel des Eigentümers, Fusionen oder radikale Änderungen in der Strategie des Anbieters.
- Äußere Umstände wie die Corona-Pandemie verändern die Art und Weise, wie die Arbeit ausgeführt wird, einschließlich des Zugriffs auf personenbezogene Daten.

Beispiele für Faktoren, die auf die Notwendigkeit einer geringeren Häufigkeit von Audits hinweisen:

- Langjährige Erfahrung mit den Auftragsverarbeitern und möglichen Unterauftragsverarbeitern, die einen stabilen Dienst und keine schwerwiegenden Sicherheitsverstöße erkennen lassen.

Audits durch den Verantwortlichen beim Auftragverarbeiter

Eine Mitwirkungspflicht besteht für den Auftragsverarbeiter nach Art. 28 Abs 3 lit. h der EU-Datenschutz-Grundverordnung 2016/679. Nach dem Wortlaut der DS-GVO hat der Auftragsverarbeiter nicht nur Überprüfungen zu ermöglichen (Duldungspflicht), sondern auch zu Inspektionen (Audits) beizutragen.

Bei der Ausgestaltung des AV-Vertrages sollten die Parteien auf ausgewogene, datenschutzrechtlich zulässige und zivilrechtskonforme Regelungen achten. Eine Vereinbarung zu Vor-Ort-Audits birgt oft ein Konfliktpotenzial und mündet nicht selten in einer unwirksamen oder nicht angemessenen Regelung durch Ein- oder Beschränkung von Auditrechten, insbesondere dann, wenn ein Auftragsverarbeiter aufgrund seiner (vermeintlichen) Machtposition (eines großen Dienstleisters) dem vermeintlichen kleineren Vertragspartner einen nicht verhandelbaren und vorformulierten Standardvertrag anbietet. Diese Problematik ist dem europäischen Gesetzgeber bewusst und daher weist er in der Leitlinie 2/2020[6] ausdrücklich auf die Pflicht des Verantwortlichen hin, bei Standardverträgen die Vertragsklauseln zu prüfen. So sieht dies auch die Aufsichtsbehörde von Baden-Württemberg: Sollte sich ein Auftragsverarbeiter weigern, den Vertrag rechtskonform anzupassen, sollte er als Vertragspartner ausscheiden.[7] Auch die DSK (Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder)

[4] BayLDA, Auftragsdatenverarbeitung nach § 11 BDSG alt; Gesetzestext mit Erläuterungen, Stand Januar 2014, Seite 8.

[5] Datatilysnet; Guidance on the use of cloud; March 2022 und die Leitlinien zur Überwachung von Auftragsverarbeitern aus Oktober 2021 (dänisch)

[6] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0, 07 July 2021, Rn. 110

[7] Der Landesbeauftragte für Datenschutz und Informationstechnik Baden-Württemberg; Handreichung Videokonferenzsysteme – Hinweise zur praktischen Nutzung aus Dezember 2021; S. 6

weist in ihrer Orientierungshilfe[8] darauf hin, dass bei Musterverträgen besonders darauf geachtet werden sollte, dass dem Verantwortlichen hinreichende Kontrollbefugnisse eingeräumt werden.

Die nach Art. 28 Abs. 3 UAbs. 1 S. 2 lit. h DS-GVO zwingend erforderliche Verpflichtung zur Ermöglichung der Kontrollen und zum aktiven Beitragen zu Kontrollen sollte zudem in vertraglichen Regelungen nicht nur auf bestimmte Handlungen beschränkt sein. Bedauerlicherweise finden sich beschränkende Formulierungen oft in den Standardverträgen wieder.

Anlasslose Vorort-Audits

Was unter der Begrifflichkeit „anlassloses Audit" verstanden wird, welches häufig in der Praxis in Zusammenhang mit Kontrollen oder Inspektion Vor-Ort verwendet wird, bedarf einer näheren Betrachtung.

Unter anlasslosen Audits sind solche Audits zu verstehen, welche über das übliche, das heißt vereinbarte und erforderliche Maß hinausgehen und nicht anlassbezogen sind. Anlasslose Audits sollten mit ausreichender Vorankündigungsfrist und nach Absprache mit dem Auftragsverarbeiter erfolgen.

In der Regel kommen anlasslose Vor-Audits allerdings eher bei Kontrollen von Datenschutzaufsichtsbehörden in Form von Prüfungen bei bestimmten, oft aktuellen Schwerpunkten des Datenschutzes vor und sind bei Wirtschaftsunternehmen eher selten, weil in der Regel kein Unternehmen Interesse daran hat, entsprechend notwendige Ressourcen für ein anlassloses Audit unnötig zu verschwenden. Da Aufsichtsbehörden andere Ziele und Vorgaben haben, sind anlasslose Prüfungen dort sicherlich sinnvoll und angemessen.

Anlassbezogene Vorort-Audits

Eine Vor-Ort-Überprüfung kann bei konkreten Anlässen wie einem Erstaudit, bei Anhaltspunkten für ein Fehlverhalten des Dienstleisters, bei Datenschutzvorfällen oder bei Beschwerden von Betroffen geboten sein.[9] Daher sollte ein solches Audit ohne langfristige Vorankündigung vertraglich nicht ausgeschlossen werden.

Kosten bei Vorort-Audits

Die DS-GVO regelt nicht, wer bei einem Vorort-Audit die dafür entstehenden Kosten trägt. Es steht den Vertragsparteien frei, eine zivilrechtliche Kostenregelung über mögliche Leistungen zu treffen. So könnte vertraglich geregelt sein, dass die Kosten bei einer anlassbezogenen Überprüfung ausschließlich zu Lasten des Auftragsverarbeiters gehen, wenn etwa erst ein Fehlverhalten des Auftragsverarbeiters oder der Verlust ausreichender Garantien das Audit notwendig werden lassen. Der Verantwortliche sollte in solchen Fällen von der Kostentragungspflicht ausgeschlossen sein, da sonst das Überprüfungsrecht faktisch entwertet würde.[10]

Soweit ein Auftragsverarbeiter Sorge hat, dass er durch Maßnahmen des Verantwortlichen nach Art. 28 Abs. 3 Satz 2 Buchst. h DS-GVO Belastungen ausgesetzt wird, welche den vertraglichen Leistungsaustausch aus dem Gleichgewicht bringen, kann er den erwartbaren Mehraufwand bei der Berechnung der vom Verantwortlichen geforderten Hauptleistung pauschal berücksichtigen.[11] Dieser Regelung kann insoweit zustimmt werden, falls die Ursache des Audits nicht beim Auftragsverarbeiter liegt. Wenn aufgrund von relevanten Änderungen von technischen und organisatorischen Maßnahmen, Verfahren oder Prozessen, welche einen Einfluss auf die Sicherheit der personenbezogenen Daten des Verantwortlichen (Auftraggebers) haben oder haben könnten, Vor-Ort-Audits erfolgen müssen, sollten die Ursachen dafür im Einzelfall betrachtet werden. Hierzu muss jedenfalls festgestellt werden, ob die Änderungen auf Wunsch oder Aufforderung des Verantwortlichen oder des Auftragsverarbeiters erfolgen.

Bei Änderungen, welche aufgrund gesetzlicher, gerichtlicher oder behördlicher Vorgaben notwendig werden, bietet sich eine Übernahme ausschließlich der eigenen Kosten für die beteiligten Parteien an. Diese Regelung dürfte angemessen sein und zu keiner Benachteiligung einer der Vertragsparteien führen.

Auch bei einem Erstaudit, welches zum Nachweis der Eignung als Auftragsverarbeiter dient, sollte eine gleichmäßige Verteilung der Kosten angestrebt werden (jede Partei trägt dabei die Kosten des eigenen Aufwands), da beide Parteien aus diesem Audit gleichermaßen Nutzen ziehen.

[8] Orientierungshilfe Videokonferenzsysteme Stand 23.10.2020 der Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder; S. 8; 3.2

[9] Vgl. dazu Orientierungshilfe Auftragsverarbeitung, Der Bayerische Landesbeauftragte für den Datenschutz, Version 2.0, 1. April 2019, S. 20

[10] Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten, Berliner Datenschutzbehörde, Version 1.0 vom 3. Juli 2020

[11] Aktuelle Kurz-Information 6; Der Bayerische Landesbeauftragte für den Datenschutz; Stand 15.11.2021

Kosten für einen dokumentierten Nachweis zur Eignung als Auftragsverarbeiters

Die Nachweise, zu denen Auftragsverarbeiter wie oben beschrieben verpflichtet sind, müssen unabhängig von einem Auftragsverarbeitungsvertrag nach Art. 32 DS-GVO vorliegen. Es ist Praxis,[12] dass der Auftragsverarbeiter die Nachweise schon aufgrund seiner eigenen Rechenschaftspflicht erstellt und diese für etwaige Nachfragen von Verantwortlichen oder Aufsichtsbehörden vorhält. Dies ist zulässig, zweckmäßig und nachvollziehbar, bedeutet aber auch, dass dieser Nachweis nicht ausschließlich für einen einzigen Auftragsverarbeiter erstellt wurde, sondern – insbesondere bei Cloud-Diensten – für eine große Zahl von Auftraggebern dient. Daher erscheint eine Vergütungspflicht des Verantwortlichen bei der Zurverfügungstellung von – im Regelfall bereits schon vorhandenen – Nachweisen und Auskünften als nicht gerechtfertigt.

Über den Autor

Harald Trettow
ist interner und externer Datenschutzbeauftragter.
Er ist außerdem langjähriges Mitglied im BvD und in der GDD.

[12] außer der unwahrscheinliche Umstand liegt vor, dass Auftraggeber erster und einziger Kunde ist

FAZIT

Der Verantwortliche hat sich vor Verarbeitungsbeginn insbesondere über die vom Auftragsverarbeiter zur Verfügung gestellten Dokumenten wie ISO-Zertifikate einer akkreditierten Zertifizierungsgesellschaft, Liste von TOM und Datenschutzkonzepte davon zu überzeugen, dass diese Nachweise tatsächlich in Bezug auf die Verarbeitungstätigkeit für den Verantwortlichen stehen und aussagekräftigt genug sind, um als geeignete und angemessene Garantien eingestuft werden zu können. Bei entsprechenden Zertifikaten einer akkreditierten Zertifizierungsgesellschaft sind zwingend der Anwendungs- und Geltungsbereich zu beachten. Zur Umsetzung der Anforderung aus Artikel 32 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 müssen regelmäßig Prüfungen durch den Verantwortlichen durchgeführt werden, was bedeutet, dass diese Maßnahmen in bestimmten Abständen bewusst geplant und organisiert sowie dokumentiert werden müssen, um die Eignung, Angemessenheit und Wirksamkeit der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters und eine sorgfältige Auswahl durch den Verantwortlichen dauerhaft sicherzustellen und – in Verbindung mit dem Grundsatz der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 der Verordnung (EU) 2016/679 – dies nachweisen zu können.

STEPHAN REHFELD

„TRUSTED DATA PROCESSOR“ (TDP) – REGELUNGSINHALTE UND VORTEILE DER VERWENDUNG

In Artikel 40 DSGVO werden Verhaltensregeln (Code of Conduct, CoC) gesetzlich geregelt. In Erwägungsgrund 98 DSGVO beschreibt der Gesetzgeber

„Verbände oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, sollten ermutigt werden, in den Grenzen dieser Verordnung Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung dieser Verordnung zu erleichtern, wobei den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen ist. […]“.

