# 25. Datenschutzbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

**Helga Block**

**für die Zeit vom 1. Januar 2019**

**bis zum 31. Dezember 2019**

Herausgeber:

Landesbeauftragte für Datenschutz und Informationsfreiheit

Nordrhein-Westfalen

Helga Block

Kavalleriestraße 2–4

40213 Düsseldorf

Tel.: 0211 / 384 24 - 0

Fax: 0211 / 384 24 - 10

E-Mail: poststelle@ldi.nrw.de

Diese Broschüre kann unter www.ldi.nrw.de abgerufen werden.

Zitiervorschlag: 25. DB LDI NRW

ISSN: 0179–2431

Düsseldorf 2020

Titelbild © psdesign1 – Fotolia.com

Gedruckt auf chlorfreiem Recyclingpapier

# Inhaltsverzeichnis

# Vorwort

Der **Blick zurück** auf den erstmals nur ein Jahr umfassenden Berichtszeitraum zeigt ein gemischtes Bild:

Die anfänglich bestehenden Unsicherheiten bei der Umstellung auf das neue von der Europäischen Union vorgegebene Recht wurden weitgehend überwunden. Die Aufsichtsbehörden konnten viele Grundsatzfragen zur Umsetzung der Datenschutz-Grundverordnung klären. Beim Zusammenspiel der europäischen Aufsichtsbehörden in grenzüberschreitenden Fällen wurden erste Erfahrungen gemacht.

Dennoch bleibt festzustellen, dass es noch viel Klärungsbedarf zu dem komplexen Regelwerk und zu seiner Anwendung in Einzelfällen gibt. Die im Jahr 2020 anstehende erste Bewertung und Überprüfung der Datenschutz-Grundverordnung durch die EU-Kommission bietet die Chance, Probleme aufzuzeigen und Änderungen anzuregen. Die deutschen Aufsichtsbehörden haben diese Chance genutzt und sich aktiv an der Evaluierung beteiligt. Ein von ihnen erstellter Bericht über ihre Praxiserfahrungen liegt der EU-Kommission vor. Der komplette Erfahrungsbericht findet sich im Anhang.

Im letzten Datenschutzbericht wurde über den enormen Anstieg von Anfragen und Beschwerden im Zusammenhang mit der EU-Reform berichtet, der meine Behörde an die Grenzen ihrer Leistungsfähigkeit gebracht hat. Trotz fortschreitender Klarstellung von unbestimmten Rechtsbegriffen und trotz der Anpassung vieler Datenverarbeitungsprozesse in Unternehmen und Behörden erreichen uns nach wie vor zahlreiche Eingaben. Deren Zahl ist im Jahr 2019 im Vergleich zum Vorjahr sogar noch etwas angestiegen. Der Schwerpunkt der Tätigkeiten lag somit auch im Jahr 2019 auf der Reaktion, denn die zum Teil fristgebundenen Beschwerden und Anfragen müssen prioritär bearbeitet werden. Die ohnehin knappen Personalressourcen reichten daher nicht aus, um unabhängig von Beschwerden Prüfungen und Kontrollen in angemessenem Umfang durchzuführen. Doch mit einigen Initiativprüfungen in verschiedenen Bereichen ist 2019 ein Anfang gelungen. In den kommenden Jahren gilt es, solche Aktivitäten zu verstetigen.

Der Blick zurück ist auch Anlass, Danke zu sagen: Ich danke meinen Mitarbeiterinnen und Mitarbeitern, die auch im Berichtszeitraum wieder mit viel Engagement und Sachverstand die täglichen Herausforderungen gemeistert haben. Dankbar bin ich auch für die gute Zusammenarbeit mit den Ressorts der Landesregierung, die trotz manch unterschiedlicher Lösungsansätze immer konstruktiv und kollegial war. Mein Dank gilt ebenfalls den Abgeordneten des Landtages, die unsere Behörde 2019 wiederum mit Planstellen und Sachmitteln verstärkt haben.

Der **Blick nach vorn** bietet reichlich Stoff für die Agenda in der nächsten Zeit:

Im Landesrecht stehen noch weitere Anpassungen von bereichsspezifischen Gesetzen an das europäische Recht an. Hier sind Landtag und Landesregierung gefordert.

Die Landesregierung sollte im Bundesrat darauf hinwirken, dass endlich ein Ländervertreter gewählt wird, der im Europäischen Datenschutzausschuss neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an den Sitzungen des Ausschusses teilnimmt. So sieht es das Bundesdatenschutzgesetz vor, doch seit zwei Jahren tagt der Europäische Datenschutzausschuss, ohne dass ein Ländervertreter gewählt ist.

In erster Linie ist es die Aufgabe der Landesbeauftragten für Datenschutz und Informationsfreiheit, die Einhaltung der datenschutzrechtlichen Regeln im Lande NRW zu überwachen und durchzusetzen und den Bürgerinnen und Bürgern, der öffentlichen Verwaltung und der Wirtschaft mit Rat und Tat bei allen Fragen des Datenschutzes zur Seite zu stehen. Die Vorlage dieses Berichtes fällt angesichts der Corona-Pandemie in eine Krisenzeit, in der die Freiheitsrechte durch Maßnahmen der Gesundheitsfürsorge stark eingeschränkt werden. Der Schutz der Grundrechte, zu denen auch das Recht auf informationelle Selbstbestimmung gehört, ist auch und gerade in einer solchen schweren Krise ein wesentliches Merkmal unserer freiheitlich-demokratischen Grundordnung, die es zu schützen gilt.

Im Jahr 2020 steht für die Behörde ein Wechsel in der Leitung an, da ich in den gesetzlichen Ruhestand treten werde.

Der zukünftigen Leitung und allen meinen Mitarbeiterinnen und Mitarbeitern wünsche ich viel Erfolg und Freude bei der Amtsführung.

Helga Block

Frühjahr 2020

# 1. Überblick

- **Entwicklung der Eingaben**

Das Jahr 2018 war von der Umstellung auf das neue europäische Datenschutzrecht geprägt. Erwartungsgemäß gab es bei allen Aufsichtsbehörden eine Flut von Anfragen und Eingaben jeglicher Art.

Viele Grundsatzfragen zur Umsetzung der DS-GVO wurden inzwischen von den Aufsichtsbehörden geklärt. Deshalb bestand zu Beginn des Jahres 2019 die Erwartung, dass die Zahl der Eingaben an uns rückläufig sein werde.

Doch das war nicht der Fall: Im Jahr 2019 haben uns über **12.500 Eingaben** erreicht. Damit sind die Eingaben gegenüber dem Jahr 2018 (rund 12.000) sogar noch einmal angestiegen.

Es gibt immer noch viele Fragen zu dem komplexen Regelwerk der DS-GVO und seiner Anwendung im Einzelfall. Außerdem ist ganz allgemein das Bewusstsein für das Datenschutzrecht und seine Geltendmachung gestiegen.

Weitere Einzelheiten zur statistischen Entwicklung finden sich unter 2. im Kapitel „Zahlen und Fakten“.

Unser Bestreben ist es nach wie vor, alle Eingaben im Rahmen unserer Kapazität zeitnah zu bearbeiten. Das ist leider nicht immer möglich, sodass wir bei der Bearbeitung neben der Einhaltung gesetzlicher Fristen vorrangig die Schwere der geltend gemachten Verstöße und das Risiko der Datenverarbeitung berücksichtigen müssen.

- **Entwicklung des europäischen Rechts – Evaluation der Datenschutz-Grundverordnung**

Die DS-GVO verpflichtet die EU-Kommission dazu, dem Europäischen Parlament und dem Rat bis zum 25. Mai 2020 einen Bericht über die Bewertung und Überprüfung der Verordnung vorzulegen. Diese Evaluation bietet die Chance, Probleme zu erkennen – seien es Unklarheiten, Regelungslücken oder Überregulierungen – und Verbesserungsmöglichkeiten anzuregen. Die Aufsichtsbehörden haben sich an der vorgesehenen Evaluierung beteiligt und einen Bericht erstellt, der die gemeinsame Sicht der deutschen Behörden darstellt. Es obliegt nun dem europäischen Gesetzgeber, die Erkenntnisse aus der Evaluation auch konsequent für die Überarbeitung der DS-GVO zu nutzen. Siehe hierzu unter 3.

- **Beratung öffentlicher Stellen**

Die Beratung öffentlicher Stellen in Fragen des Datenschutzes und der Datensicherheit ist uns weiterhin ein wichtiges Anliegen. Wie bereits im 24. Bericht in Aussicht gestellt, haben wir unser Beratungsangebot aufrechterhalten und durch zusätzliche Veranstaltungen weiter ausgebaut. Siehe hierzu unter 11.1.

- **Innere Sicherheit**

**Strategische Fahndung**

Beim ersten Einsatz des neuen polizeilichen Mittels der sog. „Strategischen Fahndung“ ergab unsere stichprobenhafte Prüfung, dass die Daten sehr vieler Personen kontrolliert wurden, ohne dass diese hierzu einen Anlass gegeben hätten. Der angestrebte polizeiliche Erfolg

der Gefahrenabwehr wurde dabei jedoch nicht erreicht. Was geblieben ist, sind die zahlreichen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen. Siehe hierzu unter 10.2.

**Zentrales Fahndungsportal der Polizei**
Öffentlichkeitsfahndungen nach gesuchten Straftäterinnen und -tätern oder vermissten Personen werden von der Polizei im Zentralen Fahndungsportal veröffentlicht. Nach anfänglichen Auffälligkeiten in mehreren Einzelfällen wurde das System korrigiert. Es ist nunmehr datenschutzgerecht ausgestaltet. Siehe hierzu unter 10.3.

- **Internet und Medien**

**Betrieb von Facebook-Fanpages**
Auf der Basis der Entscheidungen des EuGH und des BVerwG zur gemeinsamen Verantwortlichkeit von Facebook und Betreibern einer im sozialen Netzwerk unterhaltenen Fanpage vertritt die LDI NRW weiterhin nachdrücklich ihre kritische Position gegenüber den Betreibern, wobei behördlichen Fanpagebetreibern eine Vorbildfunktion zukommt. Da das Thema jedoch auch bundes- und europaweite Relevanz hat, werden die Entwicklungen auf diesen Ebenen zunächst abgewartet, bevor in NRW über weitere Schritte zu entscheiden sein wird. Bürgerinnen und Bürger sollten sich umfassend informieren und bewusst entscheiden, ob sie ein solches Netzwerk nutzen wollen. Siehe hierzu unter 4.2.

**Datenverarbeitung durch natürliche Personen**
Mit dem Ziel natürliche Personen zu schützen, nimmt die DS-GVO den so genannten „Verantwortlichen“, also den Veranlasser der Datenverarbeitung in die Pflicht. Datenschutzrechtliche Vorgaben sind nicht nur etwa von Unternehmen und Behörden zu beachten. Auch natürliche Personen sind nach der DS-GVO Verantwortliche, sobald sie nicht mehr unter das so genannte „Haushaltsprivileg“ fallen. Darunter versteht man eine Verarbeitung von Daten ausschließlich für persönliche oder familiäre Tätigkeiten. Bei der Veröffentlichung von personenbezogenen Daten Dritter im Internet, etwa bei Facebook, Instagram oder Twitter, ist in der Regel die DS-GVO anzuwenden. Siehe hierzu unter 4.7.

- **Datenschutz und Wirtschaft**

**Beratung**
Der Beratungsbedarf zur Datenschutzreform im Bereich der Wirtschaft ist nach wie vor sehr hoch. Neben unserer täglichen Beratungstätigkeit zu verschiedenen Einzelfragen aus der Praxis haben wir auf zahlreichen Veranstaltungen über die DS-GVO informiert. Zudem haben wir zu häufig angefragten Themen unsere Homepage um weitere Informationen ergänzt. Siehe hierzu unter 5.1.

**Änderung der Voraussetzungen für die Pflicht zur Benennung von betrieblichen Datenschutzbeauftragten**
Das Bundesdatenschutzgesetz wurde in einem wichtigen Punkt geändert: Erst wenn **20** Personen in einem Betrieb ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, muss ein Datenschutzbeauftragter benannt werden. Nach altem Recht bestand diese Pflicht schon ab einer entsprechenden Personenzahl von 10**.**

Auch bei Wegfall einer solchen Pflicht raten wir dazu, am Datenschutzbeauftragten festzuhalten: Die datenschutzrechtlichen Vorgaben müssen ohnehin eingehalten werden, und die fachliche Expertise eines Datenschutzbeauftragten schützt vor Sanktionsrisiken und stärkt das Vertrauen der Kundschaft in die Unternehmen. Siehe hierzu unter 5.2.

**Akkreditierungskriterien für CoC-Überwachungsstellen mit Sitz in Deutschland**

Mit Verhaltensregeln (Codes of Conduct) nach Art. 40, 41 DS-GVO wird es Wirtschafts- und Branchenverbänden ermöglicht, die abstrakten und allgemeinen Vorgaben der DS-GVO durch Verhaltensregeln sektor- und branchenspezifisch auszufüllen – Konzept der regulierten Selbstregulierung. Verhaltensregeln vereinfachen somit die wirksame Anwendung der DS-GVO und geben hierdurch Rechtssicherheit. Die Einhaltung der Verhaltensregeln wird durch unabhängige CoC-Überwachungsstellen der Wirtschaft kontrolliert. Sie müssen von der zuständigen Aufsichtsbehörde vorher akkreditiert werden. Dazu haben die deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder branchenunabhängig einheitliche Akkreditierungskriterien entwickelt und dem EDSA zur Stellungnahme vorgelegt. Siehe hierzu unter 5.3.

**Smart Metering – Digitale und intelligente Stromzähler**

Die flexible Nutzung erneuerbarer Energien bedarf intelligenter Energieversorgungsnetze. Stromnachfrage und wetterabhängige Stromeinspeisung sind dabei in Einklang zu bringen. Helfen sollen digitale und intelligente Stromzähler. Ihr Einbau und Betrieb wird jedoch nicht selten skeptisch gesehen, ist doch die private Wohnsphäre betroffen. Dazu erreichen uns häufig Fragen. Siehe hierzu unter 5.6.

- **Verein und Ehrenamt**

Auch in Vereinen und im Ehrenamt ist der Beratungsbedarf immer noch hoch. Gleiches gilt für die Zahl der Beschwerden. In der täglichen Beratungspraxis konnten wir viele Fragen klären und versachlichen. Unser praxisorientierter Ratgeber: „Datenschutz im Verein nach der DS-GVO“ mit Fallbeispielen und Mustertexten wird unverändert häufig nachgefragt. Zudem haben wir mehrere Vorträge zu speziellen Fragen des Datenschutzes im Verein und im Ehrenamt, aber auch allgemein zur Datenschutzaufsicht und zum neuen Datenschutzrecht gehalten.

- **Informationen und Öffentlichkeitsarbeit**

Um dem Informationsbedarf über den Einzelfall hinaus Rechnung zu tragen, haben wir unser Informationsangebot auf unserer Internetseite www.ldi.nrw.de zu aktuellen Entwicklungen erweitert und zahlreiche Broschüren, Orientierungshilfen und Muster veröffentlicht.

Veröffentlichungen der Datenschutzkonferenz sind auch auf der gemeinsamen Internetseite www.datenschutzkonferenz-online.de abrufbar.

Wir beteiligen uns weiterhin am **Virtuellen Datenschutzbüro** www.datenschutz.de, das Bürgerinnen und Bürgern als erste zentrale Informations- und Anlaufstelle dient. Insbesondere um Jugendliche zu erreichen beteiligen wir uns

zudem an der Webseite **www.young-data.de**.

- **Datenschutzkonferenz und Expertengruppen des Europäischen Datenschutzausschusses**

Im Jahr 2019 fanden mehrere Termine der **Datenschutzkonferenz** statt. Zudem haben wir an zahlreichen Sitzungen der Arbeitskreise der Datenschutzkonferenz teilgenommen.

Wir leiten, wie schon in den Vorjahren, die Arbeitskreise Wirtschaft (vormals Düsseldorfer Kreis), Statistik, Kreditwirtschaft und – gemeinsam mit Hessen – den Arbeitskreis Auskunfteien.

Der Europäische Datenschutzausschuss hat zu seiner Unterstützung mehrere Ausschüsse – sog. Expert Subgroups – gebildet, in denen auch die nationalen Aufsichtsbehörden vertreten sind. Die LDI NRW ist in der Key Provisions Expert Subgroup und in der Financial Matters Expert Subgroup des Europäischen Datenschutzausschusses aktiv.

- **Anlasslose Prüfungen**

Die starke Nachfrage nach Beratung zur Umsetzung der DS-GVO und die massiv angestiegenen Eingaben haben unsere Arbeitskraft mehr als gebunden. Leider reichten dadurch die Personalkapazitäten nicht aus, um unabhängig von Beschwerden wieder – wie zuvor – vermehrt Kontrollen und Prüfungen durchzuführen.