Verhaltensregeln sind Konkretisierungen der DSGVO und müssen für mehrere Unternehmen anwendbar sein. Die Konkretisierung der DSGVO erfolgt durch den Ersteller der Verhaltensregel. Pflichtinhalte sind ein Verfahren zur Überwachung der Einhaltung der Anforderungen aus der Verhaltensregel und die Beschreibung der Arbeitsweise der Überwachungsstelle.

Regelungsinhalte

Die Verhaltensregel „Trusted Data Processor“[1] konkretisiert die gesetzlichen Anforderungen an die Auftragsverarbeitung und wendet sich an Auftragnehmer. Deutsche Auftragnehmer können sich der Verhaltensregel freiwillig unterwerfen.[2] Dabei ist es möglich, dass ausländische Subauftragnehmer in einer Auftragsverarbeitung beauftragt sind/werden.

Das Siegel für die Zertifizierung zum “Trusted Data Processor”.
Das Wasserzeichen “Muster” soll Missbrauch vermeiden.

Im Rahmen der Verhaltensregel „Trusted Data Processor“ werden die folgenden Aspekte der Auftragverarbeitung konkretisiert:

- Angebotsprozess und Pflichtinformationen durch den Auftraggeber und Anforderungen an den Vertrag zur Auftragsverarbeitung. Bewusst wird kein Vertragsmuster zur Verwendung vorgeschrieben.
- Anforderungen an eine Unterbeauftragung
- Kontrolle von Unterauftragnehmern

[1] Ist abrufbar unter https://www.verhaltensregel.eu/verhaltensregel/

[2] Das konkrete Verfahren ist unter https://www.verhaltensregel.eu/produktbeschreibung/ beschrieben.

- Prozess zum Umgang mit Betroffenenrechten
- Meldung Sicherheitsvorfälle
- Inhalt der Verpflichtung auf Vertraulichkeit mit einem Muster zur Verpflichtung
- Eigenkontrolle des Auftragnehmers (interne Audits)
- Überwachung durch die Kontrollstelle

Keine Aussage wird von der Verhaltensregel „Trusted Data Processor“

- zu den technischen und organisatorischen Maßnahmen,
- zur Mitwirkung an der Erstellung von Datenschutz-Folgenabschätzungen,
- zur Verhinderung einer Datenverarbeitung zu eigenen Zwecken des Auftragnehmers,
- zur Löschung bei Auftragsbeendigung und zur Genehmigung neuer Auftragsverarbeiter

getroffen.

Vorteile für Datenschutzbeauftragte

DSB können die Verhaltensregel als Best-Practice einsetzen, ohne dass sich die betreute Organisation der Verhaltensregel unterwerfen muss. Auch können Vertragsparteien die Verhaltensregel als Muster für die Schnittstellen- und Prozessdefinition verwenden, ohne dies im Vertrag zur Auftragsverarbeitung beschreiben zu müssen. Weiterhin können DSBs die Verhaltensregel als Base-Line verwenden, um sich gegen überschießende Forderungen von Auftragnehmern zu „wehren“.

Wenn eine Organisation beschließt, sich der Verhaltensregel zu unterwerfen, kann der DSB seine Organisation selbst zur Einführung und Umsetzung der Anforderungen beraten. Da eine Verhaltensregel eine Konkretisierung der DSGVO darstellt, ist keine weitere Qualifikation des DSB erforderlich.

Vorteile für Verantwortliche

Verantwortliche profitieren von der rechtssicheren Gestaltung der erforderlichen Geschäftsprozesse zur Auftragsverwaltung, einer einheitlichen Schnittstellendefinition zu den Auftragsverarbeitern und einem Audit-Konzept für Auftragsverarbeiter. Die datenschutzrechtlichen Anforderungen an Auftragnehmer können vom Auftraggeber durch eine Referenz auf die Verhaltensregel im Vertrag zur Auftragsverarbeitung beschrieben werden.

Bei Verstößen gegen die Regelungen der Verhaltensregel können sich Auftraggeber an die Überwachungsstelle wenden, die dann nach klar definierten Regeln eingreifen wird und auch muss. Im Fall eines Datenschutzverstoßes im Rahmen der Auftragsverarbeitung, kann der Bezug auf die Verhaltensregel sich mindernd auf eine Bußgeldbemessung auswirken.

Vorteile für Auftragsverarbeiter

Durch ein grafisches Symbol können Auftragsverarbeiter ihre Investition in die Erfüllung der Anforderungen und der Selbstverpflichtung auf die Verhaltensregel gegenüber potentiellen Auftraggebern sichtbar machen. Zusätzlich wird von der Überwachungsstelle ein Register der Organisationen geführt, die sich der Selbstverpflichtung unterworfen haben.

Die Selbstverpflichtung auf die Verhaltensregel ist kostengünstiger als eine Datenschutz-Zertifizierung und führt zu einem erleichterten Vertragsabschluss mit Auftraggebern.

Bei Interesse an einer Selbstverpflichtung auf die Verhaltensregel „Trusted Data Processor“ wenden Sie sich bitte an die DSZ Datenschutz Zertifizierungsgesellschaft mbH,

▶ www.verhaltensregel.eu

Auf der Seite der DSZ kann die Verhaltensregel heruntergeladen werden und auch erforderliche Dokumente zur Teilnahme an der Verhaltensregel.

Über den Autor

Dipl.-Ök. Stephan Rehfeld
ist externer Datenschutzbeauftragter der scope & focus GmbH Hannover und akkreditierter Datenschutzauditor der DQS GmbH. Als stimmberechtigtes Mitglied des AK05 des NIA27 des DIN arbeitet er aktiv an der Erstellung und Überarbeitung von Datenschutz-ISO- und -DIN-Normen mit. Ferner ist er im Leitungskreis des GDD-Erfa-Kreises Hannover engagiert, im AK Datenschutz der Bitkom und in der Fachgruppe Datenschutz von Niedersachsen. Digital e.V. Stephan Rehfeld ist außerdem BvD-Vorstandsmitglied und Mitglied im Ausschuss Prüfaufgaben Datenschutzbeauftragter des BvD.

"WIR SEHEN NACH WIE VOR EINEN GROSSEN BERATUNGSBEDARF."

Meike Kamp ist seit Oktober 2022 neue Berliner Beauftragte für Datenschutz und Informationsfreiheit. Über ihre vordringlichsten Aufgaben, das Berliner Transparenzgesetz und die Rolle der Datenschutzbeauftragten vor dem Hintergrund der neuen EU-Rechtsakte aus Brüssel sprach die BvD-News mit Meike Kamp.

BvD-News: *Sehr geehrte Frau Kamp, zunächst herzlichen Glückwunsch zur Ernennung als Berliner Beauftragte für Datenschutz und Informationsfreiheit. Im Datenschutz sind Sie ja schon viele Jahre tätig, zunächst in Schleswig-Holstein, danach in Berlin. Was hat Sie motiviert, sich dem Thema Datenschutz anzunehmen?*

Meike Kamp: Die Themen Freiheit, Autonomie und Selbstbestimmung interessieren mich schon seit langem. Und um diese geht es beim Grundrecht auf Datenschutz. Wenn ich bestimmen kann, was andere über mich wissen oder welche Informationen über mich verarbeitet werden, schafft mir das Freiräume. Die Datenschutzbehörden helfen also auch, den Rechtsstaat und die Demokratie zu schützen – das ist eine große Motivation für mich.

BvD-News: *Welche Themen-Schwerpunkte haben Sie sich für Ihre Amtszeit und für Ihre Behörde für den Datenschutz vorgenommen?*

Meike Kamp: Es gibt eine ganze Reihe wichtiger Themen, mit denen sich die Behörde bereits heute beschäftigt. Dazu gehören beispielsweise die Digitalisierung in Schulen oder die Verarbeitung von Gesundheitsdaten in Krankenhäusern und durch digitale Anwendungen. Ein zentrales Thema der nächsten Jahre wird auch die Digitalisierung der Verwaltung sein, insbesondere im Rahmen der Umsetzung des Onlinezugangsgesetzes. Wir werden außerdem die polizeiliche Datenverarbeitung im Auge behalten, insbesondere im Hinblick auf Löschmechanismen und den Datenaustausch auf europäischer Ebene. Ein weiteres Thema ist Tracking im Internet, durch das notwendige Freiräume zur selbstbestimmten Informationsbeschaffung stark eingeschränkt werden.

Bei all diesen Themen möchte ich die laufende Arbeit fortsetzen, verbessern und noch sichtbarer werden. Mein Ziel ist es, besonders in der Verwaltung frühzeitig beratend in laufende Prozesse einzugreifen und so zu verhindern, dass rote Linien überschritten werden. Andernfalls müssen wir sanktionierend eingreifen. Dazu gehört dann auch, offene Rechtsfragen gerichtlich klären zu lassen oder auf europäischer Ebene zu lösen. Das will ich angehen.

BvD-News: *Sie treten Ihr Amt in turbulenten Zeiten an: Mitte Dezember hat die SPD die Aussprache zum Gesetzentwurf für ein Berliner Transparenzgesetz von der Tagesordnung des Digitalisierungsausschusses genommen. Was bedeutet das für die Informationsfreiheitsrechte in Berlin?*

Meike Kamp: Die erneute Verzögerung des Transparenzgesetzes ist sehr ärgerlich. Bisher sieht das Berliner Informationsfreiheitsgesetz vor, dass die Verwaltung Informationen auf Anfrage der Bürger:innen bereitstellt. Mit dem seit Jahren geplanten Transparenzgesetz sollte diese Regelung endlich an das

21. Jahrhundert angepasst werden. Bürger:innen erwarten heute verständlicherweise, dass die Verwaltung vorhandene Informationen und Daten von sich aus veröffentlicht. Das hat nicht zuletzt der Volksentscheid Transparenz in Berlin gezeigt. Gerade jetzt, in Zeiten der Krisen, halte ich es für besonders wichtig, das Handeln von Politik und Verwaltung transparent zu erklären. Und da gehören proaktive Veröffentlichungspflichten des Staates einfach dazu. Wir halten dieses Gesetz daher auch aus demokratischen Gesichtspunkten für sehr wichtig und werden weiter darauf drängen.

BvD-News: *Ihre Behörde hatte im September ein Bußgeld über 525.000 Euro wegen Interessenkollision eines betrieblichen Datenschutzbeauftragten gegen ein Unternehmen verhängt. Nehmen Sie die Stellung von Datenschutzbeauftragten und deren Aufgaben besonders in den Fokus?*

Meike Kamp: Den betrieblichen Datenschutzbeauftragten kommt eine wichtige Funktion zu. Ich würde mir wünschen, dass ihre Rolle und das Thema Datenschutz allgemein in Betrieben nicht mehr so negativ besetzt wird, sondern als Chance wahrgenommen wird, Dinge zu gestalten und Vertrauen zu verbessern. Dazu ist es zwingend notwendig, die Datenschutzbeauftragten zu befähigen, ihre Aufgaben auch wahrzunehmen. Interessenkonflikte sind hier sehr schädlich und schaden sowohl dem Vertrauen als auch der Funktion. Daher können sie zu empfindlichen Bußgeldern führen, wie der genannte Fall aus meiner Behörde zeigt. Im Jahr 2021 haben wir in einem ähnlichen Fall ebenfalls ein Bußgeld gegen eine Fachklinik verhängt, deren Inhaber und Klinikleiter gleichzeitig betrieblicher Datenschutzbeauftragter war. Die europäischen Aufsichtsbehörden haben sich kürzlich darauf verständigt, im Rahmen der zweiten koordinierten Durchsetzungsmaßnahme die unabhängige Stellung der Datenschutzbeauftragten in den Blick zu nehmen. Wir raten daher dringend, betriebliche Datenschutzbeauftragte konzernweit auf Interessenkonflikte zu überprüfen und Verstöße zu beseitigen oder gleich zu verhindern.