Aber ein Anfang ist gemacht: Im Jahr 2019 haben wir mit einigen Initiativprüfungen begonnen.

Folgende Prüfverfahren befinden sich in verschiedenen Verfahrensstadien:

- **Abrechnungspraxis von privatärztlichen Abrechnungsunternehmen**. Siehe unter 9.7.
- **Einhaltung datenschutzrechtlicher Vorgaben bei Banken, Versicherungen und Versorgungsunternehmen**. Siehe unter 5.9.
- **Beschäftigtendatenschutz bei Personaldienstleistern und Leiharbeitsunternehmen**. Siehe unter 6.3.
- **Nutzung von Internethandelsplattformen durch Apotheken**. Siehe unter 9.6.
- **Datenschutzbeauftrage bei Jobcentern der Kommunen**. Siehe unter 11.3.
- **Videoüberwachung bei Großbäckereien**. Siehe unter 7.3.

# 2. Zahlen und Fakten

Die Pflicht jeder Aufsichtsbehörde zur Erstellung eines Jahresberichtes ergibt sich unmittelbar aus der DS-GVO (Art. 59). Zu den Inhalten dieser jährlichen Berichte enthält die DS-GVO lediglich optionale Vorschläge.

Eine Vergleichbarkeit unter den Mitgliedstaaten ist wegen der ganz unterschiedlichen Strukturen und Situationen nur sehr bedingt möglich. Innerhalb Deutschlands hat die Datenschutzkonferenz sich in Bezug auf die Darstellung von bestimmten Zahlen und Fakten auf einige Kriterien zur statistischen Darstellung in den ansonsten ganz unterschiedlichen Berichten der Aufsichtsbehörden verständigt.

Vor diesem Hintergrund berichtet auch die LDI NRW in diesem ersten Jahresbericht nach der DS-GVO ausführlicher als bisher über Anzahl und Art der angefallenen Tätigkeiten.

- **Eingabesituation**

Im Jahr **2019** haben uns insgesamt über **12.500** schriftliche Eingaben erreicht – im Jahr 2018 waren es gerundet 12.000, im Jahr 2017 etwa 4.400. Grundsätzlich nicht erfasst haben wir dabei die zahlreichen telefonischen Anfragen.

Von den über 12.500 schriftlichen Eingaben in 2019 waren **2.235** Meldungen nach Art. 33 DS-GVO zu sog. Datenpannen.

Von den übrigen Eingaben waren etwa 80 Prozent Beschwerden nach Art. 77 DS-GVO und etwa 20 Prozent Beratungsanfragen.

- **Beschwerden und Beratungsanfragen**

Eine Beschwerde liegt nach Art. 77 DS-GVO vor, wenn eine Person vorträgt, dass ein sie persönlich verletzender Verstoß gegen datenschutzrechtliche Bestimmungen vorliegt. Nicht umfasst von dieser Definition sind Eingaben, die auf mutmaßliche Datenschutzverstöße hinweisen, von denen die Einsendenden jedoch nicht selbst betroffen sind. Ab 2020 werden wir derartige Eingaben wie auch weitere Unterkategorien von Eingaben differenzierter erfassen.

Der ganz überwiegende Teil der Beschwerden, nämlich weit über 80 Prozent, richtet sich gegen Datenverarbeitungen im nicht-öffentlichen Bereich, das heißt die Verantwortlichen sind kleine, mittlere und große Unternehmen vieler Wirtschaftszweige, Selbständige unter anderem aus dem Dienstleistungsbereich wie Mediendienste, Rechtsanwälte und Steuerberater sowie Vereine und auch Privatpersonen.

Schriftliche Beratungsanfragen haben wir sowohl von Verantwortlichen als auch von Auftragsverarbeitern, betroffenen Personen und auch von der öffentlichen Verwaltung auf Landes- und Kommunalebene erhalten.

- **Meldungen von Datenschutzverletzungen**

Eine Verletzung des Schutzes personenbezogener Maßnahmen, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, eine sog. **Datenpanne,** muss der Verantwortliche un-

verzüglich und möglichst binnen 72 Stunden der zuständigen Aufsichtsbehörde melden (Art. 33 DS-GVO).

Im Jahr 2019 wurden uns **2.235** solcher (vermeintlicher) Datenpannen gemeldet.

Der mit den in Art. 33 und 34 DS-GVO eingeführten Melde- und Benachrichtigungspflichten verbundene Aufwand ist erheblich – sowohl für die Verantwortlichen, als auch für die LDI NRW. Anfang des Jahres 2020 haben wir deshalb ein elektronisches Meldeportal eingerichtet. Ziel ist neben der Reduktion des Aufwands auch eine Verbesserung der Servicequalität bezogen auf die Einreichung und Bearbeitung der Meldungen. Siehe hierzu unter 12.1.

- **Abhilfemaßnahmen**

Um eine einheitliche Überwachung und Durchsetzung der DS-GVO sicherzustellen, werden den Aufsichtsbehörden in Art 58 Abs. 2 DS-GVO einheitliche Abhilfebefugnisse eingeräumt.

Von den dort genannten Abhilfemaßnahmen wurden von der LDI NRW Insgesamt **242** Maßnahmen ergriffen. Davon waren 73 Geldbußen gemäß Art. 58 Abs. 2 Buchstabe i DS-GVO. Dazu im Einzelnen:

Um eine weitgehend einheitliche Linie bei der Verhängung von Bußgeldern zu erzielen, hat LDI NRW im Jahr 2019 eine Zentrale Bußgeldstelle zur Ahndung von Ordnungswidrigkeiten eingerichtet. Kriterien für die Entscheidung, ob und in welcher Höhe ein Bußgeld verhängt werden soll, enthält Art. 83 Abs. 2 DS-GVO. Geahndet wurden im Jahr 2019 eine Vielzahl von Verstößen gegen die Auskunftspflicht gegenüber der LDI NRW, wie auch gegenüber betroffenen Personen, die unzulässige Bereitstellung und/oder Weitergabe von Daten ohne erforderliche Sicherung, die unzulässige Entsorgung personenbezogener Daten, zum Beispiel Patientendaten und Daten von Beschäftigten, sowie die Datenverarbeitung mit Hilfe von Dashcams.

Im Jahr 2019 wurden bei der Zentralen Bußgeldstelle 123 Verfahren eingeleitet. Die Verfahren sind zum Teil noch nicht abgeschlossen. Insgesamt wurden 73 Verfahren mit einem Bußgeldbescheid beendet. Die Höhe der Bußgelder reicht von 100 bis 1.500 Euro.

Ein Wort zur Erläuterung der Abhilfemaßnahmen: Im Vergleich zur Anzahl der Beschwerden fällt die Anzahl der ergriffenen Abhilfemaßnahmen gering aus. Das erklärt sich zum einen damit, dass die LDI NRW nach wie vor im Kontakt mit den Verantwortlichen den Schwerpunkt auf Beratung und Sensibilisierung setzt. Häufig können so einvernehmliche, konstruktive Lösungen gefunden werden, die nicht nur den Einzelfall datenschutzgerecht lösen, sondern auch für die zukünftige Praxis der Verantwortlichen einen Gewinn für den Datenschutz bedeuten.

Zum anderen sind viele Verfahren sehr aufwändig sowohl in zeitlicher wie in inhaltlicher Hinsicht. Nicht selten bedarf es vieler Kontakte und umfangreichen Schriftwechsels bis es am Ende zu einer Abhilfemaßnahme etwa in Form eines Bußgeldbescheides kommt. Daher wurden viele im Jahr 2019 begonnene Verfahren 2019 noch nicht beendet. Erst wenn diese abgeschlossen sind, können

die getroffenen Abhilfemaßnahmen in der nächsten statistischen Darstellung Berücksichtigung finden.

- **Europäische Verfahren**

Die DS-GVO bestimmt Verfahren für eine europäische Meinungsbildung und Entscheidungsfindung der Datenschutzaufsichtsbehörden. Das einheitliche europäische Recht soll in den Mitgliedstaaten auch einheitlich angewendet werden. Da die Regelungen der DS-GVO oft allgemein gehalten sind, haben die Aufsichtsbehörden die Aufgabe, das neue Recht in der Interpretation und in der Praxis zu harmonisieren. Dazu müssen sich die Behörden abstimmen und – teils verbindliche – Rechtsauffassungen entwickeln. Die Meinungsbildung der europäischen Aufsichtsbehörden findet in Abstimmungsverfahren der betroffenen Behörden untereinander und im Europäischen Datenschutzausschuss statt.

Für viele Abstimmungsprozesse wird das Binnenmarkt-Informationssystem (Internal Market Information System – IMI) als IT-Plattform eingesetzt. Die Plattform IMI unterstützt die Verfahren der Zusammenarbeit und Kohärenz über komplexe Module. Wird ein Modul in IMI gestartet, generiert das System eine automatische Benachrichtigung, die bei der empfangenden Behörde bearbeitet werden muss. Arbeitssprache in IMI ist Englisch.

Unter anderem tauschen sich die betroffenen Aufsichtsbehörden über grenzüberschreitende Fälle aus und stimmen Entscheidungen ab. Geht beispielsweise bei uns eine Beschwerde in Bezug auf eine grenzüberschreitende Datenverarbeitung ein, leiten wir als Eingangsbehörde die ersten notwendigen Schritte über IMI in die Wege.

Im Jahr 2019 war die LDI NRW **1390**-mal mit gestarteten IMI-Modulen befasst.

- **Förmliche Begleitung bei Rechtsetzungsvorhaben**

Im Jahr 2019 wurde die LDI NRW bei **21** Rechtsetzungsvorhaben beteiligt.

Dabei wurden wir in unterschiedlicher Intensität und in verschiedenen Phasen der Verfahren vor der Einbringung in den Landtag oder als Sachverständige im Rahmen von Anhörungen im Landtag insbesondere bei den folgenden Gesetzesvorhaben tätig:

- Gesetz zur Stärkung der Rechte von im Polizeigewahrsam festgehaltenen Personen (ehemals 7. Änderungsgesetz zum Polizeigesetz NRW)
- Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (E-Government-Gesetz Nordrhein-Westfalen – EGovG NRW)
- Schulgesetz NRW nebst schulrechtlichen Verordnungen
- Gesetz über die Sicherung und Nutzung öffentlichen Archivguts im Lande Nordrhein-Westfalen (Archivgesetz Nordrhein-Westfalen – ArchivG NRW)
- Umsetzungsgesetz zum 3. Staatsvertrag zur Änderung des Glücksspielstaatsvertrags in NRW

- Maßregelvollzugsgesetz NRW (MRVG)
- Gutachterausschussverordnung NRW
- Verordnung über die Zulassung der Datenübermittlung von Meldebehörden an andere Behörden oder sonstige öffentliche Stellen des Landes Nordrhein-Westfalen (Meldedatenübermittlungsverordnung – Meld-DÜV NRW)
- Statistikgesetz Nordrhein-Westfalen (LStatG NRW)
- Gesetz zur frühen Bildung und Förderung von Kindern (Kinderbildungsgesetz – KiBiz)
- Viertes Gesetz zur Ausführung des Kinder- und Jugendhilfegesetzes (SGB VIII)
- Pflegekammergesetz
- Gesetz über die klinische und epidemiologische Krebsregistrierung im Land Nordrhein – Westfalen (Landeskrebsregistergesetz – LKRG NRW)
- Gesetz über die Zulassung öffentlicher Spielbanken im Land Nordrhein-Westfalen (Spielbankgesetz NRW – SpielbG NRW)

Unsere Hinweise wurden vielfach aufgegriffen und umgesetzt. Ein Fokus unseres Tätigwerdens in diesem Bereich lag dabei weiterhin auf der Aufrechterhaltung des vor der DS-GVO und der JI-Richtlinie bestehenden Datenschutzniveaus in NRW.

Die LDI NRW ist frühzeitig über Entwürfe für Rechts- und Verwaltungsvorschriften zu unterrichten, wenn diese eine Verarbeitung personenbezogener Daten vorsehen (vgl. § 27 Abs. 5 Satz 2 Datenschutzgesetz NRW). Dies soll sicherstellen, dass wir die vorgesehenen Neuregelungen hinreichend gründlich prüfen und ggf. eingehend beratend tätig werden können. Diese Aufgabenwahrnehmung wird nicht selten dadurch erschwert, dass eine Rückmeldung innerhalb weniger Tage erwartet wird.

# 3. Evaluation der Datenschutz-Grundverordnung

**Die Datenschutz-Grundverordnung (DS-GVO) sieht vor, dass die EU-Kommission 2020 einen Bericht über die Bewertung und Überprüfung dieser Verordnung vorlegt. Die deutschen Aufsichtsbehörden beteiligen sich an dieser vorgesehenen Evaluierung. Dazu hat die Datenschutzkonferenz (DSK) einen Bericht erstellt, der die gemeinsame Sicht der Behörden darstellt.**

Die DS-GVO hat zwar einige Änderungen bewirkt, diese haben sich jedoch in der Praxis als nicht ganz so einschneidend herausgestellt, wie von vielen Seiten befürchtet. Es lohnt sich aber, dieses noch junge Regelwerk mit weitreichenden Auswirkungen und umstrittener Entstehungsgeschichte einer genaueren Überprüfung zu unterziehen.

Bis zum Mai 2020 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung der Verordnung vor (Art. 97 DS-GVO). Dazu kann sie Informationen unter anderem von den Aufsichtsbehörden anfordern. Die europäischen Aufsichtsbehörden koordinieren sich auch zu diesen Fragen im Europäischen Datenschutzausschuss. Die DSK hat einen gemeinsamen Bericht zur Evaluation der DS-GVO erstellt. Diesen Erfahrungsbericht hat die DSK dem Europäischen Datenschutzausschuss übersandt. Er liegt auch der EU-Kommission vor.

Der Erfahrungsbericht befasst sich mit folgenden Schwerpunkten, zu denen teils konkrete Änderungsvorschläge gemacht werden:

- **Alltagserleichterung und Praxistauglichkeit**

Informations- und Transparenzpflichten sind einerseits wichtig für die betroffenen Personen, andererseits belastend für die Daten verarbeitenden Stellen. Die Informationspflichten sollten risikogerecht so nachjustiert werden, dass die Stellen praxisgerecht entlastet werden, ohne dass die Interessen der betroffenen Personen beeinträchtigt werden. Es sollte zudem klargestellt werden, wie umfangreich der Anspruch auf eine Kopie ist. Die Meldepflicht der Kontaktdaten von Datenschutzbeauftragten bei der Aufsichtsbehörde kann entfallen, ohne dass damit eine Verschlechterung verbunden wäre, da diese Kontaktdaten ohnehin veröffentlicht werden müssen.

- **Datenpannenmeldungen**

Die Pflicht, Datenpannen zu melden, sollte risikogerechter gestaltet werden: Einerseits sollten "Kleinigkeiten" – also Schutzverletzungen mit geringem Gefährdungspotenzial – nicht gemeldet werden müssen. Andererseits sollte eine Pflicht auch dann bestehen, wenn nicht bekannt ist, ob tatsächlich eine Verletzung stattgefunden hat, dies aber wahrscheinlich ist.

**Zweckbindung**

Die Beschränkung der Verarbeitungserlaubnis auf bestimmte, im Vorhinein festgelegte Zwecke ist aus Sicht der betroffenen Personen ein besonders wichtiges Prinzip. Unklarheiten bei der Regelung

zur Reichweite der – ausnahmsweise – erlaubten Zweckänderung sollten daher beseitigt werden.

- **Data protection by design**

Die Pflicht zum Datenschutz durch Technikgestaltung haben bisher nur die Verantwortlichen. Die Pflicht sollte auch auf Hersteller, Lieferanten, Importeure und Verkäufer erstreckt werden, um das Schutzziel zu erreichen. Für Verantwortliche und Verbraucherinnen und Verbraucher würde es dann einfacher, datenschutzfreundliche Produkte einzusetzen.

- **Befugnisse der Aufsichtsbehörden und Sanktionspraxis**

Hier bestehen einige Unklarheiten, deren Beseitigung helfen würde, die Datenschutzvorschriften besser durchsetzen zu können.

- **Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz**

Klarstellungen in Verfahrensfragen und etwas längere Fristen für die Zusammenarbeit würden dabei helfen, die neuen Verfahren zwischen den Aufsichtsbehörden in den Mitgliedstaaten und dem Europäischen Datenschutzausschuss reibungslos durchzuführen.

- **Direktwerbung**

Von Direktwerbung sind europaweit viele Verbraucherinnen und Verbraucher betroffen, die Mitgliedstaaten haben dabei aber unterschiedliche Traditionen. Gesetzliche Vorgaben in der DS-GVO sollten deshalb einen europäischen Rahmen für Direktwerbung vorgeben.

- **Profiling**

Das mit der Bildung von persönlichen Profilen verbundene Risiko für die Betroffenen ist eines der zentralen datenschutzpolitischen Themen. Die DS-GVO sollte dazu einen verschärften Rechtsrahmen mit effektivem Rechtsschutz und durchsetzbaren Grenzen schaffen.