BvD-News: *Welchen Stellenwert nimmt die Beratung von Unternehmen und von Datenschutzbeauftragten für Sie ein?*

Meike Kamp: Wir sehen nach wie vor einen großen Beratungsbedarf bei den datenverarbeitenden Stellen und den Datenschutzbeauftragten. Angesichts der bekanntermaßen knappen Ressourcen der Aufsichtsbehörden müssen wir bei der Beratung jedoch Prioritäten setzen. Beratung findet primär im öffentlichen Bereich statt. Um den Unternehmen gebündelt Hilfen an die Hand zu geben, erarbeiten wir im Rahmen der Datenschutzkonferenz und des Europäischen Datenschutzausschusses zu häufig nachgefragten Themen Orientierungshilfen. Zuletzt haben wir beispielsweise eine Checkliste für Auftragsverarbeitungsverträge herausgegeben, zu der wir viele positive Rückmeldungen von Verantwortlichen erhalten haben. Speziell für kleine und mittlere Unternehmen haben wir die Start-up-Schule in Berlin initiiert, da wir in der schnell wachsenden Gründerszene einen großen Bedarf an Weiterbildung und Sensibilisierung für den Datenschutz sehen. Hier unterstützen wir praxisnah mit Online-Schulungen, um einen sicheren Umgang mit dem Datenschutzrecht zu ermöglichen.

BvD-News: *Wo sehen Sie die größten Herausforderungen für die Datenschutzbeauftragten in der Zukunft, vor allem im Hinblick auf die Gesetzgebung zur Digitalisierung in der EU?*

Meike Kamp: Mit der KI-Verordnung, dem Data Act und weiteren Rechtsakten kommen eine Reihe von europäischen Regelungen auf die Unternehmen zu, die regulatorische Auswirkungen auf die Verarbeitung von personenbezogenen Daten haben werden. Diese zu berücksichtigen und miteinander in Einklang zu bringen, wird eine große Herausforderung für Datenschutzbeauftragte und Aufsichtsbehörden gleichermaßen sein. Zudem bringen einige dieser Rechtsakte auch neue europäische Aufsichtsstrukturen hervor, die es miteinander zu vereinbaren gilt. Aus Sicht der Datenschutzbehörden ist es wichtig, dass diese neuen Rechtsakte die Regelungen aus der DSGVO nicht einschränken. Zum Beispiel wird es künftig noch stärker um die Frage der Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten gehen. Hier werden die Datenschutzbeauftragten gefragt sein, auf die Einhaltung angemessener datenschutzrechtlicher Garantien zu achten.

BvD-News: *Die Ausstattung der Datenschutz-Aufsichtsbehörden ist immer wieder ein Thema – in allen Bundesländern. Welche Ausstattung wollen Sie für Ihre eigene Behörde erreichen?*

Meike Kamp: In den letzten zwei Jahren hat sich die personelle Ausstattung meiner Behörde deutlich verbessert. Verbesserungsbedarf sehe ich im Bereich der Bildungs-, Beratungs- und Projektarbeit. Dafür werde ich mich gegenüber der Berliner Politik einsetzen.

MEIKE KAMP

Die Juristin ist im Oktober 2022 zur neuen Berliner Beauftragten für Datenschutz und Informationsfreiheit gewählt worden. Bereits zwischen 2010 und 2019 war die Expertin für Datenschutz, Medien- und Informationsfreiheit in der Behörde tätig. Außerdem vertrat sie die Bundesländer in Datenschutz-Gremien auf europäischer Ebene. Vor ihrer Wahl arbeitete Kamp für die Landesvertretung von Bremen in Berlin.

Das Interview führte

Christina Denz

ist Journalistin, Kommunikationsberaterin und Redakteurin der „BvD-News“.

MICHAEL RATH, DENNIS GÖBEL

UMGANG VON ANWENDER-UNTERNEHMEN MIT DEM DATENSCHUTZ

Sicher zur nächsten IT-Innovation:
Bewusstsein für datenschutzrechtliche Vorgaben schärfen

I. Innovationsbremse Datenschutz

Die Bitkom stellt in einer aktuellen Studie erneut fest, dass betroffene Unternehmer datenschutzrechtliche Vorgaben bestenfalls als Belastung empfinden.

Rund 98 Prozent der Befragten verwarfen danach im vergangenen Jahr mindestens ein Innovationsprojekt wegen angeblich zu hoher datenschutzrechtlicher Anforderungen, davon 93 Prozent angesichts fortbestehender Unklarheiten zu Vorgaben der Datenschutz-Grundverordnung (DSGVO). Insbesondere IT-Anwender belasten diese Unklarheiten in besonderem Maß. Dies spiegelt sich in den zentralen datenschutzrechtlichen Konflikten wider. So bereiten nach der obigen Bitkom Studie der Aufbau von Datenpools, der Einsatz von Datenanalysetools und Cloud-Diensten sowie die Verwendung von Software und künstlicher Intelligenz im Datenschutz die häufigsten Probleme.

In den vergangenen zwei Jahren fanden sich dazu in den Medien insbesondere die Diskussion um Videokonferenzsysteme beim Homeschooling und die Risiken durch die Corona-Warn-App als vorherrschende Beispiele einer gehemmten Innovation. Passend dazu äußerte sich Bitkom Hauptgeschäftsführer **Dr. Bernhard Rohleder**:

> „Datenschutz darf nicht regelmäßig dazu führen, dass Dinge nicht gemacht werden, Datenschutz muss vielmehr unterstützen, dass sie richtig gemacht werden, und letztlich den Menschen dienen.“[1]

Einige Äußerungen der zuständigen Datenschutzaufsichtsbehörden haben dieses Spannungsverhältnis zwischen Innovation und Datenschutzkonformität noch beschleunigt, indem sie die Vorsicht der Unternehmen bestärkten. In diese Richtung gehen auch Äußerungen von Bitkom-Präsident **Achim Berg:**

> „Die permanenten Warnungen einiger Datenschutzbeauftragter und Politiker vor den rein theoretischen Gefahren zum Beispiel beim Einsatz leistungsfähiger Videokonferenzsysteme im schulischen Unterricht tun ein Übriges, um die Menschen in Deutschland zu verunsichern und den freiwilligen Einsatz digitaler Technologien zusätzlich zu begrenzen.“[2]

Tatsächlich kann bedingt durch diese Wahrnehmung der Eindruck entstehen, dass der Datenschutz eine Innovationsbremse ist. Doch diese Wahrnehmung hindert Unternehmen nur daran, dass sie die eigenen Innovationspotenziale umfänglich ausschöpfen. Funktionierender Datenschutz und ein etabliertes umfängliches Datenschutzmanagement bedeuten die Möglichkeit, angedachte Innovationspotenziale dauerhaft umzusetzen und das eigene Geschäftsmodell positiv von Geschäftsmodellen anderer Wettbewerber abzugrenzen.

So lassen sich neue Vorgaben auch als neue Qualitätsmerkmale der eigenen Produkte verorten. Diese Möglichkeit zur positiven Abgrenzung folgt auch aus dem wachsenden Bewusstsein der Menschen für die eigenen Daten und einer steigenden Bedeutung der eigenen Datensouveränität. So werden sich in der Zukunft die IT-Innovationen durchsetzen, die die Datensouveränität der Menschen durch Einhaltung der Datenschutzvorgaben beachten. Richtig ist daher, dass IT-Innovation nicht trotz, sondern gerade wegen und mit Einhaltung der DSGVO funktionieren kann.

[1] Dr. Bernhard Rohleder, 2022, https://www.bitkom.org/Presse/Presseinformation/Datenschutz-deutsche-Wirtschaft-2022-DS-GVO-wenig-Wettbewerbsvorteile

[2] Achim Berg, 2022: https://www.bitkom.org/Presse/Presseinformation/Bitkom-zu-den-Ergebnissen-des-Corona-Gipfels

[3] vgl. unter https://www.bitkom.org/Presse/Presseinformation/Datenschutz-deutsche-Wirtschaft-2022-DS-GVO-wenig-Wettbewerbsvorteile

Dabei gehen Datenschutzkonformität und die Einhaltung der datenschutzrechtlichen Vorgaben für viele Anwender mit der Annahme einher, dass hier eine unbändige Flut an Vorgaben zu beachten sei. Dieser Eindruck erwächst vermutlich aus der Prämisse, dass viele Anwender sich zeitgleich mit allen Vorgaben der Datenschutzgrundverordnung (DSGVO) konfrontiert sahen. Diese Herausforderung resultierte jedoch primär aus dem Inkrafttreten der DSGVO und ihren Auswirkungen auf bereits bestehende laufende Datenverarbeitungen. Zusätzlich geschah diese Konfrontation mit neuen datenschutzrechtlichen Vorgaben zu einem Zeitpunkt, als die Vorgaben für viele Anwender nicht klar greifbar waren. Das omnipräsente Damoklesschwert empfindlicher Bußgelder für Datenschutzverstöße verstärkte diese Unsicherheit noch weiter. Mag diese Situation auch so bestanden haben, trifft sie nicht mehr die aktuelle Situation.

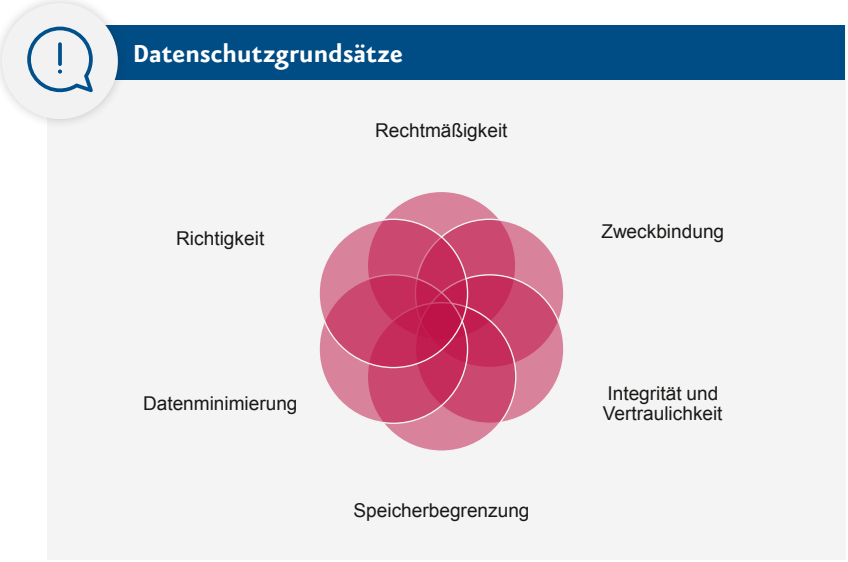
Seit Inkrafttreten der DSGVO haben sich vielmehr zentrale Bausteine für einen funktionierenden Datenschutz herausgebildet. Dies gilt insbesondere für IT-Anwender und Datenverarbeitungen mit IT-Bezug. Auch konnten viele Unklarheiten in Bezug auf datenschutzrechtliche Vorgaben durch Rechtsprechung und behördliche Informationen beseitigt oder zumindest verringert werden. Im Zuge dieser Entwicklung hat sich herausgestellt, dass auf Seiten der IT-Innovatoren eine hinreichende Sensibilität und ein Grundverständnis für Datenschutz ein entscheidender Faktor für datenschutzkonforme Innovation ist.