- **Akkreditierung**

Die Aufgabenverteilung zwischen Datenschutzaufsichtsbehörden und Deutscher Akkreditierungsstelle sollte klargestellt werden.

Zusätzlich zu diesen Schwerpunkten hat die DSK weitere Änderungsvorschläge festgehalten und auf die Hambacher Erklärung zur Künstlichen Intelligenz hingewiesen.

Der gesamte „Erfahrungsbericht der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Anwendung der DS-GVO“ ist im Anhang abgedruckt.

Die Evaluation der DS-GVO ist wichtig, weil das Regelwerk europaweit unmittelbare Wirkung hat und in der Entstehung in vielen Bereichen umstritten war. Die Evaluation bietet die Chance, Probleme zu erkennen – seien es Unklarheiten, Regelungslücken oder Überregulierungen – und Verbesserungsmöglichkeiten anzuregen. Die Aufsichtsbehörden können hier nur Vorschläge machen. Es obliegt dann dem europäischen Gesetzgeber, die Erkenntnisse aus der Evaluation auch konsequent für die Überarbeitung der DS-GVO zu nutzen.

# 4. Internet und Medien

## 4.1 Gerichtsentscheidungen

**Bundesverwaltungsgericht zu Facebook-Fanpages**

Das Bundesverwaltungsgericht hat bestätigt, dass Facebook-Fanpage-Betreiber verpflichtet werden können, ihre Fanpages abzuschalten, falls die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist. Siehe hierzu unter 4.2.

**Europäischer Gerichtshof zur wirksamen Einwilligung in die Verwendung von Website-Cookies**

Der Europäische Gerichtshof hat wichtige Aussagen zu den Voraussetzungen der wirksamen Einwilligung in die Verwendung von Cookies im Internet getroffen. Siehe hierzu unter 4.5.

**Europäischer Gerichtshof zum Webmail-Dienst von Google (Gmail)**

Der Europäische Gerichtshof hat entschieden, dass der Webmail-Dienst Gmail kein elektronischer Kommunikationsdienst ist. Webmaildienste wurden von den deutschen Datenschutzaufsichtsbehörden bislang als Telekommunikationsdienste angesehen, was nun nicht mehr möglich ist. Siehe hierzu unter 4.6.

## 4.2 Aktueller Stand zum Betrieb von Facebook-Fanpages

**Das Bundesverwaltungsgericht (BVerwG) hat entschieden, dass Facebook-Fanpage-Betreiber verpflichtet werden können, ihre Fanpages abzuschalten, falls die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist (Urteil vom 11. September 2019, Az. 6 C 15.18).**

Das Urteil des BVerwG erging auf der Grundlage des Urteils des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018 (Az. C-210/16). Der EuGH hatte hierin aufgrund der entsprechenden Vorlagefragen des BVerwG entschieden, dass der Betreiber einer Fanpage für die durch Facebook erfolgende Datenverarbeitung mitverantwortlich ist, da er durch den Betrieb der Fanpage den Zugriff auf die Daten der Fanpage-Besucher durch Facebook ermöglicht.

Beide Gerichte bestätigen die Auffassung der Datenschutzkonferenz (DSK). In ihrer Entschließung vom 6. Juni 2018 und zuletzt in ihrer Positionierung vom 1. April 2019 hat die DSK deutlich gemacht, welche Konsequenzen sich aus der gemeinsamen Verantwortlichkeit ergeben – insbesondere für die Betreiberinnen und Betreiber einer Fanpage. Bei einer gemeinsamen Verantwortlichkeit ist nach der Datenschutz-Grundverordnung (DS-GVO) unter anderem durch die Beteiligten eine Vereinbarung abzuschließen, die klarstellt, wie die Pflichten aus der DS-GVO erfüllt werden. Zudem fordert die DSK, dass Fanpage-Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DS-GVO nachweisen können müssen. Dies ergibt sich aus der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO sowie insbesondere in Bezug auf Verpflichtungen nach Art. 24, 25 und 32 DS-GVO.

Bislang fehlen ausreichend detaillierte und verbindliche Informationen über die Datenverarbeitung durch Facebook. Die Vorgaben des Art. 26 und 5 Abs. 2 DS-GVO sind auch mit der von Facebook im September 2018 eingestellten und seither auf Drängen der in Deutschland zuständigen Datenschutzbehörde mehrfach überarbeiteten sog. Seiten-Insights-Ergänzungen nicht erfüllt. Siehe 24. Bericht unter 2.2.

Wir stehen gegenwärtig in Kontakt mit Stellen, die Fanpages betreiben, und vertreten unsere Position in Bezug auf die Präsenz in Sozialen Netzwerken vor allem auch gegenüber öffentlichen Stellen nachdrücklich.

Das Thema hat jedoch nicht nur eine landesweite Relevanz, sondern auch bundes- und europaweite Aspekte. Auf diesen Ebenen wird es derzeit intensiv diskutiert. Darüber hinaus führen die deutschen Datenschutzaufsichtsbehörden regelmäßig Gespräche mit der deutschen Niederlassung von Facebook in Hamburg mit dem Ziel der datenschutzgerechteren Gestaltung der Fanpages. Dies hat bereits zu einigen Verbesserungen bei der Information der Nutzerinnen und Nutzer sowie der Betreiber von Facebook-Fanpages geführt. Die LDI NRW ist an diesem Diskussionsprozess intensiv beteiligt.

Wir werden die Entwicklungen auf den genannten Ebenen weiterverfolgen und auch künftig darauf hinwirken, dass insbesondere die sich aus der gemeinsamen Verantwortlichkeit ergebenden Fragen auf nationaler, aber auch auf europäischer Ebene weiter geklärt werden. Bevor über weitere Schritte – auch in NRW – zu entscheiden sein wird, wollen wir zunächst die Ergebnisse des laufenden Diskussionsprozesses abwarten.

Die Entscheidung des BVerwG bestätigt ebenso wie bereits das EuGH-Urteil die Auffassung der DSK. Die LDI NRW vertritt ihre kritische Position gegenüber Fanpage-Betreibern in NRW nachdrücklich. Das Thema hat jedoch auch bundes- und europaweite Relevanz. Daher werden die Entwicklungen auf diesen Ebenen zunächst weiterverfolgt und die Ergebnisse des laufenden Diskussionsprozesses abgewartet, bevor über weitere Schritte – auch in NRW – zu entscheiden sein wird.

## 4.3 Einbindung von Social Plugins auf Websites: Wichtige Entscheidung des EuGH

**Websitebetreiber, die sog. Social Plugins wie den Facebook-Like-Button in ihre Website mit einbinden, sind gemeinsam mit den Plugin-Anbietern für die Datenverarbeitung verantwortlich, die aufgrund der Einbindung dieses Plugins erfolgt. Das hat der Europäische Gerichtshof (EuGH) mit Urteil vom 29 Juli 2019 (Az. C-40/17) entschieden. Wer also mit solchen Plugins die Wahrnehmung seiner Website erhöhen will und durch das „Liken" der Nutzerinnen und Nutzer für sein Angebot werben will, muss darauf achten, dass dabei die Datenschutzrechte der Nutzerinnen und Nutzer gewahrt werden.**

Bei der Einbindung von Social Plugins raten wir Websitebetreibern seit Langem dazu, den von den Sozialen Netzwerken bereitgestellten Code nicht ungeprüft in ihre Websites einzubinden. Die damit verbundene Datenverarbeitung ist nämlich unzulässig, wenn die Einbindung nicht auf datenschutzrechtlich korrekte Weise erfolgt. Die Websitebetreiber können dafür in Anspruch genommen werden.

Problematisch ist es insbesondere, wenn bereits beim Aufruf der Website ohne Wissen der Nutzerinnen oder Nutzer Informationen über den Aufruf der Website an das Soziale Netzwerk übertragen werden. Um einen solchen Fall ging es auch in dem Klageverfahren der Verbraucherzentrale NRW gegen eine nordrhein-westfälische Online-Händlerin, in dem wir von den Gerichten beteiligt wurden. Zum Sachverhalt und zum Verfahren siehe im 24. Bericht unter 2.3 sowie im 23. Bericht unter 12.5.

Dabei wurden dem EuGH verschiedene Fragen zur Entscheidung vorgelegt, die die Auslegung des maßgeblichen europäischen Rechts betreffen. Der EuGH hat daraufhin am 29. Juli 2019 (Az. C-40/17) unter anderem die Mitverantwortung der Websitebetreiberin bestätigt.

Diese Mitverantwortung geht, wie der EuGH betont hat, so weit, wie die Websitebetreiberin über die Zwecke und Mittel (mit-) entscheidet. Für welchen Datenverarbeitungsvorgang bei der Plugin-Anbieterin, also beim Sozialen Netzwerk, dies nicht mehr gelten soll, lässt die Entscheidung im Einzelnen offen. Der EuGH beschränkt sich nämlich auf die Klärung der ihm gestellten Vorlagefragen.

Der Streitfall gelangte daraufhin zurück an das Oberlandesgericht Düsseldorf und wird dort weiterverhandelt. Dieses wird nun auch zu klären haben, welche Rechtsgrundlagen eventuell für die durchgeführten Datenverarbeitungen herangezogen werden können, und ob ihre Voraussetzungen erfüllt sind. Ferner wird es klären müssen, ob die Verantwortlichen ihren jeweiligen Pflichten, insbesondere den Informationspflichten, in ausreichendem Maße nachgekommen sind.

Das EuGH-Urteil bestätigt die LDI NRW in ihrer Auffassung, dass die Websitebetreiber bei Einbindung von Social Plugins die Datenschutzrechte ihrer Nutzerinnen und Nutzer wahren müssen. So muss insbesondere eine Rechtsgrundlage für die Datenverarbeitung vorhanden sein, und die Nutzerinnen und Nutzer sind rechtzeitig zu informieren. Da sie als gemeinsame Verantwortliche mit den Plugin-Betreibern anzusehen sind, müssen sie seit Geltung der DS-GVO außerdem mit diesen eine Vereinbarung darüber schließen, wer von ihnen welche Verpflichtungen aus der DS-GVO erfüllt.

## 4.4 Google Analytics und ähnliche Dienste nur mit Einwilligung nutzbar

**Wenn in Websites Dritt-Dienste eingebunden werden, deren Anbieter personenbezogene Daten auch für eigene Zwecke nutzen, ist das rechtlich nur zulässig, wenn eine Einwilligung der Nutzerinnen und Nutzer eingeholt wird. Zu solchen Diensten gehört auch Google Analytics.**

Im Frühjahr 2019 hat die Datenschutzkonferenz die „Orientierungshilfe für Anbieter von Telemedien“ veröffentlicht, abrufbar unter www.ldi.nrw.de. Darin ist im Einzelnen dargestellt, unter welchen Bedingungen das Verhalten von Website-Besucherinnen und -Besuchern beobachtet und ausgewertet werden darf (Tracking).

Die Orientierungshilfe gilt grundsätzlich für sämtliche Datenverarbeitungen durch Produkte und Dienste, derer sich Website- und App-Betreiber bedienen können, insbesondere auch zur Website-Analyse. Vorgaben, denen eine Einwilligung genügen muss, enthalten auch die Leitlinie des Europäischen Datenschutzausschusses zur Einwilligung (WP 259 rev. 01 vom 28. November 2017, zuletzt überarbeitet und angenommen am 10. April 2018) und das Urteil des Europäischen Gerichtshofs (Urteil vom 01. Oktober 2019, Az. C-673/17). Siehe hierzu unter 4.4.

Ältere Veröffentlichungen der Aufsichtsbehörden in diesem Zusammenhang gelten nicht mehr, da sich die Rechtslage und die Verarbeitungsprozesse geändert haben.

Website-Betreiber sollten ihre Websites auf Dritt-Inhalte und Tracking-Mechanismen überprüfen. Wer Funktionen nutzt, die eine Einwilligung erfordern, muss entweder die Einwilligung einholen oder die Funktion entfernen.

## 4.5 Urteil des EuGH zur wirksamen Einwilligung in die Verwendung von Cookies auf Websites

**Der Europäische Gerichtshof (EuGH) hat wichtige Aussagen zu den Voraussetzungen der wirksamen Einwilligung in die Verwendung von Cookies im Internet getroffen (Urteil vom 1. Oktober 2019, Az. C-673/17).**

Demnach liegt nach geltendem Recht keine wirksame Einwilligung vor, wenn Nutzer zur Verweigerung ihrer Einwilligung ein bereits angekreuztes Kästchen abwählen müssen. Vielmehr wird als Voraussetzung für eine wirksame Einwilligung auch online ein aktives Verhalten des Betroffenen vorausgesetzt.

Zudem hat der EuGH klargestellt, dass Websitebetreiber den Nutzern klare und umfassende Informationen bereitstellen müssen, damit die Einwilligung wirksam erteilt werden kann. Hierzu gehören auch die Angaben zur Funktionsdauer der Cookies und dazu, ob Dritte Zugriff auf die Cookies erhalten können. Damit hat der EuGH die bereits bislang vertretene Auffassung der Datenschutzkonferenz (DSK) bestätigt.

Das Gericht hat darüber hinaus deutlich gemacht, dass das Setzen und Abrufen von Cookies oder anderen Informationen, die im Endgerät der Nutzer gespeichert sind, grundsätzlich einer Einwilligung bedürfen. Gemeint sind Cookies, die nicht erforderlich für die Bereitstellung des von Nutzern aufgerufenen Dienstes sind. Zu den gleichen Ergebnissen kommt die von der DSK beschlossene Orientierungshilfe für Anbieter von Telemedien. Die Orientierungshilfe ist auf unserer Internetseite www.ldi.nrw.de abrufbar. Danach bedarf es für websiteübergreifende Cookies und Tools, die das Nutzerverhalten website- oder geräteübergreifend zusammenfassen (Tracking), in der Regel einer vorherigen informierten Einwilligung der Nutzer. Bei der Verwendung von IP-Adressen, Cookies oder anderen Nutzungsdaten, die für den Betrieb des Telemediendienstes erforderlich sind, können sich Verantwortliche hingegen häufig auf das berechtigte Interesse nach Art. 6 Abs. 1 Satz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) berufen.

Websitebetreiber müssen informierte Einwilligungen der Nutzer einholen, bevor website- oder geräteübergreifendes Tracking zum Einsatz kommt. Hierfür ist ein aktives Verhalten der Nutzer erforderlich. Nicht ausreichend ist es, wenn Nutzer zur Verweigerung ihrer Einwilligungen ein bereits angekreuztes Kästchen abwählen müssen.

## 4.6 Urteil des EuGH zum Google Webmail-Dienst Gmail

**Der Europäische Gerichtshof (EuGH) hat entschieden, dass der Webmail-Dienst von Google (Gmail) kein elektronischer Kommunikationsdienst ist (Urteil vom 13. Juni 2019, Az. C-193/18). Webmail-Dienste wurden von den deutschen Datenschutzaufsichtsbehörden bislang als Telekommunikationsdienste angesehen, was nun nicht mehr möglich ist.**

Begründet wird die Entscheidung unter anderem damit, dass Gmail „nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht“ (Az. C-193/18). Folglich ist in Deutschland auf solche Dienste nicht mehr wie bislang das Telekommunikationsgesetz (TKG), sondern die allgemeinen datenschutzrechtlichen Regelungen anzuwenden.

Das Urteil erging auf der Grundlage der seinerzeit geltenden EU-Richtlinie (2002/21/EG). Inzwischen gibt es eine neue EU-Richtlinie (2018/1972/EG), die es den Mitgliedstaaten ermöglicht, sog. Over The Top (OTT)-Dienste als Telekommunikationsdienste zu definieren. Diese Richtlinie muss in den EU-Mitgliedstaaten bis zum 21. Dezember 2020 umgesetzt werden, um wirksam zu werden. In Deutschland muss demnach bis dahin das TKG geändert werden.

Das Urteil des EuGH hat jedenfalls für die Übergangszeit bis zur Umsetzung der neuen EU-Richtlinie zur Folge, dass für Webmail-Dienste nicht mehr wie bislang der Bundesbeauftragte für Datenschutz und Informationsfreiheit zuständig ist. Vielmehr überwachen die Landesdatenschutzbehörden die Einhaltung der Datenschutzvorgaben. Zuständig ist die jeweilige Datenschutzaufsichtsbehörde, in deren Land das Unternehmen seinen Sitz hat, das den Webmail-Dienst betreibt.

## 4.7 Datenverarbeitung durch natürliche Personen

**Uns erreichen vermehrt Eingaben zur Datenverarbeitung durch natürliche Personen. Auch diese müssen die datenschutzrechtlichen Vorgaben einhalten, soweit diese auf Datenverarbeitungen zu privaten Zwecken anwendbar sind. Das ist nicht der Fall, wenn es sich um rein persönliche oder familiäre Tätigkeiten handelt. Die Voraussetzungen hierfür sind allerdings eng gefasst.**

Die Datenschutz-Grundverordnung (DS-GVO) geht vom Prinzip der Verantwortung aus. Dies bedeutet, dass die Verordnung sich an den sog. „Verantwortlichen" richtet, der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet und daher die Vorgaben der DS-GVO einzuhalten hat. Umgekehrt gehört es zu den Zielen der DS-GVO, die natürlichen Personen zu schützen, deren Daten verarbeitet werden (Art. 1 Abs. 1 und Abs. 2 DS-GVO).

Diese Grundkonstellation führt häufig zu der Vorstellung, die datenschutzrechtlichen Vorgaben müssten ausschließlich von juristischen Personen (zum Beispiel von Unternehmen oder Vereinen), von Behörden und sonstigen Einrichtungen eingehalten werden, nicht aber im Privatbereich. Dabei wird übersehen, dass auch eine natürliche Person „Verantwortlicher" oder „Verantwortliche" gemäß Art. 4 Nr. 7 DS-GVO sein kann.

Die Zahl der Eingaben bei der LDI NRW, die sich auf Datenverarbeitungen durch natürliche Personen beziehen, ist in den letzten beiden Jahren stark gestiegen. Während im Jahr 2017 lediglich 27 Eingaben dieser Art zu verzeichnen gewesen sind, stieg die Zahl im Jahr 2018 auf 110 Eingaben und im Jahr 2019 auf 147 Eingaben an. Typische Problemkreise sind die Veröffentlichungen von personenbezogenen Daten Dritter insbesondere im Internet und in sozialen Medien (zum Beispiel Facebook, Instagram und Twitter) sowie die Weitergabe von Informationen zum Beispiel über Beschäftigte und Kolleginnen und Kollegen am Arbeitsplatz. Das Handeln einer Person ist stets danach zu beurteilen, ob es eine datenschutzrechtliche Relevanz hat oder aber rein privater Natur ist und damit den datenschutzrechtlichen Vorschriften nicht unterfällt.

Zu beachten ist zunächst eine Ausnahmeregelung, die in Art. 2 Abs. 2 Buchstabe c DS-GVO geregelt ist und auch als „Haushaltsprivileg" bezeichnet wird. Danach endet der Anwendungsbereich der DS-GVO dort, wo natürliche Personen eine Datenverarbeitung vornehmen, die „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" erfolgt. Nach Erwägungsgrund 18 zur DS-GVO ist eine Tätigkeit persönlich bzw. familiär, wenn sie keinen Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit hat. Ein typisches Beispiel hierfür sind Datenverarbeitungen im Zusammenhang mit Freizeitaktivitäten oder Familienfeiern. Hintergrund für diese Ausnahmeregelung ist die Annahme, dass im rein persönlichen bzw. familiären Bereich die Möglichkeiten der Datenverarbeitung – und damit die Risiken für davon

betroffene Personen – üblicherweise geringer sind als im beruflichen bzw. wirtschaftlichen Kontext.

Das Haushaltsprivileg ist allerdings eng auszulegen.

Viele Eingaben betreffen Fälle, in denen personenbezogene Daten im Internet veröffentlicht werden. Auch hier stellt sich die Frage, ob die zuvor beschriebene Ausnahmeregelung eingreift. Nach Erwägungsgrund 18 zur DS-GVO könnten als persönliche oder familiäre Tätigkeit auch die Nutzung sozialer Netze oder Online-Tätigkeiten gelten. Ausschlaggebend sind insoweit allerdings die Zugriffsmöglichkeiten auf die bereitgestellten Informationen. Kann lediglich ein begrenzter Personenkreis Kenntnis von den Informationen erlangen, so liegt eine ausschließlich persönliche Tätigkeit nahe. Dies kann etwa der Fall sein, wenn Informationen nur im Rahmen von Einzel- oder Gruppennachrichten zwischen Familienangehörigen oder engsten Freunden veröffentlicht werden. Sofern zwischen den einzelnen Personen regelmäßig auch ein individueller Kontakt besteht, lassen sich Gruppennachrichten ebenfalls dem ausschließlich persönlichen Bereich zuordnen. Anders ist dies bei größeren Teilnehmerkreisen, wenn die Informationen auch solche Personen erreichen, zu denen ansonsten keine persönliche Kommunikation oder Beziehung besteht.

Erfolgt eine Veröffentlichung sogar an einen unbestimmten Personenkreis, so handelt es sich keinesfalls mehr um eine ausschließlich persönliche Tätigkeit. Das Haushaltsprivileg greift nicht, und die Datenverarbeitung unterliegt den Vorgaben der DS-GVO. Dies gilt insbesondere bei Veröffentlichungen im Internet und in sozialen Medien, wie auch der Europäische Gerichtshof (EuGH) bereits zur wortgleichen Vorgängerregelung entschieden hat (Urteil vom 6. November 2003, Az. C-101/01 – Lindqvist; Urteil vom 16. Dezember 2008, Az. C-73/07 – Satamedia).

Eine datenschutzrechtliche Verantwortlichkeit natürlicher Personen kann zudem bei sog. Exzessen im Rahmen von Beschäftigungsverhältnissen bei nicht-öffentlichen Stellen entstehen. Datenverarbeitungen im Zusammenhang mit einem Beschäftigungsverhältnis werden grundsätzlich dem Arbeitgeber zugerechnet, da dieser über die Zwecke und Mittel entscheidet. Handelt eine beschäftigte Person jedoch über ihre Befugnisse hinaus, so kann ein Exzess vorliegen – etwa dann, wenn die Mittel des Arbeitgebers zu privaten Zwecken für eine nicht erlaubte Datenverarbeitung oder Informationsbeschaffung genutzt werden. Ein Beispiel ist die Weitergabe von Informationen über Mitarbeiter und Mitarbeiterinnen am Arbeitsplatz, etwa zu deren Arbeitsverhalten, krankheitsbedingten Fehlzeiten oder privaten Verhältnissen. Für derartige Exzesse ist der Beschäftigte verantwortlich, und sein Verhalten kann nach den jeweils einschlägigen Regelungen sanktioniert werden.

Für Beschäftigte öffentlicher Stellen enthält das Datenschutzgesetz Nordrhein-Westfalen in § 33 einen eigenen Bußgeldtatbestand, der an die handelnde natürliche Person als Täter anknüpft. Zu nennen sind hier zum Beispiel die Informationsbeschaffungen über Dritte, aus Melderegistern oder polizeilichen Informationssystemen.

Auch natürliche Personen können datenschutzrechtlich Verantwortliche sein. Eine Ausnahme besteht, soweit eine Datenverarbeitung zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt. Diese Ausnahme greift aber nicht, sobald ein Bezug zu einer beruflichen bzw. wirtschaftlichen Tätigkeit vorliegt oder wenn personenbezogene Daten im Internet veröffentlicht werden. Eine datenschutzrechtliche Verantwortung natürlicher Personen kann es auch im Rahmen von Beschäftigtenverhältnissen geben.

# 5. Wirtschaft

## 5.1 Beratungen und Veröffentlichungen

**Vortrags- und Erfahrungsaustausch-veranstaltungen:**

- Erfahrungsaustausch mit Kreditinstituten
- Arbeitskreis West der Versicherungsunternehmen
- Sitzung der Arbeitsgruppe DSGVO des FinTechRates. Der FinTechRat berät das Bundesministerium der Finanzen in Fragen der digitalen Finanztechnologie.
- Sitzung des Arbeitskreises Finanzdienstleistung des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.
- Austausch mit den Sparkassenverbänden in NRW (RSGV – Rheinischer Sparkassen- und Giroverband – und SVWL – Sparkassenverband Westfalen-Lippe)
- Vortrag vor dem Verbraucherbeirat der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Zahlungsdiensterichtlinie (PSD2)
- Arbeitskreis Datenschutz des Bundesverbands Deutscher Inkassounternehmen e.V. (BDIU)

**Veröffentlichungen der LDI NRW**

- Umsetzungshilfe zu den Datenschutzhinweisen „Information über die Erhebung von personenbezogenen Daten nach Art. 13, 14 und 21 Datenschutz-Grundverordnung“
- Personalausweis und Datenschutz
- Muster für Datenschutzhinweise auf Websites
- Broschüre „Datenverarbeitung in Inkassounternehmen – Antworten auf häufig gestellte Fragen“

**Veröffentlichungen der Datenschutzkonferenz:**

- Beschluss vom 24.05.2019: Asset Deal – Katalog von Fallgruppen

## 5.2 Betriebliche Datenschutzbeauftragte – Änderung bei der Benennungspflicht nach dem BDSG

**Die Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragten besteht für nicht-öffentliche Stellen nach neuer Rechtslage erst ab einer Personenzahl von 20 – nach altem Recht waren es 10.**

Mit dem 2. Datenschutz-Anpassungs- und Umsetzungsgesetz EU, das seit dem 26. November 2019 in Kraft ist, wurde § 38 Abs. 1 Satz 1 BDSG geändert.

Die alte Regelung des § 38 BDSG sah vor, dass nichtöffentliche Stellen wie etwa Unternehmen und Vereine Datenschutzbeauftragte benennen müssen, soweit sie in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Mit der Gesetzesänderung ist diese Personengrenze von 10 auf 20 angehoben worden. Insbesondere für zahlreiche kleinere Stellen gibt es nun keine Benennungspflicht von Datenschutzbeauftragten mehr.

Unabhängig von der Änderung des BDSG müssen Stellen, bei deren Kerntätigkeit ein besonderes Risiko besteht, weiterhin aufgrund der Datenschutz-Grundverordnung (DS-GVO) Datenschutzbeauftragte benennen.

Das ist der Fall bei umfangreicher systematischer Überwachung (Art. 37 Abs. 1 Buchstabe b DS-GVO) und bei besonderen Datenkategorien nach Art. 9 DS-GVO oder bei Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DS-GVO (Art. 37 Abs. 1 Buchstabe c DS-GVO).

Die Anhebung der Personengrenze im BDSG mag zunächst als eine Entlastung empfunden werden, mittelfristig geht jedoch notwendige datenschutzrechtliche Kompetenz innerhalb der Stellen verloren. Denn die Vorteile von Datenschutzbeauftragten liegen auf der Hand:

Sie stehen für eine hohe interne Beratungsqualität, Vermeidung von Datenschutzverstößen durch interne Beratung und Kontrolle und infolgedessen für ein niedriges Sanktionsrisiko. Sie sorgen mit dafür, dass bei betroffenen Personen Vertrauen geschaffen wird. Dies ist in Zeiten der Digitalisierung ein wichtiger Faktor.

Die Datenschutzaufsichtsbehörden haben deshalb im April 2019 in einer Entschließung gegen eine Abschaffung oder Verwässerung der nationalen Regelungen plädiert (siehe Entschließung der Datenschutzkonferenz „Keine Abschaffung der Datenschutzbeauftragten“ vom 23. April 2019, Abdruck im Anhang).

Statt der Erhöhung der relevanten Personenzahl wäre eine Klarstellung in Bezug auf die Regelung „ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt“ sinnvoller gewesen.

Es wäre hilfreich gewesen klarzustellen, welche Kriterien die maßgeblichen Personen in den Betrieben erfüllen müssen, um im Sinne des BDSG mitgezählt zu werden. Wir verstehen dieses Merkmal des § 38 BDSG im Einklang mit der Gesetzesbegründung wie bisher so:

- **„ständig“**

Es reicht aus, dass die Tätigkeit auf Dauer angelegt ist und die betreffende Person immer dann tätig wird, wenn es notwendig ist, selbst wenn die Tätigkeit nur in zeitlichen Abständen (zum Beispiel monatlich) anfällt. Der Begriff ist also nicht so auszulegen, dass die Datenverarbeitung andauernd oder im Schwerpunkt erfolgen müsste. Unser Verständnis entspricht der Begründung des Gesetzgebers.

- **„mit der automatisierten Verarbeitung von personenbezogenen Daten“**

Die Verarbeitung erfolgt nur dann automatisiert, wenn sie unter Einsatz von Datenverarbeitungsanlagen (beispielsweise Computer, Tablets, Smartphones) erfolgt. Personen, die nicht mit einer automatisierten Datenverarbeitung befasst sind, werden bei der Ermittlung der Personenzahl nicht mitgezählt. Ebenfalls ist eine Verarbeitung anderer Daten als solchen zu natürlichen Personen nicht zu berücksichtigen.

- **„beschäftigt“**

Die Art des Beschäftigungsverhältnisses spielt bei der Frage, welche Personen für die Datenverarbeitung zu berücksichtigen sind, keine Rolle. Sowohl die Leitung als auch angestellte Beschäftigte, Aushilfen, Auszubildende oder Leiharbeitskräfte sind gleichermaßen zu berücksichtigen. Unerheblich ist auch, ob die jeweiligen Personen in Voll- oder Teilzeit arbeiten.
Entscheidend ist, dass die Verarbeitung von personenbezogenen Daten Bestandteil der Tätigkeit ist, also in der Aufgabenbeschreibung bzw. Aufgabenzuweisung eingeschlossen ist. Das ist beispielsweise bei Reinigungskräften, Fahrern oder Gärtnern in der Regel nicht der Fall, so dass diese bei der Berechnung nicht mit zu berücksichtigen sind.

Soweit keine Pflicht (mehr) zur Benennung von Datenschutzbeauftragten vorliegt, ist in vielen Fällen eine freiwillige Benennung sinnvoll und wird unsererseits unterstützt. Auf bereits benannte Datenschutzbeauftragte sollte nicht verzichtet werden, weil ihre datenschutzrechtliche Kompetenz weiterhin wichtig bleibt. Denn die datenschutzrechtlichen Vorgaben müssen in jedem Fall von Verantwortlichen und Auftragsverarbeitern eingehalten werden, unabhängig davon, ob ein Datenschutzbeauftragter zu benennen ist.

Im Falle einer freiwilligen Benennung von Datenschutzbeauftragten unterliegen deren Benennung, Stellung und Aufgabenbereich den gleichen Anforderungen wie bei einer obligatorischen Benennung (Art. 37 bis 39 DS-GVO). Der besondere Abberufungs- und Kündigungsschutz gilt für betriebliche Datenschutzbeauftragte jedoch nur, soweit deren Benennung verpflichtend ist (§ 38 Abs. 2 BDSG).

Die BDSG-Regelungen zum Abberufungs- und Kündigungsschutz (§ 38 Abs. 2 in Verbindung mit § 6 Abs. 4 BDSG) stellen rein arbeitsrechtliche Regelungen dar. Zur Frage, wie mit Datenschutzbeauftragten umzugehen ist, die aufgrund der bisherigen Benennungspflicht benannt wurden und nach der Gesetzesänderung nun nicht mehr verpflichtend zu benennen wären, berät die LDI NRW aus diesem Grund insoweit nicht.

Wir raten den Stellen, die von der neuen Regelung des § 38 BDSG vermeintlich „profitieren“, auch weiterhin ihre bisherige Datenschutzorganisation beizubehalten und freiwillig an ihrer bzw. ihrem Datenschutzbeauftragten festzuhalten. Eine fundierte Datenschutzorganisation schützt vor Sanktionsrisiken und stärkt das Vertrauen der betroffenen Personen wie Kundinnen und Kunden oder Vereinsmitglieder.

## 5.3 Akkreditierungskriterien für CoC-Überwachungsstellen mit Sitz in Deutschland

**Am 4. Juni 2019 hat der Europäische Datenschutzausschuss seine Leitlinien über Verhaltensregeln und Überwachungsstellen verabschiedet (Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679). Damit Verhaltensregeln nach Art. 40 DS-GVO von der zuständigen Aufsichtsbehörde genehmigt werden können, muss in den Verhaltensregeln eine Überwachungsstelle benannt sein, die von der zuständigen Aufsichtsbehörde als zur effektiven Überwachung der Verhaltensregeln in der Lage akkreditiert ist. Eine Ausnahme gilt nur für Verhaltensregeln von Behörden und öffentlichen Stellen. Was heißt das nun für die in Deutschland von Wirtschafts- und Branchenverbänden bereits vor dem 4. Juni 2019 erstellten Verhaltensregeln?**

Die DS-GVO enthält eine Vielzahl von abstrakten und allgemeinen Vorgaben, mit der europaweit ein einheitliches Regelungsniveau und ein verbindlicher Rechtsrahmen geschaffen wird. Der Rechtsanwender muss in der alltäglichen Praxis diese abstrakten und allgemeinen Vorgaben für seine einzelfallbezogene Datenverarbeitung konkretisieren. Mit der Förderung und Anerkennung von Verhaltensregeln nach Art. 40, 41 DS-GVO ermöglicht die DS-GVO Wirtschafts- und Branchenverbänden, die abstrakten und allgemeinen Vorgaben durch Verhaltensregeln sektor- und branchenspezifisch auszufüllen und schafft damit ein Konzept der regulierten Selbstregulierung. Verhaltensregeln vereinfachen also die wirksame Anwendung der DS-GVO und geben hierdurch den für die Datenverarbeitung Verantwortlichen, Auftragsverarbeitern und betroffenen Personen Rechtssicherheit. Die Kontrolle der Einhaltung der Verhaltensregeln erfolgt nach Art. 41 DS-GVO durch unabhängige Überwachungsstellen der Wirtschaft. Diese CoC-Überwachungsstellen müssen von der zuständigen Aufsichtsbehörde vorher akkreditiert werden. Die Verhaltensregeln entfalten die mit der Genehmigung verbundene privilegierende Wirkung erst, wenn eine akkreditierte CoC-Überwachungsstelle existiert.