II. Überblick über den Datenschutz

Vor einer Ausdifferenzierung einzelner Vorgaben gilt es daher primär, dass der IT-Anwender eine IT-Innovation im Bewusstsein und unter Einhaltung der Datenschutzgrundsätze vorantreibt. Dazu erfordert es in einem ersten Schritt im Wesentlichen nicht viel mehr als dass sich ein Anwender bereits zu Beginn des Innovationsprozesses die Frage stellt, ob eine dadurch erfolgende Verarbeitung von Daten

- in die Rechte betroffener Personen übermäßig eingreift und
- ihm nicht weniger eingriffsintensive Lösungen zur Verfügung stehen.

Bereits hier geschieht eine erste Weichenstellung für datenschutzkonforme Innovation. Erst in einem zweiten Schritt sind dann die Grundsätze des Datenschutzrechts genauer zu beleuchten. So hat eine Verarbeitung unter der Berücksichtigung folgender Aspekte zu erfolgen:



Zusammenstellung der zentralen Datenschutzgrundsätze

Im Kern beinhalten diese Grundsätze die Forderung an eine gewünschte Grundhaltung bei der Verarbeitung personenbezogener Daten. Diese meint im Wesentlichen, dass sorgfältig und bedacht mit den Daten anderer umzugehen ist und diese eine hinreichende Möglichkeit zur Kenntnis vom Umgang anderer mit ihren Daten erhalten. Findet eine Verarbeitung statt, hat diese Verarbeitung daher

- sich auf das notwendige Maß zu beschränken,
- nur zu vorgenannten Zwecken zu erfolgen,
- nur unter Verarbeitung richtiger Daten zu erfolgen,
- nicht über die notwendige Dauer anzudauern,
- sich auf rechtmäßige und transparente Verarbeitungen zu beschränken und
- bei der Verarbeitung die Integrität und Vertraulichkeit der verarbeiteten Daten zu wahren.

Neben den rudimentären Leitlinien dieser omnipräsenten Grundsätze des Datenschutzes lassen sich die zentralen datenschutzrechtlichen Fragestellungen in Zusammenhang mit IT-Innovationen verkürzt in fünf weitere Themenblöcke unterteilen. Es handelt sich dabei um

- die Einhaltung datenschutzrechtlicher Informationspflichten, also betroffenen Personen die erforderlichen Informationen für ein hinreichendes Verständnis von der Datenverarbeitung in leicht zugänglicher Weise zur Verfügung zu stellen,

- die Rechtspflichten bei gemeinsamer Verantwortlichkeit bzw. Auftragsverarbeitung, also die Aufteilung der Beteiligten in Verantwortliche und Auftragsverarbeiter sowie der Abschluss der zugehörigen Vereinbarungen über die Verarbeitung,
- die Vorgaben bei Übermittlungen von Daten in Drittländer, also die Prüfung der Zulässigkeit einer Übermittlung von Daten in unsichere Länder außerhalb EU/EWR,
- die Vorgaben für besondere Verarbeitungssituationen (wie z.B. im Beschäftigtenverhältnis) und
- die Achtung der Betroffenenrechte, also insbesondere der Umgang mit Auskunftsansprüchen und den weiteren Betroffenenrechten.

III. Datenschutzrechtliche Themen am Life-Cycle der IT-Innovation

Mit Sicht auf den vorgezeichneten Rahmen ist für den IT-Anwender jedoch noch nicht allzu viel Erkenntnis gewonnen. Er fragt sich weiterhin, was habe ich zu welchem Zeitpunkt zu tun, um mir den Datenschutz zum Freund und Unterstützer zu machen. Sprechen wir über die Vorgaben der DSGVO, bleibt die Wahrnehmung des IT-Anwenders regelmäßig unberücksichtigt. Stets ist die Rede von Sanktionen, Informationspflichten und Datensparsamkeit. Doch was bedeutet das für einen Entwickler und IT-Anwender?

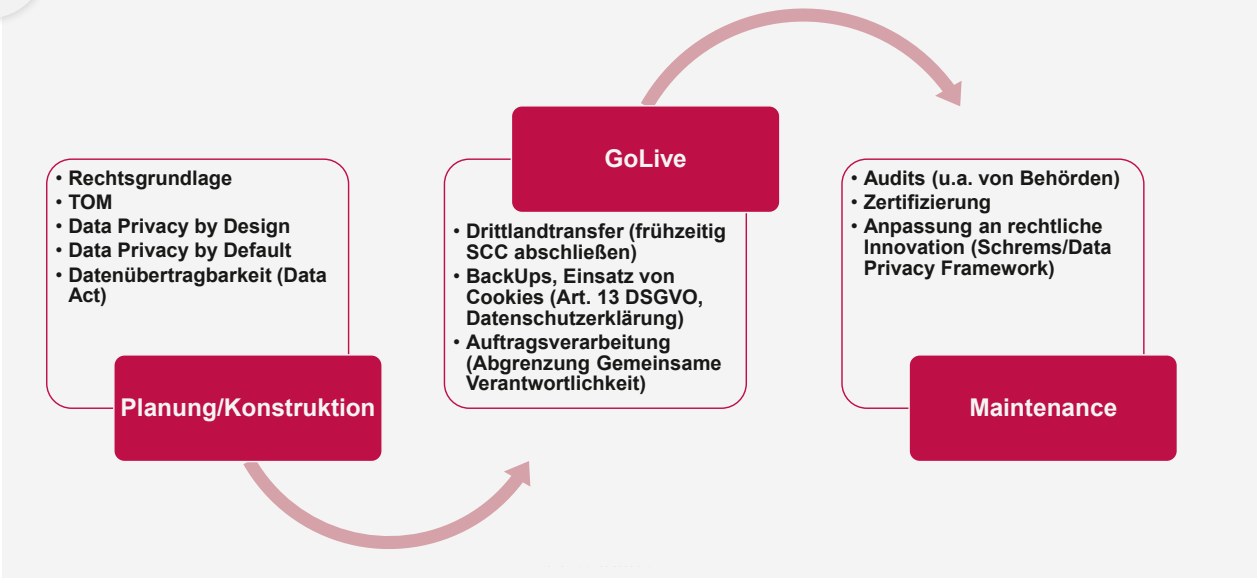
Entscheidend ist für ihn der Entwicklungs- und Lebenszyklus seiner Innovation. Der Innovationsprozess vollzieht sich in verschiedenen Phasen, nach denen die Projektplanung aufgebaut ist. Indes lassen sich die zentralen datenschutzrechtlichen Vorgaben auch auf die verschiedenen Phasen einer Innovation spiegeln:

Der IT-Anwender erhält durch diesen Blick auf die chronologische Abfolge datenschutzrechtlicher Pflichten die Möglichkeit, seine ToDos zu entzerren. Folgt er dieser Aufteilung, so entwickelt er die datenschutzrechtlichen Vorgaben zusammen mit seiner IT-Innovation innerhalb der Phasen seiner Projektplanung. Dadurch kann er schrittweise einzelne Vorgaben erfüllen, wodurch er über einen längeren Zeitraum geringere Kapazitäten vorhalten muss. Diese Aufteilung erspart ihm überdies, dass er alle Vorgaben zugleich erfüllen muss und entsprechend auch die gesamten wirtschaftlichen Aufwendungen zu einem Zeitpunkt zu erbringen hat.

Bei Betrachtung der Abbildung bietet sich im Anschluss mithin eine zumindest dreistufige Vorgehensweise an.

1. **Planung/Konstruktion:** Schon zu Beginn seiner Planung bezieht der Anwender Leitlinien des Datenschutzes ein, indem er sich etwa für die datensparsamere von zwei Alternativen entscheidet. Vor Ende der Planung eruiert der Anwender sodann die potenzielle Rechtsgrundlage, auf die er Verarbeitungen seiner Innovation zu stützen beabsichtigt. Fehlt es daran in zentralen Bereichen, ist eine rechtskonforme Anpassung zu diesem Zeitpunkt und ein Abbruch des Projekts noch kostensparsam durchführbar. Besteht eine Rechtsgrundlage ist es empfehlenswert bereits bei erster Konstruktion des Vorhabens eine hohe Wahrscheinlichkeit für Datenschutzkonformität des IT-Vorhabens zu schaffen, indem der Anwender bereits an dieser Stelle technisch-organisatorische Maßnahmen, datenschutzfreundliche Voreinstellungen und Konfigurationen aufnimmt.
2. **GoLive:** Ist die Konstruktionsphase abgeschlossen, sind vor dem GoLive zusätzliche Vorgaben auf ihre Relevanz

Überblick: Datenschutz in den Phasen der IT-Innovation



Phasenweise Darstellung der datenschutzrechtlichen Pflichten

zu prüfen. Zentral ist dabei der Aspekt, ob neben dem IT-Anwender weitere Personen und Unternehmen die personenbezogenen Daten verarbeiten und an welchem Ort die Verarbeitung stattfindet. Erfolgt die Verarbeitung durch andere Personen und/oder außerhalb der EU/des EWR, hat der IT-Anwender weitere datenschutzrechtliche Vorgaben einzuhalten. Ferner ist vor dem GoLive einer Innovation insbesondere zu beachten, dass die datenschutzrechtlichen Informationen vor oder spätestens mit dem GoLive zur Verfügung stehen und für Betroffene leicht einsehbar sind (etwa über die Datenschutzerklärung auf der eigenen Webseite).

3. **Maintenance:** Hat eine IT-Innovation den Zeitpunkt der GoLive überschritten, so enden damit nicht die datenschutzrechtlichen Pflichten des IT-Anwenders. So gilt es durch interne oder externe Audits die Wahrung der einschlägigen Vorgaben fortlaufend zu prüfen und die eigenen Maßnahmen und Prozesse fortlaufend an die weitere Entwicklung in Recht und Technik anzupassen. Überdies ist es wichtig, dass der IT-Anwender einen Prozess für den Umgang mit Anfragen und Rechten Betroffener vorhält, um möglichst schnell auf das jeweilige Begehr reagieren zu können.

Innerhalb dieses Pflichtenkanons lassen sich drei Themen (Rechtsgrundlage, Drittlandtransfer und Abschlüsse datenschutzrechtlicher Vereinbarungen) ausmachen, die bei Rückschau regelmäßig von besonderer Bedeutung für die IT-Anwender sind. Die Bedeutung resultiert dabei nur in Teilen aus der Komplexität der Rechtsfrage und in Teilen aus der Besonderheit von Innovationen mit informationstechnologischem Schwerpunkt. Dabei lassen sich zumindest grobe Leitlinien für den Umgang mit diesen Themen im Zuge der IT-Innovation an die Hand geben.