Voraussetzung für die Akkreditierung einer CoC-Überwachungsstelle ist neben der Stellung eines Antrags die Erfüllung der in Art. 41 Abs. 2 DS-GVO genannten Vorgaben. Die für die Akkreditierung zuständige Aufsichtsbehörde prüft die Erfüllung der in Art. 41 Abs. 2 DS-GVO genannten Vorgaben anhand von ihr zuvor verfasster und nach Durchführung des Kohärenzverfahrens nach Art. 63 DS-GVO veröffentlichter Akkreditierungskriterien (vgl. Art. 41 Abs. 3 in Verbindung mit Art. 57 Abs. 1 Buchstabe p 1. Alternative DS-GVO).

Die deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder haben sich Anfang 2019 entschieden, für CoC-Überwachungsstellen mit Sitz in Deutschland branchenunabhängig einheitliche Akkreditierungskriterien zu entwickeln. Der AK Wirtschaft, ein Arbeitskreis der Datenschutzkonferenz (DSK),

hat im Verlauf des Jahres 2019 die deutschen Akkreditierungskriterien durch einen hierfür eingerichteten Unterarbeitskreis entwickeln lassen. Insgesamt 18 mit diesem Thema befassten Verbänden der Wirtschaft wurde Gelegenheit zur Stellungnahme gegeben. Nachdem die DSK dem Entwurf der Akkreditierungskriterien zugestimmt hatte, wurde er Ende 2019 im Wege des Kohärenzverfahrens an den Europäischen Datenschutzausschuss (EDSA) zur Einholung einer Stellungnahme nach Art. 64 Abs. 1 lit c DS-GVO weitergeleitet.

Die von den deutschen Aufsichtsbehörden entwickelten Akkreditierungskriterien orientieren sich an den Vorgaben der DS-GVO, den Leitlinien des EDSA über Verhaltensregeln und Überwachungsstellen vom 04.06.2019 (CoC GL) und bemühen sich um einen einheitlichen Maßstab zu den Anforderungen für Zertifizierungsstellen nach Art. 43 DS-GVO, soweit diese beiden Rechtsinstitute miteinander vergleichbar sind. Die Kriterien geben so Aufsichtsbehörden und den betroffenen Stellen konkrete Anhaltspunkte für die Akkreditierung von CoC-Überwachungsstellen, ohne die gesetzlichen Vorgaben zu verschärfen. Die Akkreditierungskriterien konkretisieren unter anderem die Vorgaben der DS-GVO zur organisatorischen und personellen Unabhängigkeit der Überwachungsstelle (Art. 41 Abs. 2 Buchstabe a DS-GVO) sowie zur Vermeidung von Interessenkonflikten (Art. 41 Abs. 2 Buchstabe d DS-GVO). So stellen sie zum Beispiel klar, dass Überwachungsstellen auch bei den die Verhaltensregeln einreichenden Verbänden bzw. Einrichtungen gemäß Art. 40 Abs. 2 DS-GVO (sog. internen Überwachungsstellen) eingerichtet werden können, nicht aber bei den einzelnen Unternehmen, die sich zur Einhaltung der Verhaltensregeln verpflichtet haben. Sowohl juristische Personen als auch natürliche Personen können sich als Überwachungsstelle akkreditiert lassen, wobei aber die Anforderungen an eine natürliche Person als Überwachungsstelle besonders sorgfältig zu regeln sind, insbesondere auch im Hinblick auf Nachfolgeregelungen für den Fall eines plötzlichen Wegfalls der Überwachungsperson. Weiterhin machen die Akkreditierungskriterien konkrete Vorgaben zum Nachweis des erforderlichen Fachwissens (Art. 41 Abs. 2 Buchstabe a DS-GVO). Gleiches gilt für die Nachweise an die erforderlichen Verfahren und Strukturen für die Kontrolle der Verhaltensregeln durch die Überwachungsstelle nach Art. 41 Abs. 2 Buchstabe b DS-GVO sowie für das Beschwerdeverfahren nach Art. 41 Abs. 2 Buchstabe c DS-GVO.

Der deutsche Entwurf der Akkreditierungskriterien für CoC-Überwachungsstellen lag bei Redaktionsschluss dem EDSA im Rahmen des Art 64-Verfahrens vor.

Mit der Förderung und Genehmigung von Verhaltensregeln geben die deutschen Aufsichtsbehörden den Wirtschafts- und Branchenverbänden eine Möglichkeit an die Hand, die Regelungen der DS-GVO zu konkretisieren und damit mittelbar insbesondere den kleinen und mittleren Unternehmen sowie den Kleinstunternehmen einen sicheren Rechtsrahmen zu geben. Die deutschen Aufsichtsbehörden hoffen, das europäische Kohärenzverfahren beim EDSA zügig durchlaufen zu können, um so CoC-Überwachungsstellen in Deutschland schnellstmöglich

zu akkreditieren. Erst mit erfolgreicher Akkreditierung einer Stelle, die für die Überwachung der zur Genehmigung vorgelegten Verhaltensregeln zuständig ist, kann das Genehmigungsverfahren für die Verhaltensregeln abgeschlossen werden.

## 5.4 Neue Onlinebanking-Regeln seit September 2019: Das Zusammenspiel von PSD2 und DS-GVO

**Seit dem 14. September 2019 gelten in der EU neue Sicherheitsvorgaben beim Onlinebanking und auch beim Kauf über das Internet. Zusätzlich zur PIN brauchen Bankkunden nun die zweite Authentifizierung per TAN, die sog. starke Kundenauthentifizierung (Strong Customer Authentifizierung – SCA). Online- und Kartenzahlungen müssen nun grundsätzlich durch zwei unabhängige Merkmale aus den Kategorien Wissen (z. B. PIN, Passwort), Besitz (zum Beispiel Handy, Karte, TAN-Generator) und Inhärenz (z. B. Fingerabdruck) bestätigt werden. TAN-Listen auf Papier sind nicht mehr erlaubt. Außerdem soll es spezielle Schnittstellen geben, über die auch Nicht-Banken Zahlungsdienstleistungen anbieten können, beispielsweise sog. Zahlungsauslösedienste oder auch Kontoinformationsdienste. Das bedeutet, dass man sich zum Beispiel bei einem Einkauf im Internet nicht extra in das Online-Banking eines Kreditinstituts einloggen muss, sondern die Überweisung über einen auf der Händlerseite angebotenen Zahlungsauslösedienst beauftragen kann. Durch die Nutzung eines Kontoinformationsdienstes besteht die Möglichkeit sich für alle Zahlungskonten bei verschiedenen Banken Kontostände und Umsätze in aufbereiteter Form anzeigen zu lassen. Datenschutzbehörden und Verbraucherschutzorganisationen ist es wichtig, dass bei diesen neuen Diensten die Rechte der Betroffenen gewahrt werden.**

Mit der Zweiten Zahlungsdiensterichtlinie, auch bekannt als PSD2 (Payment Services Directive2), wird ein Rechtsrahmen für die Aufnahme der Zahlungsauslösedienste und der Kontoinformationsdienste in den Katalog der Zahlungsdienste geschaffen. Die PSD2 ist in Deutschland mit dem bereits am 13. Januar 2018 in Kraft getretenen Zahlungsdiensteaufsichtsgesetz (ZAG) umgesetzt. Die Verpflichtung zur starken Kundenauthentifizierung und die Öffnung der Zahlungskonten für die neuen Zahlungsdienstleister wurden in Technischen Regulierungsstandards der Europäischen Kommission (RTS, Regulatory Technical Standards) näher spezifiziert, die nunmehr als Delegierte Verordnung (EU 2018/389 vom 27.11.2017) am 14. September 2019 in Kraft getreten ist.

Zahlungsauslösedienste initiieren Überweisungen im Onlinebanking und Kontoinformationsdienste dienen zur Abfrage und Auswertung von Kontodaten. Sie gelangen aber, in Abgrenzung zu Banken als klassische Dienstleister, nicht in den Besitz von Kundengeldern. Dennoch müssen sich Kontoinformationsdienstleister bei der deutschen Bankenaufsicht, der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), registrieren lassen. Zahlungsauslösedienstleister benötigen sogar eine Erlaubnis der BaFin.

Die PSD2 erlaubt den neuen Zahlungsdienstleistern, für die Zwecke der Erbringung der betreffenden Dienstleistungen Zugang zu den Kontodaten zu erhalten. Zugang wird diesen Anbietern aber nur

gewährt, wenn die kontoinhabende Person dem ausdrücklich zustimmt hat. Ohne deren ausdrückliche Zustimmung wird keine Zahlung ausgeführt und es darf kein Dienstleister auf die Kontodaten zugreifen.

Viele Fragen zum Zusammenspiel zwischen den Vorgaben der PSD2 und der DS-GVO sind noch nicht geklärt. So haben nach der PSD2 die neuen Zahlungsdienstleister das Recht auf Zugang zu den Kontodaten der Zahlungsdienstnutzer. In diesen Kontodaten können Daten Dritter enthalten sein, wie zum Beispiel Name und Kontonummer der Personen, die keinen neuen Zahlungsdienstleisters nutzen, aber in Zahlungsvorgänge mit der Nutzerin oder dem Nutzer eingebunden sind (zum Beispiel Zahlungsempfänger). Die PSD2 als EU-Richtlinie zur Regulierung von Zahlungsdiensten und Zahlungsdienstleistern hat im Wesentlichen zum Ziel, die Sicherheit im Zahlungsverkehr zu erhöhen, Innovationen zu fördern und den Wettbewerb im Markt zu steigern. Sie hat aber nicht den Datenschutz im Fokus. So muss anhand der Vorgaben der DS-GVO geklärt werden, wie die in den Kontodaten möglicherweise enthaltenen Daten Dritter datenschutzrechtlich unter Beachtung der PSD2 angemessen zu schützen sind. Die Kontodaten können auch besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO enthalten, zum Beispiel indem politische Meinungen und religiöse Überzeugungen durch Spenden an politische Parteien oder Organisationen, Kirchen oder Religionsgemeinschaften enthüllt werden oder die Mitgliedschaft in einer Gewerkschaft durch den Abzug eines jährlichen Mitgliedsbeitrags vom Bankkonto einer Person offenbart wird. Datenschutzrechtlich ist daher die Frage nach der Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten sowohl der Nutzer der neuen Dienstleister als auch der Daten Dritter zu klären. Die Frage nach der Rechtsgrundlage im datenschutzrechtlichen Sinne stellt sich auch in den Fällen, in denen die neuen Zahlungsdienstleister unter Verwendung der Kontodaten weitere Dienste anbieten, die über die von der PSD2 erfassten Dienstleistungen eines Zahlungsauslöse- oder Kontoinformationsdienstes hinausgehen (Zweitverwendung), wie zum Beispiel die Erstellung von Bonitätsanalysen, die an Dritte für eine Kreditwürdigkeitsprüfung weitergegeben werden, oder die Sammlung von Daten über die Gesundheit einer Person durch Analyse der von einer betroffenen Person gezahlten medizinischen Rechnungen.

Der Europäische Datenschutzausschuss arbeitet derzeit zusammen mit den nationalen Aufsichtsbehörden intensiv an der Erstellung von Richtlinien zum Zusammenspiel der PSD2 mit der DS-GVO. Bereits mit Schreiben vom 5. Juli 2018 hatte der Europäische Datenschutzausschuss eine erste Stellungnahme hierzu abgegeben (EDPB-84-2018). So sind sich die Datenschutzbehörden einig, dass die Verarbeitung personenbezogener Daten durch Zahlungsauslösedienstleister oder Kontoinformationsdienstleister nach Art. 6 Abs. 1 Satz 1 Buchstabe b DS-GVO rechtmäßig ist, wenn die Verarbeitung für die Erfüllung des von der betroffenen Person in Anspruch genommenen Zahlungsauslösedienst oder Kontoinformationsdienst erforderlich ist und keine Daten besonderer Kategorien nach Art. 9

Abs. 1 DS-GVO erfasst sind. Rechtsgrundlage für die Verarbeitung der Daten Dritter zur Erbringung von Zahlungsauslöse- und Kontoinformationsdiensten kann das berechtigte Interesse an der Ausführung des Vertrages mit dem Nutzer des neuen Zahlungsdienstes sein (Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO). Dies gilt allerdings nur insoweit, wie keine Daten besonderer Kategorien im Sinne des Art. 9 Abs. 1 DS-GVO verarbeitet werden. Außerdem wird das berechtigte Interesse begrenzt und bestimmt durch die berechtigten Erwartungen der Zahlungsdienstnutzer und insbesondere der engen Zweckbindung nach der DS-GVO. Der kontoführende Dienstleister, also die Bank des Zahlungsdienstnutzers, ist zur Gewährung des erforderlichen Zugriffs bzw. Zugangs für die Diensterbringung durch die neuen Dienstleister verpflichtet, so dass diese Offenlegung durch die Bank nach Art. 6 Abs. 1 Satz 1 Buchstabe c DS-GVO rechtmäßig ist. Als Rechtsgrundlage für die Zweitverwendung personenbezogener Daten für andere Zwecke als für die Erfüllung eines neuen Zahlungsdienstes kommt eine freiwillige, informierte und unmissverständlich erteilte Einwilligung durch den Zahlungsdienstnutzer nach Art. 6 Abs. 1 S. 1 Buchstabe a DS-GVO in Betracht. Auf die Zweitverwendung von Daten Dritter kann sich die Einwilligung des Zahlungsdienstnutzers allerdings nicht erstrecken. Zum Verhältnis der „ausdrücklichen Zustimmung“ gemäß Art. 94 Abs. 2 der PSD2 (§ 59 Abs. 2 ZAG) zur „Einwilligung“ nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO, im Englischen in beiden Gesetzestexten einheitlich als „Consent“ bezeichnet, haben die europäischen Datenschutzbehörden im oben genannten Schreiben vom 05. Juli 2018 des Europäische Datenschutzausschuss (EDPB-84-2018) festgehalten, dass die ausdrückliche Zustimmung nach der PSD2 ein zusätzliches Erfordernis zivilvertraglicher Natur ist, das von der datenschutzrechtlichen Einwilligung zu unterscheiden ist. Das heißt, mit dem Auftrag an den Zahlungsdienstleister ist keineswegs automatisch eine Einwilligung nach dem Datenschutzrecht verbunden. Diese muss vielmehr separat erteilt werden.

Die mit der PSD2 für den Zahlungsverkehr in der Europäischen Union gewünschte Förderung von Innovation und Wettbewerb muss mit den Vorgaben der europäischen Datenschutz-Grundverordnung im Einklang stehen. Das Ergebnis der weiteren Arbeiten der europäischen Aufsichtsbehörden an den Leitlinien zum Zusammenspiel von PSD2 und DS-GVO wird nicht zuletzt von den neuen Zahlungsdienstanbietern mit Spannung erwartet.

## 5.5 Informationspflichten beim kartengestützten Zahlungsverkehr im stationären Handel

**Wenn im stationären Handel mit Karte bezahlt wird, sind an diesem kartengestützten Zahlungsverkehr verschiedene Verantwortliche beteiligt. Kundenkontakt besteht jedoch regelmäßig nur zwischen den (Einzel-)Händlern im Geschäftslokal und der Kundschaft. Wie können bei dieser komplexen Datenverarbeitung die Informationspflichten unter Beachtung der Vorgaben zur Datenschutzinformation nach Art. 13, 14 DS-GVO eingehalten werden?**

In einem Zahlungsprozess mit Karte oder Kreditkarte sind mehrere Beteiligte involviert, und jeder von ihnen verarbeitet Kundendaten. Akzeptiert der stationäre Handel die Zahlung mit Karte, wird für die Kartenzahlung ein sog. Terminal am Point-of-Sale (POS-Terminal) benötigt, das über eine Bank oder einen sog. Netzbetreiber erhältlich ist. Netzbetreiber stellen nicht nur die Kartenterminals zur Verfügung, sondern betreiben insbesondere das Netz, an dem die Terminals angeschlossen sind. Sie nehmen dabei mehrere Funktionen wahr, unter anderem die technische Überwachung des Netzes, Weiterleitung, Routing und Rückmeldung von ec-cash-Autorisierungsanfragen und Kreditkarten-Autorisierungsanfragen, eventuell Überwachung von internen Sperrlisten und am Tagesende (nach Kassenschnitt oder Tagesabschluss des Terminals) die Einleitung der Zahlungsverkehrs-Abwicklung. Wenn Händler auch Kreditkarten akzeptieren, schließen sie einen Vertrag mit dem Acquirer als Transaktionsabwickler der (Kredit)-Karten und als Verrechner. Ein Acquirer wird auch Händlerbank genannt und ist ein Unternehmen, das die Händler als Vertragspartner für Kreditkartenzahlungen betreut und Akzeptanzverträge für die Kreditkartenorganisationen (zum Beispiel MasterCard, Visa) abschließt. Auch Acquirer verarbeiten im kartengestützten Zahlungsverkehr die personenbezogenen Daten der Karteninhaber. Erheben die Händler im kartengestützten Zahlungsverkehr personenbezogene Daten ihrer Kundschaft im Kassensystem, so sind neben Netzbetreiber, und – bei Kreditkartenzahlung – Acquirer auch die Händler im datenschutzrechtlichen Sinne Verantwortliche der Datenverarbeitung. Alle drei Beteiligten treffen die Informationspflichten nach Art. 13, 14 DS-GVO.

Wie soll also ein so komplexer Verarbeitungsprozess schnell transparent gemacht werden?

In der Praxis haben allein die Händler den direkten Kontakt zu den betroffenen Karteninhabern und müssen in die Lage versetzt werden, ihre Informationspflichten zu erfüllen. Umgekehrt bedürfen die übrigen Beteiligten, Netzbetreiber und ggf. Acquirer, der Mithilfe der im direkten Kundenkontakt stehenden Händler, um rechtzeitigt „bei Erhebung“ der für den Bezahlvorgang am POS-Terminal erforderlichen Daten ihre Informationspflichten nach Art. 13,14 DS-GVO erfüllen zu können.

Der Bundesverband der electronic cash – Netzbetreiber (BecN) e.V. mit Sitz in Frankfurt hatte den deutschen Aufsichtsbehörden ein Informationsblatt gemäß

Art. 13, 14 DS-GVO an Point of Sale-Terminals zu kartengestützten Zahlungen zukommen lassen. Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) hat dem Bundesverband Hinweise erteilt und sich am 4. Juli 2019 mit der von dem Verband BecN vorgeschlagenen Vorgehensweise einverstanden erklärt.

Danach erfüllen Händler die Informationspflichten des Netzbetreibers und, sofern er Kreditkarten akzeptieren, auch die Informationspflichten des/der Acquirer(s) zusätzlich zu den ggf. sie betreffenden eigenen Informationspflichten nach der DS-GVO. Hierfür wird ein gut sichtbarer Aufkleber mit der Aufschrift "Datenschutz-Informationen für Karteninhaber" am POS-Terminal oder an der Ladenkasse angebracht, möglichst auch zusätzlich beim Karten-Akzeptanzaufkleber an der Ladeneingangstür. Statt des Aufklebers sind auch Aufsteller oder Aushänge möglich. Dort sind die Kontaktdaten des Händlers bzw. der Händlerin angegeben. Der Aufkleber zeigt zusätzlich einen QR-Code und/oder eine URL. Beides führt zu einer Website des Netzbetreibers mit den nach der DS-GVO erforderlichen Informationen. Zusätzlich wird an der Kasse ein Papierausdruck der Datenschutzinformationen hinterlegt. Werden auch Kreditkarten akzeptiert, müssen an der Kasse oder als Aushang zusätzlich der Name und die Kontaktdaten des/der Acquirer(s) sowie die Kontaktdaten seines bzw. seiner jeweiligen Datenschutzbeauftragten und der jeweiligen zuständigen Aufsichtsbehörde vorgehalten werden.

Das von BecN entwickelte einheitliche Informationsblatt der am kartengestützten Zahlungsverfahren Beteiligten, also Händler, Netzbetreiber und Acquirer, erfüllt die datenschutzrechtlichen Vorgaben der Art. 13, 14 DS-GVO. Zwar sind die konkreten Datenströme von den jeweiligen Zahlverfahren und Kassensystemen abhängig, so dass die konkrete Ausgestaltung, wer der drei im Bezahlvorgang Beteiligten welche Daten bereitstellt, vom Einzelfall abhängig ist. Gleichwohl ist eine Aufspaltung in bis zu drei Informationspakete nicht sinnvoll. Ein einheitliches Informationsblatt wahrt – bei entsprechender Ausgestaltung – hinreichend die Funktion der Art. 13, 14 DS-GVO, dem von der Datenverarbeitung Betroffenen in eigener Selbstbestimmung über die Datenverarbeitung zu entscheiden, hierzu bei Erhebung Stellung zu nehmen und seine Betroffenenrechte wirksam auszuüben. Auch ist ein Verbot des Medienbruchs, also des Wechsels der Kommunikationsform, der DS-GVO nicht zu entnehmen. Vielmehr kann sich der Verantwortliche unterschiedlicher Mittel und Wege bedienen, wie hier eines Papierausdrucks des Informationsblattes an der Kasse sowie zusätzlich eines QR-Codes und/oder einer URL, so lange er die gesetzlichen Anforderungen an den Umfang und den Zeitpunkt einhält. Der Einbeziehung weiterer Beteiligter bei Kartenzahlungen, wie zum Beispiel das kartenausgebende Unternehmen (Issuer), bedarf es nicht. Händler, Netzbetreiber und Acquirer können ihre Informationspflichten auf eine transparente und verständliche Weise ohne diese weiteren Beteiligten erfüllen.

Wir begrüßen die Entwicklung eines einheitlichen Informationsblattes der am kartengestützten Zahlungsverfahren beteiligten datenschutzrechtlich Verantwortlichen. Das Gebot der DS-GVO an einer insbesondere transparenten und leicht verständlichen Information (Art. 12 Abs. 1 DS-GVO) einerseits und die Komplexität der Datenströme bei Kartenzahlungen andererseits lassen es empfehlenswert erscheinen, dass Händler, Netzbetreiber und Acquirer sich auf einen gemeinsamen Ansatz bei der Informationserteilung einigen.

## 5.6 Smart Metering – Digitale und intelligente Stromzähler

**Die flexible Nutzung erneuerbarer Energien macht es erforderlich, intelligente Energieversorgungsnetze aufzubauen. Stromnachfrage und wetterabhängige Stromeinspeisung müssen in Einklang gebracht werden. Hilfe für diese Energiewende wird in der Digitalisierung gesehen. Doch sind mit der Digitalisierung auch Risiken für die Privatsphäre verbunden. So wird ein hohes Datenvolumen erhoben und verarbeitet, das zu Personenprofilen genutzt werden kann. Die automatische Übermittlung erfolgt unbemerkt, und die Masse der Daten kann ihrer eigentlichen Zweckbestimmung entzogen und missbraucht werden. Außerdem ist der Kommunikationsweg über das Internet anfällig. Diese Aspekte müssen bei der Ausgestaltung der Netzstruktur beachtet werden.**

Mit dem Messstellenbetriebsgesetz (MsbG) vom 29. August 2016, zuletzt geändert durch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 20. November 2019 (BGBl. I 2019 S. 1626, 1679 – 1681) hat der Bund – unter Beteiligung der Datenschutzaufsicht – sehr detaillierte Datenschutzregelungen für das Smart Metering geschaffen (§§ 19 – 28, 49 – 70 MsbG). Der Einbau von digitalen Stromzählern wird sowohl von Mieterseite als auch von Seiten der Immobilieneigentümerschaft nicht selten mit Skepsis gesehen, greifen sie doch in die private Wohnsphäre ein.

Die LDI NRW erreichen dazu immer wieder Anfragen besorgter Bürgerinnen und Bürger.

Hier Antworten auf eine Auswahl von häufig gestellten Fragen im Überblick:

***Worin unterscheiden sich „digitale Stromzähler“ von „intelligenten Stromzählern (Smart Metern)“?***

Intelligente Stromzähler bestehen aus einer digitalen Messeinheit, die über ein Kommunikationsmodul (Smart-Meter-Gateway) mit dem Internet verbunden ist. Über diesen Weg können die Verbrauchsdaten aus der Ferne ausgelesen und verarbeitet werden.

Bei dem digitalen Stromzähler handelt es sich nur um eine moderne elektronische und stationäre Ableseeinrichtung ohne Anbindung an das Internet und ohne Funkübertragungsmöglichkeit. Die digitalen Stromzähler können jedoch bei Bedarf mit dieser Kommunikationskomponente nachgerüstet werden.

***Ab wann besteht eine gesetzliche Einbaupflicht?***

Intelligente Stromzähler sind erst ab einem Jahresstromverbrauch von mindestens 6.000 Kilowattstunden einzubauen (§ 29 MsbG). Zum Vergleich: Der durchschnittliche Stromverbrauch eines 4-Personen-Haushalts in Deutschland beträgt rund 3.500 Kilowattstunden Strom pro Jahr. Damit dürften die durchschnittlichen Familienhaushalte von einer Einbaupflicht nicht betroffen sein. Für diese gilt aber, dass bis zum Jahr 2032 zumindest digitale Stromzähler ohne Funkübertragungsmöglichkeit verbaut werden. Der Einbau intelligenter Stromzähler ist bei einem Jahresstromverbrauch un-

terhalb der Schwelle von 6.000 Kilowattstunden aber möglich (§ 29 Abs. 2 MsbG).

***Wer ist datenschutzrechtlich verantwortlich für die Datenverarbeitung in den intelligenten Stromzählern?***
Das sind Messstellenbetreiber, also Stromversorger oder von diesen beauftragte Dienstleister. Messstellenbetreiber sind für den Einbau, den Betrieb und die Wartung des Stromzählers zuständig. Darüber hinaus kümmern sie sich auch um die Datenübertragung der gemessenen Werte. Nicht verantwortlich sind Vermieterinnen und Vermieter. Sie können sich aber an die Stromversorger wenden und dort Informationen zum intelligenten Stromzähler einfordern und diese dann an die Mieter weitergeben, um so für Transparenz zu sorgen.

***Wer kann sich gegen den Einbau aussprechen?***
Verbraucherinnen und Verbraucher haben keine Möglichkeit, einem geplanten Einbau zu widersprechen. Wie bisher bei herkömmlichen Stromzählern ist auch der Einbau von intelligenten Messsystemen zu dulden.

Mieter und Vermieter haben ein Recht ihren Messstellenbetreiber frei auszuwählen. Ab 1. Januar 2021 geht das Auswahlrecht des Vermieters dem Auswahlrecht des Mieters vor (§§ 5, 6 MsbG).

***Welche Datenströme gibt es im Zusammenhang mit digitalen und intelligenten Zählern?***
Eine digitale Messeinrichtung, bei der kein Kommunikationsmodul eingebaut ist, sendet und empfängt keine Daten. Die Daten verbleiben im Messsystem und müssen wie bei herkömmlichen Zählern weiterhin ausgelesen werden. Anders verhält es sich bei intelligenten Messsystemen: Hier erhalten die Stromversorger des Haushalts ebenso wie Netzbetreiber und Messstellenbetreiber automatisch die jeweiligen Verbrauchswerte. Von Haushalten mit einem Jahresverbrauch von weniger als 10.000 Kilowattstunden bekommen sie aber alle – wie bei herkömmlichen Zählern auch – ausschließlich die Summe des Stromverbrauchs für das gesamte Jahr. Nur wenn im Vertrag mit dem Stromversorger ausdrücklich etwas anderes vereinbart ist – etwa für variable Tarife – fließen detailliertere Daten. Auch bei einem Verbrauch über 10.000 Kilowattstunden werden mehr Daten übertragen. Ein so hoher Verbrauch ist jedoch bei den üblichen Familienhaushalten nicht gegeben.

***Werden bei intelligenten Messsystemen laufend Daten übermittelt?***
Nein. Bei Verbrauchern mit einem Jahresverbrauch von bis zu 10.000 Kilowattstunden werden die Daten „vor Ort“ allein zum Zwecke der eigenen Verbrauchsveranschaulichung vorgehalten. Grundeinstellung ist hier die jährliche Übermittlung an den Stromlieferanten. Nur für den Fall, dass ein Tarif gewählt wird, der eine feinere Messung und Übermittlung erfordert, werden weitere Daten an Netzbetreiber und Lieferanten versendet. Ein durchschnittlicher 4-Personen-Haushalt in Deutschland verbraucht rund 3.500 Kilowattstunden Strom pro Jahr.

***Welche personenbezogenen Daten sind betroffen?***
Die Messwerte geben den Verbrauch im häuslichen Bereich zu bestimmten Zeiten

wieder und können in Bezug gesetzt werden zu einer Einzelperson oder zu einer Gruppe von Personen (zum Beispiel Familie, Wohngemeinschaft). Da ein Großteil der Handlungen im Alltag mit Energieverbrauch verbunden ist, lässt der Stromverbrauch Rückschlüsse auf die Lebensgewohnheiten und persönlichen Verhältnisse zu. Je umfangreicher die Datenerhebung ist und je häufiger die Datenübertragung in einem Zeitintervall stattfindet, desto größer ist das Risiko eines Verhaltensprofils. Dies gilt vor allem dann, wenn die Messsysteme den Verbrauch einzelner Hausgeräte erfassen und analysieren.

***Welche Auskunftsrechet bestehen?***

Messstellenbetreiber stellen Datenblätter zur Verfügung, die den Datenverlauf nachvollziehbar erläutern (§ 54 MesbG). Zudem besteht ein umfangreiches Auskunftsrecht nach § 53 MesbG, Art. 12, 15 DS-GVO. Danach haben Messstellenbetreiber auf Verlangen von Nutzern die im elektronischen Speicher- und Verarbeitungsmedium gespeicherten auslesbaren personenbezogenen Daten mitzuteilen und Einsicht in die nicht personenbezogenen Daten zu gewähren. Dies hat unentgeltlich zu erfolgen.

***Wie wird die Datensicherheit gewährleistet?***

Digitale Stromzähler, die über das Kommunikationsmodul mit dem Internet verbunden sind, könnten von außen gehackt werden. Deshalb stellt das MsbG hohe Anforderungen an die Sicherheit der Soft- und Hardware der Messstellenbetreiber, deren Einhaltung über Zertifizierungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nachgewiesen werden müssen.

Um ein einheitliches und sehr hohes Sicherheitsniveau zu gewährleisten, erklärt das MsbG Schutzprofile und Technische Richtlinien für intelligente Messsysteme zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität für verbindlich (§§ 19 ff. MesbG). Diese wurden unter Beteiligung der Datenschutzaufsicht erarbeitet und können auf der Homepage des BSI www.bsi.bund.de nachgelesen werden. Mit einem Siegel des BSI werden nur solche Systeme ausgezeichnet, die die sehr hohen Datenschutz- und Datensicherheitsanforderungen nachweislich erfüllen.

***Wer darf die personenbezogenen Daten verarbeiten?***

Grundsätzlich dürfen nur die nach § 49 Abs. 2 MsbG berechtigten Stellen die personenbezogenen Daten in dem dort geregelten Umfang verarbeiten. Das sind: Messstellenbetreiber, Netzbetreiber, Bilanzkoordinatoren, Bilanzkreisverantwortliche, Direktvermarktungsunternehmen und Energielieferanten. Andere Stellen dürfen das nur, wenn der Anschlussnutzer vorher ausdrücklich eingewilligt hat. Der Einsatz von Auftragsverarbeitern ist zulässig (§ 49 Abs. 3 MsbG).

**Kurzübersicht zu den datenschutzrechtlichen Anforderungen des MsbG**

Teil 3 des MesbG enthält zahlreiche datenschutzrechtliche Vorgaben:

- Bereichsspezifische Rechtsgrundlage für die Datenverarbeitung, § 50 MsbG.
- Definition der Zwecke für die Datenverarbeitung, § 50 Abs. 2 MsbG.
- Kopplungsverbot, § 49 Abs. 5 MsbG.
- Verschlüsselungspflicht, § 52 Abs. 1 MsbG.

- Pflicht zur Anonymisierung oder Pseudonymisierung, soweit möglich, § 52 Abs. 3 MsbG.
- Umfassendes Auskunftsrecht und Transparenzgebot, §§ 53, 54 MsbG.
- Spezielle Regelungen zur Datenübermittlung und Löschung, §§ 60 ff MsbG.
- Eine über die abschließende Aufzählung in §§ 60 bis 64 MsbG hinausgehende Datenübermittlung ist nur bei Einwilligung des Anschlussnutzers möglich (Art. 6 Abs. 1 Unterabs. 1 Buchstabe a DS-GVO, oder wenn die Übermittlung auf nicht personenbezogene Daten beschränkt ist (§ 65 MsbG).