- Rechtsgrundlage: Findet bei einer Innovation gleich welcher Art eine Verarbeitung personenbezogener Daten statt, so bedarf es hierfür einer Rechtsgrundlage. Liegt eine wirksame Einwilligung für die gesamte Verarbeitung vor, bedarf es keiner weiteren Überlegungen. Nur selten wird dies der Fall sein. Vielmehr werden häufig bei komplexen IT-Anwendungen mehrere Rechtsgrundlagen in Betracht kommen und eine Einwilligung aus Gründen der Praktikabilität und Benutzerfreundlichkeit zumindest als alleinige Rechtsgrundlage ausscheiden. Je komplexer die Verarbeitungen einer Innovation sind, umso umfangreicher fällt die Relevanz der Frage nach der einschlägigen Rechtsgrundlage aus. Häufig übersehen Anwender, dass sie nur für Teile ihrer angestrebten Innovation die zutreffende Rechtsgrundlage gewählt haben. Vielfach lassen sie dabei die Besonderheiten (besonders sensible oder umfangreiche Verarbeitung) ihrer eigenen Innovation außer Acht. Diese führt dann nicht selten zu einer abweichenden Rechtsgrundlage mit abweichenden Vorgaben. Ebenso ist nicht selten zu beobachten, dass Anwender voreilig das berechtigte Interesse an einer Verarbeitung als Rechtsgrundlage bemühen.
- Drittlandtransfer: Mittlerweile bekannt ist die besondere Schwierigkeit bei Datenverarbeitungen mit Datenübermittlungen in unsichere Drittländer. Ungeachtet der Bekanntheit dieser Thematik herrscht weiterhin große Unsicherheit, wann eine Übermittlung von Daten in das Drittland tatsächlich einschlägig ist und wann eine Übermittlung in ein unsicheres Drittland ausnahmsweise zulässig ist. Neben behördlichen Stellungnahmen tragen auch einige gerichtliche Einzelfallentscheidungen hier zu einer weiterhin unklaren Rechtlage bei. Eine Zulässigkeit ist bei einem Drittlandtransfer regelmäßig nur für einen Anwender anzunehmen, wenn ein einschlägiger Angemessenheitsbeschluss für das jeweilige Drittland besteht.
- Abschlüsse datenschutzrechtlicher Vereinbarungen mit anderen Unternehmen: Schließlich kommt gerade bei IT-Projekten den datenschutzrechtlichen Vereinbarungen mit anderen Unternehmen besondere Bedeutung zu. Denn typischerweise findet bei einer IT-Innovation eine arbeitsteilige Umsetzung statt, die regelmäßig mehrere Unternehmen umfasst. Findet eine Datenverarbeitung in Teilen bei anderen Unternehmen statt, so bedarf es dazu einer tragfähigen Grundlage. Diese kann je nach Ausgestaltung in einer Vereinbarung über eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit münden. Allerdings hat diese Vereinbarung wiederum den Vorgaben der DSGVO zu genügen, um datenschutzrechtliche Fehltritte und daraus möglicherweise resultierende Sanktionen zu vermeiden. Erhebliche Unsicherheit herrscht in diesen Fällen insbesondere vor, wenn es um auf die Cloud bezogene Aspekte von Innovationen geht und die Verarbeitung durch andere Unternehmen erfolgt. IT-Anwender stehen hier typischerweise vor der Frage, ob und welche datenschutzrechtliche Vereinbarung in diesen Fällen zu schließen ist.

IV. Handlungsempfehlung

Im Ergebnis sollte man den Datenschutz als Teil der Innovation betrachten, indem die datenschutzrechtlichen Belange von Beginn an in den Prozess der Innovation eingebunden sind. Dazu gilt es für innovative Unternehmen (insbesondere im IT-Sektor) frühzeitig eine datenschutzrechtliche Expertise im Unternehmen zu schaffen, um Innovationspotenziale auszuschöpfen.

Naheliegend ist hierfür die frühzeitige Benennung eines internen oder externen Datenschutzbeauftragten. Denn neben seiner datenschutzrechtlichen Expertise besitzt der Datenschutzbeauftragte aufgrund seiner Position typischerweise

VOICE E.V.

VOICE e.V. ist der Bundesverband der IT-Anwender sowie Digital-Entscheider der Anwenderseite. Die rund 400 Mitglieder repräsentieren einen Querschnitt aus insgesamt 2.600 DAX-, MDAX- und mittelständischen Unternehmen. Ziel ist es, die Wettbewerbsfähigkeit von Mitgliedsunternehmen durch den Einsatz von digitalen Technologien zu stärken. Vorsitzende des VOICE-Präsidiums ist die Wirtschaftsingenieurin und Betriebswirting Dr. Bettina Uhlich, Wolfgang Stork ist Geschäftsführer. Partner sind unter anderem der Bundesverband Materialwirtschaft, Einkauf und Logitik, die GFFT, Gemeinnützige Gesellschaft zur Förderung des Forschungstransfers sowie das Landeskriminalamt Nordrhein-Westfalen. VOICE ist außerdem Mitglied in der Arbeitsgruppe „Prävention von Internet- und Computerkriminalität" des Landespräventionsrats NRW.

umfassende Kenntnisse von den internen Abläufen und der datenschutzrechtlichen Organisation innerhalb des Unternehmens. Dadurch ist er in der Lage die Lösung datenschutzrechtlicher Fragestellungen erheblich zu beschleunigen. Insofern bietet sich die Benennung des Datenschutzbeauftragten unabhängig vom Bestand einer Benennungspflicht (zum Beispiel auch für Start-Up-Unternehmen) an.

Stellen sich dem Anwender Unklarheiten bezüglich der Einordnung seiner Innovation, ist eine frühzeitige Klärung offener Fragen und Unsicherheiten zu empfehlen. So erhält sich der Anwender die eigene Innovation, indem rechtliche Fragestellungen unter frühzeitiger Einbeziehung der notwendigen Expertise effizient und kostensparend in den Entwicklungsprozess Berücksichtigung finden.

Neben dem Aufbau einer internen Expertise zu relevanten datenschutzrechtlichen Fragestellungen bietet sich dazu die Kooperation mit externen Experten an. Der Erfahrungsschatz und die zusätzlichen Kapazitäten externer Berater eröffnen regelmäßig neue Potenziale für die Umsetzung einer Innovation. Eine frühzeitige Einbeziehung externer Berater hilft zugleich Kosten zu sparen. Eine frühzeitige Beratung kann dabei je nach Bedürfnis eines Unternehmens an ganz unterschiedlichen Punkten ansetzen:

- Konkret kann die Beratung die Leistung sein, bei einem im Aufbruch begriffenen Start-Up frühzeitig ein Bewusstsein für relevante Vorgaben zu schaffen, um etwa nach dem GoLive seiner Innovation auch den datenschutzrechtlichen Vorgaben an Informationspflichten rechtzeitig nachzukommen.
- Auch kann es die Erkenntnis sein, dass nach dem risikoorientierten Ansatz der Datenschutz-Grundverordnung der befürchtete Verstoß nicht vorliegt oder das Risiko einer Verletzung geringer ist als gedacht.
- Ebenso kann die Leistung darin bestehen, ein funktionierendes Datenschutzmanagementsystem (DSM) bei einem Konzern zu implementieren.

Ein frühzeitiges Bewusstsein steigert zudem die Wahrscheinlichkeit, dass ein Unternehmen im Zuge einer IT-Innovation datenschutzrechtliche Pflichten erfüllt. Dies kann etwa die Fertigstellung von Datenschutz-Informationen im Zeitpunkt des Inverkehrbringens der Innovation sein.

Für IT-Innovationen bieten sich einem innovativen Unternehmen zusätzliche Kosteneinsparungen, indem es verwandte rechtlich relevante Themen an einen Experten auslagert. So liegen rechtliche Fragestellungen aus dem Recht der Informationstechnologie, dem Medienrecht und dem Datenschutzrecht üblicherweise nah beieinander. Besitzt ein Experte ausgewiesenes Fachwissen in sämtlichen Bereichen, lassen sich durch Synergieeffekte weitere Kosten sparen. Im Übrigen ist es empfehlenswert, eine datenschutzrechtliche Compliance als Unterscheidungsmerkmal gegenüber Wettbewerbern zu erkennen. So lässt sich immer stärker beobachten, dass Nutzer den Risiken für ihre Daten stärkere Bedeutung bei der Wahl eines neuen Produkts beimessen.

Synergieeffekte bei der Umsetzung und Gestaltung von IT Projekten

Kosteneinsparungen durch Synergieeffekte

V. Ausblick

Auch zukünftig verbleiben die dargestellten Fragestellungen ein relevanter Faktor für die Durchsetzung von IT-Innovationen.

Zudem gesellen sich zu den altbekannten Fragen weitere Themenbereiche mit Bezug zur Datenverarbeitung, die neue Gesetzesvorhaben aufwerfen. Primär gilt das bereits jetzt für das neue Kaufrecht, das auch digitale Produkte umfasst und erstmalig datenschutzrechtliche Fragestellungen in das Kaufrecht aufnimmt. Nicht weniger bedeutsam dürfte der Data Act in seiner Wirkung sein, der die Datensouveränität und Datenportabilität umfassend regeln soll. Gerade für letztgenannten Data Act gilt das Postulat einer frühzeitigen Befassung mit problematischen Fragestellungen. Denn hier besteht zumindest noch eine Umsetzungsfrist, die es ermöglicht eine rechtskonforme Innovation zu schaffen und Fallstricke einer verspäteten Problembehebung zu vermeiden.

Schließlich werfen verschiedene Gesetzesvorhaben mit Bezug zur künstlichen Intelligenz ihren Schatten voraus (insbesondere der Artificial Intelligence Act), die allesamt Querverbindungen zu datenschutzrechtlichen Fragestellungen (wie etwa den Umgang mit Trainingsdaten) aufweisen und in naher Zukunft große Bedeutung erlangen dürfen (z.B. für Fragestellungen rund um den Einsatz von ChatGPT und vergleichbaren Tools).

Über die Autoren

Dr. Michael Rath
ist Rechtsanwalt, Fachanwalt für Informationstechnologie-Recht und Partner der Luther Rechtsanwaltsgesellschaft mbH mit Sitz in Köln. Zudem ist er Certified ISO/IEC 27001 Lead Auditor. Seine Beratungsschwerpunkte sind das IT-Recht, Datenschutzrecht und der Gewerbliche Rechtsschutz. Dr. Michael Rath ist u.a. Mitglied in der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI) und akkreditierter Schlichter für IT-Streitigkeiten bei der Schlichtungsstelle der DGRI.

Dennis Göbel
ist Rechtsanwalt bei der Luther Rechtsanwaltsgesellschaft mbH mit Sitz in Köln. Seine Beratungsschwerpunkte sind das Medienrecht, IT-Recht, Datenschutzrecht und der gewerbliche Rechtsschutz.

CHRISTINA DENZ

VON IDENTITÄTSDIEBSTAHL, ZEITRAUB UND DATEN-SAMMELWUT

Die Nominierten für den Datenschutz Medienpreis 2022

Zum sechsten Mal hat die Jury drei Nominierte ausgewählt, die auf die mit 3.000 Euro dotierte Auszeichnung hoffen. Bei ihrer Sitzung am 1. März kürte die Jury die folgenden drei Beiträge für die Endrunde.

Audio-Reportage

„Identitätsdiebstahl über Jobportale".

In ihrem Beitrag für das Podcast-Format „Der Funkstreifzug" des Bayerischen Rundfunks geht Autorin Sabina Wolf Fällen von Identitätsdiebstahl über gefälschte Stellenangebote im Netz nach. Besonders perfide: Die Betrugsmasche läuft als Job-Angebot auf bekannten Online-Stellenportalen. Erste Anfragen und Arbeitsbedingungen klingen für die späteren Opfer seriös. Erst wenn sie alle Daten preisgeben und sich per Video auf ein Ident-Verfahren einlassen, stellen sich Unregelmäßigkeiten auf ihrem Konto ein oder sie geraten ins Visier von Polizeiermittlungen. Autorin Sabina Wolf hat mit Opfern gesprochen und gibt Tipps, wie sich der Identitätsdiebstahl auf Jobportalen verhindern lässt.