Jede Digitalisierung bringt datenschutzrechtliche Herausforderungen mit sich. So auch im Energiesektor mit den Smart Metern. Vor dem Hintergrund großer Vorteile im Gesamtzusammenhang – wie zum Beispiel detaillierte Verbrauchsanalyse und flexible Energielieferung – werden die datenschutzrechtlichen Risiken durch detaillierte Regelungen im MesbG ausgeglichen. Die Messstellenbetreiber, Energieunternehmen und Vermieterinnen und Vermieter sollten jedoch unbedingt darauf achten, dass den Verbraucherinnen und Verbrauchern verständliche Informationen zur Verfügung gestellt werden. So kann die nachvollziehbare Skepsis aufgefangen werden.

## 5.7 Die grenzüberschreitende Verarbeitung von Daten im Zahlungsverkehr

**Die LDI NRW setzt sich erfolgreich für die datenschutzrechtlichen Belange der Bürgerinnen und Bürger auf internationaler Ebene ein.**

Ein Bürger hatte vergeblich versucht, bei einem von ihm genutzten international tätigen Zahlungsdienstleister Auskunft nach Art. 15 DS-GVO über die von ihm verarbeiteten personenbezogenen Daten zu erhalten. Der Zahlungsdienstleister verlangte eine vollständige und ungeschwärzte Kopie des Personalausweises, obwohl der Kunde das Auskunftsersuchen in seinem im Online-Account eingeloggten Zustand über die Kommentarfunktion gestellt hatte. Auch hatte der Kunde beim Zahlungsdienstleister bereits mehrfach mit Kreditkarte gezahlt und zusätzlich seine Anschrift hinterlegt.

Wir haben uns, wie in grenzüberschreitenden Fällen üblich, über das Verfahren der europäischen Zusammenarbeit nach Art. 60 ff. DS-GVO (One-Stop-Shop-Verfahren) an die zuständige Aufsichtsbehörde in Luxemburg gewandt. Die Kolleginnen und Kollegen dort haben den Zahlungsdienstleister davon überzeugt, dass im Zusammenhang mit Auskunftsersuchen nach Art. 15 DS-GVO die Vorlage eines Personalausweises oder sonstigen Ausweises nicht mehr erforderlich ist, wenn die betroffene Person bei der Einreichung eines Antrags über ihren Kundenaccount eingeloggt ist oder das Standard-Verifizierungsverfahren des Zahlungsdienstleisters verwendet hat – also bereits hinreichend identifiziert ist.

Der Bürger bedankte sich bei der LDI NRW mit den Worten: „Es ist schön, dass man auch gegen Großkonzerne zumindest *etwas* ausrichten kann."

Die mittlerweile etablierten Verfahren zum Austausch der europäischen Aufsichtsbehörden untereinander ermöglichen es den deutschen Aufsichtsbehörden, sich auf schnelle und effektive Art und Weise für den Datenschutzschutz ihrer Bürgerinnen und Bürger einzusetzen.

## 5.8 Die Auswertung personenbezogener Daten zur Erstellung von Finanzanalysen

**Die LDI NRW koordinierte 2019 erfolgreich Beschwerden in verschiedenen Bundesländern im Zusammenhang mit den neuen Einwilligungsformularen zur Erstellung von Finanzanalysen der Sparkassen-Finanzgruppe.**

Über die Verbraucherzentrale erreichte die LDI NRW Ende 2018 die Bitte, sich mit den neuen Einwilligungsformularen zur Erstellung von Finanzanalysen der Sparkassen-Finanzgruppe auseinanderzusetzen. Auch erreichten uns einige Beschwerden unmittelbar. Im Wesentlichen wurden zwei datenschutzrechtliche Aspekte kritisiert:

- Vorausgefüllte Formulare: Die von den Sparkassen vorgelegten Formulare seien in allen Abschnitten bereits durch die Sparkasse vorangekreuzt.
- Freiwilligkeit der Einwilligungserklärung: Kundinnen und Kunden seien durch Beschäftigte der Sparkasse unter sozialem Druck oder unter Verweis auf das Geldwäschegesetz und insofern durch Täuschung zur Abgabe der Einwilligung bewegt worden. Auch sei suggeriert worden, dass die Sparkasse ohne entsprechende Erklärung die Geschäftsbeziehung nicht aufrechterhalten könne.

Ähnliche Beschwerden lagen weiteren Aufsichtsbehörden der Länder vor.

In den jeweiligen Fällen lagen besondere Umstände des Einzelfalles vor, aufgrund derer sich bei den Beschwerdeführern fälschlicherweise der Eindruck festsetzte, dass die Formulare vorausgefüllt oder die Einwilligung nicht freiwillig erteilt wurde.

Dennoch setzte sich die LDI NRW als Vorsitzende des zuständigen Arbeitskreises Kreditwirtschaft mit dem zuständigen Bundesverband – Deutscher Sparkassen- und Giroverband – DSGV – in Verbindung und bat, ihre Mitgliedsinstitute entsprechend zu sensibilisieren, dass eine Vorausfüllung unterbleibt, kein Druck auf die Kundschaft ausgeübt wird und im Rahmen der (Nicht-) Erteilung einer Einwilligung eine umfassende Information der Betroffenen erfolgt. Ergänzend regten wir an, die Formulare in einzelnen Punkten differenzierter und transparenter zu gestalten. Auch sollten die Mitgliedsinstitute ihre Kundinnen und Kunden transparent auf diese hinweisen.

Die Sparkassen-Finanzgruppe erklärte sich bereit, die Einwilligungserklärungen spätestens Ende 2019/Anfang 2020 zu überarbeiten. Auch wurden die Mitgliedsinstitute gebeten, ihre Beschäftigten zu sensibilisieren, die Vorgaben der Datenschutzbehörden beim Einsatz der Einwilligungserklärungen zu beachten. So konnte ein verbraucherfreundlicher Beitrag zu mehr Transparenz geschaffen werden.

## 5.9 Prüfung der Einhaltung datenschutzrechtlicher Vorgaben bei Banken, Versicherungen und Versorgungsunternehmen

**Nachdem sich die Unternehmen zwei Jahre auf die europäische Datenschutz-Grundverordnung haben vorbereiten können und diese seit Mai 2018 anzuwenden ist, wird der Stand der Umsetzung in drei Wirtschaftsbereichen stichprobenartig geprüft.**

Während in den Jahren 2016 bis 2018 die LDI NRW ihren Schwerpunkt auf die Beratung der Wirtschaftsunternehmen und ihrer Verbände gelegt hatte, wurden im Jahr 2019 Prüfverfahren bei Banken, Versicherungen und Versorgungsunternehmen gestartet.

Auf diesem Weg wird in Erfahrung gebracht, wo in den Unternehmen die Problemschwerpunkte in der täglichen Anwendung der DS-GVO liegen. Auch soll festgestellt werden, welche Best Practices sich herausbilden.

Die LDI NRW hat große bis mittelgroße Unternehmen ausgesucht und führt derzeit ein dreistufiges Verfahren durch:

- Zunächst werden der Geschäftsführung per elektronischem Fragebogen eine Reihe von Fragen gestellt. Dabei geht es allgemein um den Stand der Umsetzung der DS-GVO. Einen weiteren Schwerpunkt bilden Fragen zu den Rechtsgrundlagen für die Datenverarbeitungen, zum Beschwerde-Management und zu der Erfüllung der Betroffenenrechte. Auch die Praxis der Rechenschafts- und Dokumentationspflichten wird erfragt. Daneben gibt es für jede Branche wirtschaftsbereichsspezifische Fragen. Der mehrseitige Fragebogen ist im Anhang beigefügt. Die ausgefüllten Fragebögen der Unternehmen liegen nunmehr vor und müssen jetzt im Detail analysiert werden.
- In einem zweiten Schritt werden die Rückläufe ausgewertet und zunächst weiter im schriftlichen Verfahren verfolgt.
- In Einzelfällen bietet sich dann eine dritte Stufe an, wenn bei besonderen Datenschutzdefiziten Vor-Ort-Termine bei einem Unternehmen notwendig werden.

Nach einer Phase der Orientierung im neuen Recht soll durch stichprobenartige Initiativprüfungen des Datenschutz-Managements von Unternehmen ein Impuls zur Sicherstellung eines hohen Datenschutzniveaus gesetzt werden. Die wesentlichen Ergebnisse des noch laufenden Verfahrens werden im nächsten Bericht ausgeführt.

# 6. Datenschutz am Arbeitsplatz

## 6.1 Verarbeitung von Gesundheitsdaten durch Arbeitgeber – Krankmeldungen unter Nutzung von WhatsApp

**Mit der Übersendung von Krankmeldungen übermitteln Arbeitnehmerinnen und Arbeitnehmer stets sensible Daten über ihre Gesundheit im Sinne des Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) an ihre Arbeitgeber. Hierfür sind nur sichere Kommunikationswege geeignet, die Zugriffe Dritter ausschließen. Diese Voraussetzungen erfüllt der Messenger-Dienst WhatsApp nicht.**

Aufgrund einer Beschwerde wurde uns bekannt, dass ein Arbeitgeber alle Beschäftigten seines Unternehmens schriftlich dazu aufforderte, Krankmeldungen mit Belegen per WhatsApp an die Personalabteilung zu schicken.

Der Arbeitgeber erklärte der LDI NRW, dass es sich dabei nur um ein zusätzliches Angebot an die Beschäftigten zur Übermittlung von Unterlagen mit personenbezogenen Daten handelte. Aus dem entsprechenden Schreiben zur Erklärung des Verfahrens an die Beschäftigten ging allerdings gerade nicht hervor, dass dieser Weg der Übermittlung lediglich zusätzlich angeboten werde.

Außerdem hielt der Arbeitgeber die Übermittlung für sicher, da eine Ende-zu-Ende-Verschlüsselung bestehe.

Wir haben dem Arbeitgeber empfohlen, von einer Kommunikation über WhatsApp für dienstliche Zwecke generell abzusehen. Mit der Nutzung von WhatsApp sind nämlich erhebliche Risiken im Hinblick auf Zugriffe durch Unbefugte verbunden, zum Beispiel Facebook.

Facebook kann auf die Verkehrsdaten (Wer kommuniziert wann mit wem?) und auf die Bestandsdaten (Wer ist für den Dienst angemeldet?) der Nachrichten zugreifen. Zudem liest die App das Adressbuch auf dem Gerät des Nutzers aus und gleicht die Daten mit den bei WhatsApp gespeicherten Daten ab, unabhängig davon, ob die Nutzer, auf die sich die Daten beziehen, davon wissen oder dies wollen.

Das gilt auch im Fall einer Ende-zu-Ende-Verschlüsselung.

Der Arbeitgeber hat keinen Einfluss auf die Datenverarbeitungsvorgänge bei WhatsApp oder Facebook. Daher stehen ihm die erforderlichen technisch-organisatorischen Mittel für einen effektiven Schutz der Beschäftigtendaten nicht zur Verfügung. Bietet der Arbeitgeber die Nutzung von WhatsApp dennoch an, verstößt er gegen die Grundsätze der Sicherheit der Datenverarbeitung gemäß Art. 32 und 5 Abs. 1 Buchstabe f DS-GVO. Ein weiteres Risiko besteht darin, dass die Endgeräte sowohl des Arbeitsgebers als auch der Beschäftigten häufig nicht hinreichend abgesichert sind.

Der Arbeitgeber kann sich auch nicht auf eine freiwillige Mitwirkung der Beschäftigten und damit auf deren Einwilligung

im Sinne der DS-GVO berufen. Es ist nämlich davon auszugehen, dass die Beschäftigten – jedenfalls in der Regel – nicht hinreichend über die Risiken einer Kommunikation über WhatsApp und den mangelnden Schutz ihrer Daten informiert sind. Eine wirksame Einwilligung in die Nutzung von WhatsApp im Arbeitsverhältnis scheidet daher aus.

Im konkreten Beschwerdefall stellte der Arbeitgeber in der Folge unserer Hinweise das Angebot einer Kommunikation über WhatsApp an die Arbeitnehmerinnen und Arbeitnehmer ein.

Die Verbreitung eines Kommunikationsdienstes wie WhatsApp und dessen allgemeine Beliebtheit bei Anwenderinnen und Anwendern sagt nichts über die Sicherheit des Kommunikationswegs und den Schutz vor unberechtigten Zugriffen Dritter aus. Eine Nutzung dieses Dienstes durch den Arbeitgeber für den Transport von Beschäftigtendaten, insbesondere für die Übermittlung von sensiblen Daten wie Gesundheitsdaten, ist datenschutzrechtlich nicht zulässig.

## 6.2 Einsatz von Fingerabdruckscannern zur Erfassung der Arbeitszeit

**Die Erfassung der täglichen Arbeitszeit unter Verwendung von Fingerabdruckscannern ist unzulässig, da zur reinen Zeiterfassung weniger risikobehaftete Mittel zur Verfügung stehen, die die Rechte der Arbeitnehmer weniger beeinträchtigen.**

Veranlasst durch eine Beschwerde hat die LDI NRW die Frage der Zulässigkeit von Fingerabdruckscannern zum Zweck der Arbeitszeiterfassung geprüft.

Arbeitgeber sind zur Erfassung der täglichen Arbeitszeit ihrer Beschäftigten berechtigt und verpflichtet.

Der EuGH hat in einem Urteil zu Vertrauensarbeitszeit und Überstunden, die nicht genau erfasst werden (Urteil vom 14. Mai 2019, Az. C-55/18), entschieden, dass Unternehmen verpflichtet sind, ein System zur Erfassung der täglichen effektiv geleisteten Arbeitszeit der Arbeitnehmer zu schaffen. Der EuGH stützte seine Entscheidung auf die europäische Arbeitszeit-Richtlinie (2003/88/EG) sowie die EU Grundrechte Charta, die jedem Arbeitnehmer das Recht auf eine Begrenzung der Höchstarbeitszeit und auf tägliche und wöchentliche Ruhezeiten einräumt.

Unternehmen sind also nicht nur berechtigt, sondern auch verpflichtet, diese Vorgaben zu beachten. Technisch stehen dazu verschiedene Möglichkeiten zur Verfügung

Bei der Verwendung von Fingerabdruckscannern ist zu beachten, dass es sich bei solchen biometrischen Merkmalen um sensible persönliche Daten im Sinne von Art. 9 DS-GVO und § 26 Abs. 3 BDSG handelt.

Eine Speicherung der aus den entsprechenden Aufnahmen/Bildern gewonnenen Informationen, den sog. Templates, kann aus Gründen der Datensicherheit und des Datenschutzes problematisch sein.

Insbesondere bei einer zentralen Speicherung könnten die Templates von einer Person ohne Zugangsberechtigung abgefragt und bearbeitet werden. So könnte sich ein unbefugter Dritter etwa mit einem nachgemachten Fingerabdruck erfolgreich für eine andere Person ausgeben.

Biometrische Verfahren können zudem hinsichtlich der Verlässlichkeit ihrer Erkennungsrate und der Datensicherheit Fehler und Schwächen aufweisen, was besondere Risiken für die Rechte und Freiheiten der Betroffenen mit sich bringt. So können Fehler bei der Erkennung biometrischer Daten erhebliche Konsequenzen für die Betroffenen haben, zum Beispiel wenn sie hierdurch einem Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt würden.

An die Einführung und Nutzung biometrischer Erfassungs- und Identifizierungssysteme sind daher stets hohe Anforderungen im Hinblick auf die Erforderlichkeit und die Frage des Einsatzes gegenüber möglicherweise ebenso geeigneten,

aber weniger einschneidenden Maßnahmen, wie zum Beispiel der Nutzung von herkömmlichen Ausweisdokumenten oder Chipkarten mit Magnetstreifen, zu stellen.

Bei der Arbeitszeiterfassung sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten. Unzulässig sind die Erfassung besonders schützenswerter biometrischer Daten von Arbeitnehmern (vgl. dazu Art. 9 DS-GVO und § 26 Abs. 3 BDSG), zum Beispiel durch Fingerabdruck- oder Irisscanner, wenn dies nicht durch besondere Sicherheitsbedürfnisse im Unternehmen zu rechtfertigen ist. Für Zwecke der reinen Arbeitszeiterfassung sind solche Datenverarbeitungen in der Regel nicht erforderlich, da mildere Mittel zur Verfügung stehen – etwa Chipkarten, Stempelanlagen und Stundenzettel.

Im Einzelfall können besondere Umstände den Einsatz biometrischer Erfassungs- und Identifizierungssysteme rechtfertigen. So kann bei Vorliegen eines erhöhten Sicherheitsinteresses an der Personenerkennung zu Autorisierungs- und Authentifikationszwecken aus betrieblichen Gründen, etwa bei Betreten und Verlassen eines Sicherheitsbereichs, zum Beispiel in Laboren oder Forschungseinrichtungen, oder beim Einloggen in ein Firmennetzwerk der Einsatz solcher Systeme erforderlich sein. Dabei sind an die sichere Speicherung wegen der Gefahr des unberechtigten Zugriffs allerdings hohe Anforderungen zu stellen. Eine dezentrale Speicherung, etwa auf einem Token, ist daher angezeigt.