©Bayerischer Rundfunk (BR)

Darum nominierte die Jury die Einreichung:

„Der Beitrag von Sabina Wolf verdeutlicht insbesondere die neuen Vorgehensweisen von Betrügern im World Wide Web: Da neue Verfahren wie das Videoident-Verfahren zur Eröffnung von Bankkonten immer häufiger Verwendung finden, gibt es mit Sicherheit eine größere Anzahl Bürger:innen, die deshalb bei einem Bewerbungsgespräch ihren Ausweis vorzeigen würden. Eine vollumfängliche Sicherheit ist somit selbst auf integren Plattformen nicht mehr gegeben, weshalb der Beitrag bei der gesellschaftlichen Aufklärung umso wichtiger ist. Alles in Allem: sehr kurzweilig, aufklärend und für jeden geeignet."

Tobias Meisel, Mitarbeiter der DATEV-Stiftung Zukunft

Text-Reportage

„Was Google über uns weiß"

Für die „Süddeutsche Zeitung" recherchierten Sabrina Ebitsch, Berit Kruse, Sophie Menner, Sead Mujic, Leonie Rothacker, Marie-Luise Timcke und David Wünschel, was Google mit den Daten seiner Nutzerinnen und Nutzer anfängt. Dazu hat das Team knapp zwölf Profile analysiert. Diese realen Daten fassten sie in der fiktiven Protagonistin „Sofia" zusammen.

In ihren Recherchen fördert das Team auch Unbekanntes zutage, etwa, dass bei Google pro Sekunde weltweit rund 100.000 Suchanfragen eingehen. Sie erläutern das hochumstrittene Real Time Bidding, bei dem Google im Bruchteil einer Sekunde meistbietende Werbeanzeigen gezielt platziert und befragte Experten und Expertinnen nach ihrer Einschätzung, darunter Johnny Ryan von der irische Nicht-Regierungsorganisation Irish Council for Civil Liberties. Außerdem bietet David Wünschel eine Anleitung, wie Nutzer und Nutzerinnen ihre Daten bei Google einsehen und die Datensammelwut einschränken können.

©Sead Mujic. Mit freundlicher Genehmigung von Süddeutsche Zeitung Content.

Darum nominierte die Jury die Einreichung:

„Neben der Tatsache, dass einen der Artikel von Beginn an fesselt, haben mich die umfangreichen Analyse- und Recherchearbeiten des Autoren-

Teams sehr beeindruckt. Die Erläuterungen zum Real-Time-Bidding und vor allem zur möglichen politischen Einflussnahme von Google durch das gezielte Ranking von politischer Werbung an die oberste Stelle der Suchergebnisse, ohne, dass diese mit dem eigentlichen Suchbegriff zu tun haben, haben mich zum einen wachgerüttelt und bereiten mir zum anderen große Sorge für die Zukunft.“

Lars Kolan, Geschäftsstellenleiter Deutscher Spendenrat e.V.

Video-Clip

„Gemeinsam für die Privatsphäre. Damit Du mehr Zeit für Fußball hast.“

Andrina Schmid und der Videograf Samuel Wetter, beide aus Zürich, bringen in dem nur eine Minute und vierzig Sekunden kurzen Clip die Auswirkungen des permanenten Online-Checks auf den Punkt. Dafür haben sie die Figur „Max“ entwickelt, die sie in humorvollen Alltagssequenzen am Smartphone filmen. Die beiden wollen zeigen: Weniger Online gibt mehr Zeit für die liebsten Dinge offline.

Mit dem Clip gewannen die beiden 24 und 25 Jahre alten Video-Filmenden bereits den ersten Preis des Datenschutzbeauftragten des Kanton Zürichs im vergangenen Jahr.

©Andrina Schmid, Samuel Wetter

Darum nominierte die Jury die Einreichung:

„Der eindrucksvolle Kurzfilm zeigt in prägnanter und amüsanter Weise, wieso Datenschutz in unserem Alltag so eine wichtige Rolle spielt. Es wird verdeutlicht, wie gerade Jugendliche, tagtäglich durch die Nutzung des Internets und der sozialen Medien beeinflusst werden und ihre tiefste Privatsphäre offen gelegt und verletzt werden kann.“

Eric Hohenadel, klicksafe-Jugendjuror

Die Jury des Datenschutz Medienpreises 2022:

Hans Block (Laokoon-Gruppe), Filmregisseur und Preisträger DAME 2021
Birgit Kimmel Päd. Leitung klicksafe, Medienanstalt Rheinland-Pfalz
Stefanie Rack Päd. Referentin klicksafe, Medienanstalt Rheinland-Pfalz
Eric Hohenadel klicksafe-Jugendjuror
Frederick Richter Vorstand Stiftung Datenschutz
Wolfgang Stückemann Vorstandsvorsitzender Deutscher Spendenrat
Thomas Spaeing Vorstandsvorsitzender BvD
Tobias Meisel Mitarbeiter DATEV-Stifung Zukunft
Barbara Thiel Landesbeauftragte für den Datenschutz Niedersachsen
Marion Zinkeler Vorständin Verbraucherzentrale Bayern

Der BvD rief den Datenschutz Medienpreis 2017 ins Leben, um kreative Ideen zu fördern, die Aspekte des Datenschutzes konkret und gezielt verständlich aufbereitet. Seit 2021 führt die gemeinnützige privacy4people gGmbH die Ausschreibung fort.

Alle Beiträge finden Sie auf
▶ www.datenschutzmedienpreis.de

Über die Autorin

Christina Denz
ist Journalistin, Kommunikationsberaterin und Redakteurin der „BvD-News“.

Medienpartner: klicksafe

Förderer: DATEVSTIFTUNG ZUKUNFT, STIFTUNG DATENSCHUTZ, Deutscher Spendenrat e.V. Die gute Tat im Blick

NEUE PRAKTIKUMS-BÖRSE DES BVD

Kooperation mit der Hochschule Ansbach

Der BvD bietet seit Januar eine kostenlose Datenschutz-Praktikumsbörse an. Sie ist Teil einer Kooperation mit der Hochschule Ansbach und deren Bachelorstudiengang „Datenschutz & IT-Sicherheit“, um Studierenden eine praxisnahe Ausbildung im Bereich Datenschutz und IT-Sicherheit zu ermöglichen. Auch Studierenden anderer Hochschulen und Universitäten steht die Praktikumsbörse offen.

„Wir würden uns sehr freuen, wenn möglichst viele Unternehmen oder auch öffentliche Stellen dieses Projekt unterstützen würden, indem sie Praktikumsplätze im Bereich Datenschutz auf dieser Plattform anbieten“, so Jürgen Hartz, stellvertretender Vorstandsvorsitzender des BvD, der die Kooperation initiiert hat. „Diese Möglichkeiten sind für junge Menschen, die sich in diesem Bereich ausbilden lassen möchten, von unschätzbarem Wert. Gleichzeitig leisten wir damit einen konkreten Beitrag zur Förderung des Berufsbildes von Datenschutzbeauftragten, ein für uns wichtiger Schritt in der fortwährenden Qualifizierung und Professionalisierung vor dem Hintergrund unserer immer komplexeren digitalen Welt.“

Die Kooperation umfasst neben der Praktikumsbörse unter anderem einen Austausch von Referentinnen und Referenten zwischen dem BvD und der Hochschule, sowie die Veröffentlichung von Fachartikeln von Hochschulmitarbeitenden in den BvD-News und die Möglichkeit der Erarbeitung gemeinsamer Studien und Arbeitshilfen. Auch eine kostenfreie Probemitgliedschaft im BvD für Studierende der Hochschule Ansbach ist Teil der zum Jahresbeginn gestarteten Zusammenarbeit. Von der Kooperation sollen zukünftig auch die BvD-Mitglieder profitieren. Durch den Austausch von Referentinnen und Referenten und die Möglichkeit der Teilnahme an ausgewählten Modulen der Hochschule sollen BvD-Mitglieder die Möglichkeit erhalten, ihr Fachwissen zu vertiefen und zu erweitern.

Auch die Hochschule Ansbach zeigt sich erfreut über die neue Kooperation: „In unserem Studiengang Datenschutz und IT-Sicherheit bilden wir künftige Datenschutz-Expertinnen und -Experten auf akademischem Niveau aus. Durch die Kooperation mit dem BvD haben unsere Studierenden die Möglichkeit, ihr Wissen zu erweitern und sie erhalten außerdem auf ihre Kenntnisse zugeschnittenen Stellenangebote. Auch die Lehre profitiert durch Gastvorträge und eine Plattform, auf der Forschungsergebnisse veröffentlicht werden können“, so die Co-Leiterin des Studiengangs Datenschutz und IT-Sicherheit (DIS) an der Hochschule Ansbach, Prof. Dr. Stefanie Fehr.

STELLEN SIE JETZT KOSTENLOS IHR PRAKTIKUMSANGEBOT EIN UNTER:

▶ https://www.bvdnet.de/datenschutz-praktikumsboerse/
Ihr Eintrag ist kostenlos und innerhalb von wenigen Minuten über ein Formular erstellt.

LINK-TIPP

BfDI-Diskussionsforum

Der Bundesbeaulragte für den Datenschutz und die Informamationsfreiheit (BfDI) bietet ein öffentliches Dikussionsforum zum Datenschutz unter:

▶ https://forum.bfdi.bund.de/

EU-Rechtsprechungen

„JURE“ heißt die Datenbank der Europäischen Kommission zu gerichtlichen Entscheidungen, in der sich detailliert und gezielt nach Verfahren und ihren Ausgängen suchen lässt. Die Datenbank enthält unter anderem Entscheidungen von EU-Gerichten und Gerichten der Mitgliedsstaaten in Zivil- und Handelssachen.

▶ https://eur-lex.europa.eu/collection/n-law/jure.html

Welche Homepage und/oder Link können Sie empfehlen? Schreiben Sie uns an bvd-news@bvdnet.de.

DS-GVO / BDSG

DATENSCHUTZ-GRUNDVERORDNUNG VO (EU) 2016/679 BUNDESDATENSCHUTZGESETZ

Prof. Peter Gola, Prof. Dr. Dirk Heckmann (Hrsg.)

Im 5. Jahr der Datenschutz-Grundverordnung erscheinen immer weitere Kommentierungen und, natürlich der Aktualität und Weiterentwicklung geschuldet, neue Auflagen bereits erschienener Werke. Und es wird wohl kaum einen Datenschutz-Experten geben, der die „orange Kommentierung" der DS-GVO von Gola nicht kennt. Neben Prof. Peter Gola ist bei der 3. Auflage auch Prof. Dr. Dirk Heckmann Mitherausgeber.

Bisher erschienen getrennte Kommentierungen zur DS-GVO und zum BDSG. Aber wie verhält sich die Datenschutz-Grundverordnung zum nationalen Recht, dem Bundesdatenschutzgesetz? In der neuen Auflage werden diese beiden Kommentierungen in einem Band zusammengefasst. Außerdem berücksichtigt die 3. Auflage weitere gesetzliche Neuerungen wie zum Beispiel in der Telekommunikation (TTDSG) und im Beschäftigtendatenschutz sowie Stellungnahmen von Datenschutzaufsichtsbehörden und die aktuelle Rechtsprechung.

Es wird immer wieder Bezug auf unternehmerische Problemstellungen genommen. Die Kommentierungen sind daher praxisnah und unterstützen bei der Beurteilung von datenschutzrechtlichen Fragestellungen. Die Kommentierungen sind gut verständlich und praxisnah, gepaart mit vielen – zwangsläufig nach fast fünf Jahren Anwendbarkeit – Literaturverweisen, um somit auch im Bedarfsfalle noch tiefer in eine Thematik einsteigen zu können.

Damit umfasst die 3. Auflage 1.864 Seiten, davon entfallen etwa ein Drittel auf die BDSG-Kommentierung.

Das Stichwortverzeichnis ist sehr umfangreich und erleichtert das Finden, da es eben nicht nur Begrifflichkeiten aus den Gesetzestexten umfasst.

Das Werk wächst und bleibt seiner Übersichtlichkeit und Verständlichkeit dennoch treu, wie auch seiner Praxisnähe.

Mit 99 Euro zählt die Kommentierung zu den günstigeren – aber nicht minder eine aus der Kategorie „sehr gutes und praxisnahes Nachschlagewerk" zur Beurteilung von datenschutzrechtlichen Themen.

Prof. Peter Gola/Prof. Dr. Dirk Heckmann (Hrsg.)
DS-GVO / BDSG
DATENSCHUTZ-GRUNDVERORDNUNG VO (EU) 2016/679 BUNDESDATENSCHUTZGESETZ

C.H.Beck

3. Auflage 2022
1 864 Seiten
99,00 Euro
ISBN: 978-3-406-78266-4

Rezension von

Regina Mühlich (CIPM)
ist Wirtschaftsjuristin, Datenschutzbeauftragte und -auditorin, CIPM (IAPP) sowie Compliance Officer. Sie ist Geschäftsführerin der AdOrga Solutions GmbH und Vorstandsmitglied im BvD e.V. sowie Mitglied im Ausschuss Recht & Politik.

▶ www.AdOrgaSolutions.de

KÜNSTLICHE INTELLIGENZ UND ALGORITHMEN IN DER RECHTSANWENDUNG

Prof. Dr. Martin Kment, Sophie Borchert

Aufmerksame Leser dieser Rubrik werden sich entsinnen, dass an dieser Stelle in den vergangenen Heften diverse Neuerscheinungen zum Thema Künstliche Intelligenz besprochen worden sind. Alle Werke unterschieden sich wesentlich, was die Zielgruppe, den wissenschaftlichen Anspruch und die Art des Werkes betrafen. So hebt sich auch dieses Werk ab und beansprucht einen legitimen Platz in der Reihe zu empfehlender Publikationen zur künstlichen Intelligenz.

Der Band mutet zunächst durch sein sehr handliches Format an. Die Autoren haben es tatsächlich geschafft, ihre Gedanken auf gerade einmal 120 Seiten zu bündeln. Dabei befassen sie sich in sechs Kapiteln mit den informatorischen Grundlagen, der Rechtsanwendung in der digitalen Welt, den Problemen im Zusammenhang mit dem Einsatz von Algorithmen sowie den Möglichkeiten, diese zu regulieren. Ihre Bewertung orientieren die Autoren nicht an etablierten Rechtsgebieten (z.B. Datenschutzrecht, Zivilrecht, Steuerrecht), sondern liefern eine ganz eigenständige Bewertung, wobei sie für sich selbst in Anspruch nehmen, einen Überblick über den substanziellen Nexus der Thematik liefern zu wollen.

Die rechtliche Bewertung erfolgt weitgehend anhand ausgewählter Anwendungsfälle des Algorithmuseinsatzes im privaten und öffentlichen Kontext, wobei der Fokus auf Umweltschutz und Mobilität liegt. Dabei konzentrieren sie sich vor allem auf verfassungsrechtliche Aspekte, psychologische Phänomene und das weite Feld der Datensicherheit. Hierbei imponiert das Bewusstsein der Autoren, dass die Informationstechnik der Rechtswissenschaft stets einen Schritt voraus ist. So ist das 5. Kapitel (Regulierungsmöglichkeiten für den Algorithmuseinsatz) besonders lesenswert, da es nicht nur die verschiedenen Möglichkeiten des Gesetzgebers aufzeigt, sondern gleichzeitig den Leser in die Lage versetzt, den Entwurf des Artifical Intelligence (AI) Act, der aktuell in der Europäischen Union diskutiert wird, besser zu verstehen. Hierzu trägt bei, dass die Autoren methodisch verschiedene Herangehensweisen des Gesetzgebers zu erklären wissen, indem sie aufzeigen, dass es sowohl risikobasierte, repressive als auch präventive Regulierungsoptionen inklusive Totalverbot und Zulassungskontrolle gibt. Der Leser wird dadurch animiert, sich ein eigenes Bild von der Güte des vom europäischen Gesetzgeber gewählten Ansatzes zu machen.

Vor diesem Hintergrund erhält das Werk eine besondere Leseempfehlung für diejenigen Kolleginnen und Kollegen, die sich frühzeitig auf eine höchst relevant werdende und wahrscheinlich unsere Zukunft in erheblichem Maße beeinflussende Regulierung auseinandersetzen und den Diskurs mitgestalten wollen.

Prof. Dr. Martin Kment, Sophie Borchert
KÜNSTLICHE INTELLIGENZ UND ALGORITHMEN IN DER RECHTSANWENDUNG

C.H.Beck

2022
124 Seiten
49,00 Euro
ISBN 978-3-406-78619-8

Rezension von
Dr. Christoph Bausewein, CIPP/E, CIPT
ist BvD-Vorstandsmitglied und Director & Counsel, Data Protection & Policy bei CrowdStrike.

DER VORBEHALT MENSCHLICHER ENTSCHEIDUNGEN IM ARBEITSVERHÄLTNIS

Maurice Heine

Es gibt kaum einen Bereich, der von der Anwendung Künstlicher Intelligenz ausgeschlossen scheint. Auch im Arbeitsverhältnis sind Entscheidungen oder Vorbereitungen dazu nicht nur denkbar, es gibt bereits erste Tools, die hier Unterstützung versprechen. Umso erfreulicher, dass eine wissenschaftliche Auseinandersetzung mit den entsprechenden datenschutzrechtlichen Aspekten im Rahmen einer Dissertation veröffentlicht wurde. Welche Arbeitgeberentscheidungen sind geeignet mittels Einsatz Künstlicher Intelligenz unterstützt oder getroffen zu werden? Wann ist dabei der Anwendungsbereich des Art. 22 DS-GVO eröffnet und wie sind in diesem Kontext die Ausschließlichkeitskriterien bei Entscheidungsvorbereitungen zu bewerten? Welches Instrumentarium zur Absicherung bieten individual- und kollektivrechtliche Rahmenbedingungen? Mit diesen Fragen befasst sich das Werk.

Nach einer Einleitung und der Beschreibung des Gegenstands der Betrachtung erläutert der Autor zunächst die Grundlagen der Algorithmisierung und beschreibt dann, welche Arbeitgeberentscheidungen hierfür geeignet wären. Nach einer rechtlichen Bewertung widmet er sich den Rechtspositionen der Arbeitnehmer, bevor ausgewählte Fallgruppen algorithmisierter Arbeitgeberentscheidungen betrachtet werden. Das letzte Kapitel beleuchtet dann die praktische Durchsetzung inklusive den Fragestellungen zu individual- und betriebsverfassungsrechtlichen Absicherungen. Erfreulich ist dabei, dass bereits die Ergänzungen des Betriebsverfassungsgesetzes durch das Betriebsrätemodernisierungsgesetz Eingang in die Betrachtung gefunden hat. Das Werk endet mit einem Ausblick.

Maurice Heine
DER VORBEHALT MENSCHLICHER ENTSCHEIDUNGEN IM ARBEITSVERHÄLTNIS

Verlag Duncker & Humblot

2023
484 Seiten
119,90 Euro
ISBN: 978-3-428-18817-8

Ungeachtet des wissenschaftlichen Anspruchs liest sich das Werk flüssig und ist auch diesbezüglich zu empfehlen. Auch wenn maßgebliche Rechtsgrundlagen wie der § 26 BDSG, dessen Wortlaut bezüglich der Umsetzung des Art. 88 DS-GVO bereits dem EuGH zur Prüfung vorliegt, womöglich nicht von Dauer sind, finden sich in den Ausführungen Überlegungen, die auch in einem künftigen Beschäftigten-Datenschutz Berücksichtigung finden sollten. Die Berücksichtigung der Erkenntnisse hilft nicht nur Stellen, die zum Datenschutz und insbesondere zum Einsatz von Künstlicher Intelligenz im Personalbereich beraten. Sie können auch den Einheiten helfen, die Entwicklungsbereiche rechtlich unterstützen, die Software für den Einsatz in der Personalverwaltung konzipieren, um einen rechtskonformen Einsatz von vornherein zu ermöglichen.

DATENSCHUTZRECHT:
DS-GVO; BDSG; GRUNDLAGEN; BEREICHSSPEZIFISCHER DATENSCHUTZ

Prof. Dr. Heinrich Amadeus Wolff, Dr. Stefan Brink (Hrsg.)

Das Werk hatte sich bereits in der ersten Auflage schnell als Standardwerk etabliert. Das lag zum einen an der Auswahl der Autoren, die sich aus Expert:innen von Aufsichtsbehörden und beratender Praxis zusammensetzen. Zum anderen aber auch an der Struktur und Tiefe der Darstellungen.

Auch in der zweiten Auflage wurde die qualitativen Anforderungen an die Auswahl der Kommentator:innen fortgeführt. Neben der DS-GVO wird auch das BDSG ausführlich kommentiert. Nicht nur für „Neueinsteiger" in das Rechtsgebiet bietet die Darstellung der Prinzipien des Datenschutzrechts vor die Klammer gezogene Erkenntnisse, die zwar teilweise auch bei der Kommentierung zu Art. 5 DS-GVO angesprochen werden, dort aber durch einen anderen Bearbeiter. Dies ermöglicht die Auseinandersetzung mit unterschiedlichen Schwerpunkten, Sichtweisen und Argumentationen innerhalb des Werkes. Gerade die Herausarbeitung unterschiedlicher Argumentationslinien bei komplexen Themen haben sich die Herausgeber laut Vorwort vorgenommen – und ist ihnen meines Erachtens nach gelungen.

Dies wird besonders deutlich, wenn eine Thematik an unterschiedlichen Stellen behandelt wird. Dabei finden sich oftmals fundierte Kommentierungen neuer Probleme, die sich nicht nur auf die Wiedergabe bestehender Rechtsprechung und Aufsichtspraxis beschränkt, sondern Lösungswege beschreiben und begründen. Naturgemäß können dabei unterschiedliche rechtliche Bewertungen entstehen. Dies ist aber in meinen Augen gerade der Mehrwert des Bandes, weil in einem so jungen Rechtsgebiet wie der Auslegung europäischen Rechts sowie der rasanten technischen Entwicklung und gesellschaftlichen Änderungen nur in wenigen Fällen von Anfang an Konsens zu Interpretationen und Einschätzungen bestehen dürfte.

Prof. Dr. Heinrich Amadeus Wolff, Dr. Stefan Brink (Hrsg.)
DATENSCHUTZRECHT: DS-GVO; BDSG; GRUNDLAGEN; BEREICHSSPEZIFISCHER DATENSCHUTZ

C.H.Beck

2. Auflage 2022
1.763 Seiten
Preis: 169,00 Euro
ISBN 978-3-406-78990-8

Die Fülle der Vorlageentscheidungen an den EuGH bestätigt diese Wahrnehmung. So sind hier keine einfachen Antworten zu erwarten, sondern in den meisten Fällen werden argumentativ und mit Quellenangabe Problematiken unter Schilderung der Vorgehensweise einem Lösungsvorschlag zugeführt.

Erfreulich bleibt wie bereits in der ersten Auflage die Darstellung bestimmter bereichsspezifischer Datenschutzthematiken wie „Datenschutz bei Gerichten und Staatsanwaltschaften" oder bei „freien Berufen".

Das gedruckte Werk basiert auf der 38. Edition des im gleichen Verlag als Online-Version erschienen Kommentars. Allein hier sind Verbesserungen denkbar, dass mit dem Kauf des Werkes auch eine zeitlich begrenzte Nutzung der Online-Version ermöglicht werden könnte.

Ein rundum empfehlenswertes Werk, das umfassend mit Grundlagen zu datenschutzrechtlicher Beratung und Bewertung unterstützt.

Rezensionen von

Rudi Kramer
ist Syndikusanwalt und Sprecher der AK Schule sowie des AK Finanzdienstleistungen im BvD e.V.

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE

Die wichtigsten Daten der BvD-Gremien

Detaillierte Informationen zu den Treffen und Terminen finden Sie unter:

- www.bvdnet.de/regionalgruppen
- www.bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

03.04.2023	RG Schwäbisch Gmünd		
12.04.2023	RG Sachsen	**13.06.2023**	RG Sachsen
27.04.2023	RG Nord	**16.06.2023**	RG Karlsruhe
04.05.2023	RG Gütersloh	**16.06.2023**	RG Karlsruhe
04.05.2023	RG West	**21.06.2023**	AK FinanzDL
11.05.2023	AK Externe	**23.06.2023**	RG Nürnberg
05.06.2023	RG Schwäbisch Gmünd	**29.06.2023**	RG Nord

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

Termine und Anmeldung finden Sie auf unserer Webseite:

- www.bvdnet.de/termine/

BVD-STELLENBÖRSE

Sie suchen ausgewiesenes Datenschutz Know-how für Ihr Unternehmen? Mit einer Anzeige in der BvD-Stellenbörse finden Sie zertifizierte Datenschutzbeauftragte für eine Festanstellung oder als externe Berater. Zur Stellenbörse:

- www.bvdnet.de/bvd-stellenboerse

VERNETZEN SIE SICH MIT UNS:

- www.bvdnet.de

Mastodon: https://mastodon.social/@bvd@privacyofficers.social

LinkedIn: www.linkedin.com/company/berufsverband-der-datenschutzbeauftragten

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

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

BVD PARTNERSHIP PROGRAM

Mit seinem Partnership Program bietet der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. Unternehmen die Möglichkeit die Sichtbarkeit in ihrer Zielgruppe zu erhöhen und somit ihre Marke vor einer der größten Gemeinschaften von Datenschutzfachleuten in Deutschland zu präsentieren. Bei BvD-Events können die Partner zudem vom BvD-Netzwerk profitieren und wertvolle Kontakte knüpfen.

Gleichzeitig tragen Partner durch ihr finanzielles Engagement dazu bei die Beiträge für die BvD-Mitglieder stabil zu halten. Dem Verband wird außerdem ermöglicht seine von den Satzungszwecken vorgegeben Aktivitäten weiter auszubauen. Denn die zunehmende Komplexität unserer Kommunikationsgesellschaft erfordert einen starken Berufsverband für Datenschutzbeauftragte.

Bei der Auswahl geeigneter Partner hat sich der BvD auf einen Code of Conduct verpflichtet, welcher die Integrität, Neutralität und die Wahrung der Verbandssatzung sicherstellt.

» Bei Fragen zu oder Interesse an einer Partnerschaft wenden Sie sich bitte an:

Karsten Füllhaase
Geschäftsführer
Tel. +49 (0)30 20 62 14 41
▶ karsten.fuellhaase@bvdnet.de

Wir danken unseren Silver Partnern:

OneTrust PRIVACY, SECURITY & GOVERNANCE

▶ www.onetrust.de

RHENUS OFFICE SYSTEMS

▶ www.rhenus.group/de

WEITERE WICHTIGE KONTAKTE

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

Informationen zu Anzeigen und Werbemöglichkeiten in der BvD-News erhalten Sie unter bvd-news@bvdnet.de.

BvD-Fortbildungen & Veranstaltungen

BvD e.V.
DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Termin	Thema
BvD-Fortbildungen	
05.04.2023	**Online-Seminar: Werkzeugkasten für den DSB – Kontrollen und Analysen in der Datenschutzpraxis durchführen**
18.04.2023	**BvD-Blitzlicht: Big Data Best Practices – Wie Sie die Datenflut bewältigen und Sicherheitsrisiken minimieren**
20.04.2023	**Online-Seminar: Jura für Datenschutzbeauftragte: Rechtstexte verstehen**
27.04.2023	**BvD-Blitzlicht: Wie man als Datenschützer Websites auf Schwachstellen untersucht**
08.05.2023	**Sonderseminar: Beschäftigtendatenschutz** Berlin
08.05.2023	**Sonderseminar: Die datenschutzkonforme Umsetzung von MS365** Berlin
06.06.2023	**Seminar: Verantwortlicher, Auftragsverarbeiter oder Joint Controller – Was nun und wie dann?** Düsseldorf
21.06.2023	**BvD-Blitzlicht: Wie man als Datenschützer Websites auf Schwachstellen untersucht**
BvD-Veranstaltungen	
08.05.2023	**Ordentliche Mitgliederversammlung des BvD** Berlin
09. – 10.05.2023	**BvD-Verbandstage 2023** Berlin
05.07.2023	**2. Datenschutztag Hessen & Rheinland-Pfalz** Frankfurt/Main
18. – 20.10.2023	**BvD-Herbstkonferenz & Behördentag** München

JETZT ANMELDEN:
www.bvdnet.de/termine

Jetzt 3 Monate ZD kostenlos testen.

ZD – Zeitschrift für Datenschutz

13. Jahrgang. 2023. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 319,–
Vorzugspreis für BvD-Mitglieder, für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 245,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 17,– jährlich.

beck-shop.de/go/ZD

Die große Zeitschrift zum Datenschutz

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

Geschaffen für die Unternehmenspraxis

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

Alles inklusive:

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

3 Hefte gratis

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

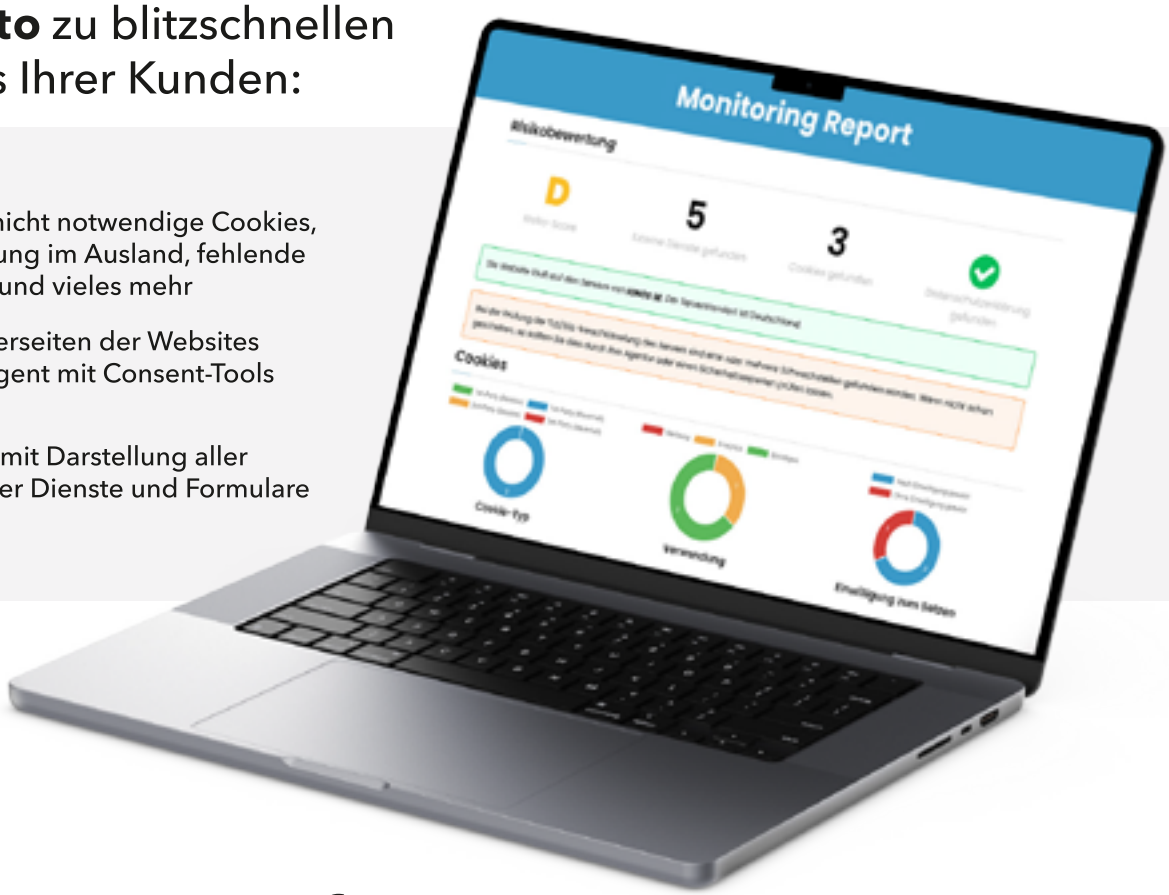
Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 173613
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK

Websites manuell auf Datenschutzlücken zu durchsuchen ist Vergangenheit!

Mit **decareto** zu blitzschnellen DSGVO-Scans Ihrer Kunden:

- decareto prüft nicht notwendige Cookies, Datenverarbeitung im Ausland, fehlende Einwilligungen und vieles mehr
- durchsucht Unterseiten der Websites und geht intelligent mit Consent-Tools um
- erstellt Reports mit Darstellung aller Cookies, externer Dienste und Formulare



Sind Sie bereit dafür, Ihre Zeit besser zu nutzen?

- Mit dem **Report in Ihrem eigenen Branding** können Sie Ihrer Prüfpflicht nachkommen und Ihren Kunden fachliche Kompetenz demonstrieren.
- Unser DSGVO-Scanner erledigt zeitaufwändige Website-Prüfungen, damit Sie **Freiraum für anspruchsvollere Arbeiten** haben.
- Unsere Website-Überwachung schützt Ihre Kunden vor Abmahnungen und Bußgeldern und **stärkt damit Ihre Kundenbindung**.
- Prüfen Sie ohne viel Aufwand potentielle Neukunden auf Datenschutzlücken und erhöhen Sie Ihre **Akquise-Power**.

decareto

Alle Informationen finden Sie auf **www.decareto.de**
Vereinbaren Sie noch heute einen **Beratungstermin** unter **decareto.de/demo** oder besuchen Sie unsere Website für eine kostenfreie **14-Tage-Testphase.**