Im konkreten Fall sollten die Fingerabdruckscanner ausschließlich zur Erfassung der täglichen Arbeitszeit eingesetzt werden. Da hierfür weniger risikobehaftete technische Mittel zur Verfügung stehen, war die Erforderlichkeit der Maßnahme zu verneinen.

Infolge unserer rechtlichen Hinweise hat der Arbeitgeber von der Einführung der biometrischen Datenerhebung Abstand genommen.

Der Einsatz von Fingerabdruckscannern oder eine Verwendung von anderen biometrischen Daten ausschließlich für Zwecke der Zeiterfassung sind regelmäßig datenschutzrechtlich nicht zulässig.

## 6.3 Prüfung des Beschäftigtendatenschutzes bei Leiharbeitsunternehmen und Personalvermittlern

**Die LDI NRW hat 2019 eine Initiativprüfung im Bereich Beschäftigtendatenschutz bei Personaldienstleistern und Leiharbeitsunternehmen vorbereitet und Anfang 2020 in die Wege geleitet.**

Im Beschäftigungsverhältnis sind durch die enge soziale Beziehung und das wirtschaftliche Abhängigkeitsverhältnis die Auswirkungen von Datenschutzverletzungen für Betroffene potenziell groß. Umgekehrt sind die eigenen Schutzmöglichkeiten der beschäftigten Person gering oder mit der Gefahr von Repressalien verbunden.

Diese von Abhängigkeiten bestimmte Situation ist bei Bewerberinnen und Bewerbern sowie bei Beschäftigten in den zu untersuchenden Bereichen besonders ausgeprägt. Die Betroffenen haben oftmals nur wenige Wahlmöglichkeiten, zeitnah andere Beschäftigungsverhältnisse zu erhalten. Die Unsicherheit dieser Beschäftigungsform geht zudem oft mit geringeren Bruttoarbeitsentgelten einher.

Zur Vermittlung von Arbeitnehmern werden eine Vielzahl von Daten erhoben und mit Dritten geteilt. Daher sind solche Beschäftigtenverhältnisse potenziell besonders geeignet, tief in die Datenschutzrechte von Betroffenen einzugreifen.

Für unsere Prüfung haben wir eine Auswahl von Unternehmen zusammengestellt, die eine möglichst breite Abdeckung der Branche bietet, und die Prüfung erstreckt sich dabei jeweils auf verschiedene Bereiche der Datenverarbeitung.

Zeitarbeitnehmende haben nach § 26 Abs. 8 Nr. 1 BDSG zwei „Arbeitgeber“, das entleihende Unternehmen und das Unternehmen an das entliehen wird. Diese Aufteilung erzeugt im Vergleich zu regulären Beschäftigungsverhältnissen eine weitergehende Streuung von personenbezogenen Daten und eine damit einhergehende Unübersichtlichkeit von Verantwortlichkeiten. Daher werden die eigenen Rollenverständnisse und das Bewusstsein der datenschutzrechtlichen Verantwortlichkeit bei den zu prüfenden Unternehmen abgefragt.

Die Abgrenzung zwischen Auftragsverarbeitung und Übermittlung und die entsprechende Umsetzung in der Praxis werden untersucht. Zudem wird generell die Transparenz der Verarbeitung für die Betroffenen untersucht.

Den Betroffenen wird bei der Bewerbung eine Vielzahl von Daten abverlangt. Daher haben wir Fragen zur konkreten Erhebung der Daten von Betroffenen in der Bewerbungssituation gestellt.

Insbesondere in Bewerbersituationen ist bei Unternehmen der Arbeitnehmerüberlassung nach unserer Erfahrung die Anfertigung von Ausweiskopien nicht unüblich. Auf die Einhaltung der in diesem Zusammenhang zu beachtenden rechtlichen Vorgaben haben wir deshalb unser Augenmerk gerichtet.

Hinsichtlich der Betroffenenrechte haben wir die ausgewählten Unternehmen insbesondere um Stellungnahme zu der Wahrnehmung ihrer Informationspflichten gemäß Art. 13 und 14 DS-GVO und ihrer Auskunftspflicht gemäß Art. 15 DS-GVO gegenüber Beschäftigten und Bewerbern befragt.

Im Nachgang der Rechtsprechung des Landesarbeitsgerichts Baden-Württemberg zur Kopie von personenbezogenen Leistungsdaten auf Grundlage von Art. 15 Abs. 3 Satz 1 DS-GVO (LAG Baden-Württemberg, Urteil vom 20. Dezember 2018, Az. 17 Sa 11/18) ist es von Interesse, wie in den Unternehmen mit dem Recht des Betroffenen auf Kopie umgegangen wird.

Zudem werden die Konzepte zur Löschung der Daten und vor allem die Speicherdauer insbesondere der Bewerbungsunterlagen betrachtet.

Häufig werden Bewerberdaten an interessierte Arbeitgeber zum Zwecke der Personalauswahl übermittelt. Es wird insoweit untersucht, wie die vermittelnden Unternehmen die Möglichkeit einer Übermittlung von anonymen Bewerberdaten beurteilen.

Geprüft wird auch, welche Daten an wen auf welcher Rechtsgrundlage weitergegeben werden.

Beschäftigtendatenschutz bei Personaldienstleistern und Leiharbeitsunternehmen ist wegen der besonderen Vulnerabilität der Betroffenen ein Thema, bei dem sich die Verantwortlichen ihrer datenschutzrechtlichen Pflichten besonders bewusst sein sollten. Wir haben uns daher veranlasst gesehen, diese Branche im Rahmen einer Initiativprüfung verstärkt zu beobachten.

# 7. Videoüberwachung

## 7.1 Kfz-Kennzeichenerfassung beim Parken

**Immer mehr Parkhäuser, Parkplätze, aber auch Campingplätze sind mit Kfz-Kennzeichenerfassungssystemen ausgestattet. Mit dieser Technik soll langfristig auf Schrankenanlagen und Parktickets verzichtet werden können. Verantwortliche profitieren vor allem durch eine höhere Inkassosicherheit von den Systemen. Weitere Effekte sind zum Beispiel, dass auf die übliche Pauschale bei Verlust des Parktickets verzichtet werden kann, der Ein- und Ausfahrtprozess bei Wegfall von Parktickets beschleunigt wird und das Material für die Herstellung von Parktickets gespart wird. Parkkunden stehen den Kfz-Kennzeichensystemen oft kritisch gegenüber.**

Vermehrt gehen Beschwerden von Autofahrern zu Kfz-Kennzeichenerfassungssystemen bei uns ein. Aber auch Betreiber derartiger Systeme wenden sich mit Beratungsanfragen an uns.

Je nach Hersteller und Einsatzszenario unterscheiden sich die Kfz-Kennzeichenerfassungssysteme. Die meisten Systeme haben jedoch Folgendes gemeinsam:

Bei Einfahrt in ein Parkhaus bzw. auf einen Parkplatz wird das Kfz-Kennzeichen mit einer sog. LPR-Kamera (LPR steht für License Plate Recognition) erfasst. Die Bilder zeigen nicht das gesamte Fahrzeug, also auch nicht den Fahrer oder die Fahrerin. Es wird eine Bilddatei generiert. Über eine in die LPR-Kamera integrierte Texterkennungssoftware wird das Kfz-Kennzeichen aus der Bilddatei ausgewertet und dann gespeichert. In einer Datenbank werden zum Einfahrtsvorgang das Kfz-Kennzeichen des Parkkunden, die Bilddatei, Datum und Uhrzeit des Parkvorgangs gespeichert.

Die Bilddatei wird mit Daten abgeglichen, die zum Beispiel für eine Parkplatzreservierung oder einen dauerhaften Mietvertrag über einen Parkplatz erhoben wurden. Das Kfz-Kennzeichen dient also als „Identifizierungskennzeichen“.

Vor Verlassen des Parkhauses geben Kunden, die einen Parkplatz nicht dauerhaft gemietet haben, am Kassenautomaten ihr Kfz-Kennzeichen ein oder führen das Parkticket ein. Wird das eingegebene bzw. auf dem Parkticket hinterlegte Kfz-Kennzeichen in der Datenbank gefunden, so wird die Höhe der Parkgebühr ermittelt und der Kunde entrichtet die Parkgebühr.

Bei der Ausfahrt wird wieder mit einer LPR-Kamera das Kfz-Kennzeichen erfasst. Findet das System den zu diesem Kfz-Kennzeichen gehörigen Datensatz und wurde die Parkgebühr entrichtet, öffnet sich – sofern vorhanden – die Schranke und der Parkvorgang wird abgeschlossen. Die Daten des Bezahlvorgangs werden vor allem zur Erfüllung buchhalterischer Zwecke und zur Erfüllung handelsrechtlicher Vorschriften weiterverarbeitet.

Letzteres geschieht jedoch nicht erst seitdem Kfz-Kennzeichenerfassungssysteme eingesetzt werden. Diese Daten-

verarbeitungsvorgänge sind normalerweise mit jedem Bezahlvorgang verbunden.

Daher beziehen sich Beratungsanfragen meist gezielt auf die Datenverarbeitungsvorgänge, die mit der Erfassung der Kfz-Kennzeichen und der anschließenden Weiterverarbeitung der Kennzeichendaten verbunden sind.

Bei der Bearbeitung derartiger Anfragen prüfen wir üblicherweise zunächst, wer von der konkreten Datenverarbeitung betroffen ist. In der Regel sind mindestens folgende Betroffene zu berücksichtigen: sog. Kurzzeitparker, Kunden, die dauerhaft einen Parkplatz gemietet haben (Dauerparker) sowie Halter und Fahrer eines Kraftfahrzeugs. Auch Beschäftigte können Betroffene sein, wenn Arbeitgeber ihren Beschäftigten Parkplätze zur Verfügung stellen.

Sodann ist festzustellen, an welchem Maßstab die Rechtmäßigkeit der konkreten Verarbeitung der personenbezogenen/personenbeziehbaren Daten der Betroffenen zu prüfen ist.

Im Einzelfall können Betroffene in eine bestimmte Verarbeitung ihrer Daten eingewilligt haben (Art. 6 Abs. 1 Buchstabe a DS-GVO). Insbesondere bei der Gruppe der Dauerparker kann der Mietvertrag als Rechtsgrundlage für eine Datenverarbeitung in Betracht kommen (Art. 6 Abs. 1 Buchstabe b DS-GVO).

Letztlich haben wir bei vielen Verarbeitungsvorgängen zu prüfen, ob die Voraussetzungen des Art. 6 Abs. 1 Buchstabe f DS-GVO vorliegen. Danach ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen (in der Regel der Parkhausbetreiber) oder eines Dritten erforderlich ist, sofern nicht die Interessen der Betroffenen überwiegen.

In einem Fall hat ein verantwortliches Unternehmen dargelegt, dass ihm durch Betrugsfälle ein beträchtlicher finanzieller Schaden entsteht. Pkw-Fahrer ziehen bei Einfahrt in ein Parkhaus ein Ticket und parken ihr Fahrzeug mehrere Wochen lang. Bei der Ausfahrt wird behauptet, das Parkticket sei abhandengekommen. Bislang ist in diesen Fällen die übliche Pauschale angefallen, die bei Verlust des Parktickets erhoben wird. Die tatsächlich geschuldete Parkgebühr liegt üblicherweise deutlich darüber. Ein derartiges Vorgehen ist nicht mehr möglich, wenn das Kfz-Kennzeichen bei der Einfahrt erfasst und bis zum Verlassen des Parkhauses gespeichert wird. So kann die tatsächliche Parkdauer exakt bestimmt werden. Im vorliegenden Fall haben wir das Überwiegen des wirtschaftlichen Interesses des verantwortlichen Unternehmens bejaht.

Ein Großteil der Beschwerden richtet sich gegen fehlende oder unzureichende Hinweise und Informationen über die Kfz-Kennzeichenerfassung.

Nach Art. 5 Abs. 1 Buchstabe a DS-GVO müssen personenbezogene Daten auf rechtmäßige Art und Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies bedeutet, dass Kundinnen und Kunden mit Hinweisschildern auf den Umstand der Kfz-Kennzeichenerfassung hingewiesen werden müssen. Dies kann unter anderem durch

ein aussagekräftiges Piktogramm erfolgen. Außerdem sind den Betroffenen die Informationen nach Art. 13 DS-GVO in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln (Art. 12 Abs. 1 DS-GVO). Eine betroffene Person muss, nachdem ihr der Umstand der Kfz-Kennzeichenerfassung bekannt wird, die Möglichkeit haben, mit dem Kraftfahrzeug umzukehren und sich so der Datenverarbeitung zu entziehen.

In einigen Fällen haben wir festgestellt, dass zwar eine Hinweisbeschilderung mit Piktogramm existiert, dieses Piktogramm aber eher auf eine Videoüberwachung im Sinne von Übersichtsaufnahmen hindeutet. Dass eine Kfz-Kennzeichenerfassung erfolgt, konnte den Schildern nicht auf den ersten Blick entnommen werden.

Nicht selten treten Parkhausbetreiber an uns heran und erklären, dass eine Hinweisbeschilderung aufgrund der Lage oder Bauweise eines Parkhauses nicht möglich ist. So werden zum Beispiel Parkhäuser, die vor vielen Jahren in einer Innenstadt mit dichter Bebauung und hohem Verkehrsaufkommen errichtet wurden, umgerüstet. Oft fehlt es im Einfahrtsbereich dieser Bauten an dem Platz, der erforderlich wäre, um Fahrern vor der Einfahrt in das Parkhaus noch ein Umkehren zu ermöglichen. In diesen Fällen haben wir es als zulässig bewertet, dass Kunden die Möglichkeit haben, innerhalb einer bestimmten Zeit (wenige Minuten) nach Einfahrt in das Parkhaus dieses wieder zu verlassen, ohne dass Parkgebühren anfallen. In diesen Fällen werden die Daten, die aufgrund der Einfahrt durch das Kfz-Kennzeichenerfassungssystem verarbeitet wurden, umgehend gelöscht. So wird der Eingriff in die Rechte und Freiheiten der Betroffenen geringgehalten.

Das Parken mit Kfz-Kennzeichenerfassung ist mit einer Vielzahl von Datenverarbeitungsvorgängen verbunden, die einzeln zu bewerten sind. Beschwerden zeigen, dass die Datenverarbeitungen gegenüber den Betroffenen mitunter nicht ausreichend transparent gemacht werden.

## 7.2 Videotechnik im Kino zur Abrechnungskontrolle

**Zur Abrechnungskontrolle wird moderne Videotechnik im Kino eingesetzt. Dabei gilt es, die Aufnahmetechnik so zu gestalten, dass der Datenschutz der Kinobesucher gewahrt wird.**

Um „Schwarzseher“ zu ermitteln, überprüft der Betreiber eines Kinos die Sitzplätze in den Sälen mit Kameras. Dabei werden die belegten Plätze mit dem Kassensystem abgeglichen. Die Kameras werden automatisch 20 Minuten nach Beginn der Filmvorstellung aktiviert. Es wird zunächst ein Standbild generiert, das anschließend innerhalb eines Zeitfensters von 20 Minuten zur Kontrolle mehrmals automatisch oder manuell aktualisiert und gespeichert wird. Die Kamera wird nach Ablauf der 20 Minuten automatisch deaktiviert. Die Säle werden also nicht dauerhaft überwacht und es werden keine bewegten Bilder übermittelt oder gespeichert.

Das Programm kennzeichnet zunächst alle noch nicht verkauften Plätze mit einem grünen Rahmenfenster. Die Rahmen sind so gewählt, dass grundsätzlich die Köpfe der dort zukünftig sitzenden Personen verdeckt werden können. Wird ein – ausschließlich sitzplatzbezogenes – Kinoticket verkauft, wird der Rahmen automatisch gelb gekennzeichnet. Der Kopf des Kinobesuchers wird dann üblicherweise von dem gelben Feld überdeckt. Die Auflösung des Kamerabildes lässt nur schemenhaft erkennen, dass ein Platz belegt ist.

Wenn eine Person auf einem Platz sitzt, für den kein Ticket verkauft wurde, ist der dort vorhandene Rahmen nicht gelb gefüllt. In diesem Fall wird auf dem Standbild geprüft, ob an anderer Stelle ein Platz mit gelb gefülltem Rahmen frei ist. Das würde bedeuten, dass insgesamt die Zahl der belegten Plätze mit denen der verkauften Tickets übereinstimmt; eine weitere Prüfung findet dann nicht mehr statt. Bevor dieses Standbild nun manuell gespeichert wird, rückt das gelbe Feld manuell auf den belegten Platz und die Füllung des leeren verkauften Sitzplatzes wird entfernt. Auf diesen Platz wird dann ein blauer Rahmen gesetzt.

Zweck des so gestalteten Abgleichs zwischen gekauften und besetzten Plätzen ist der Nachweis der Abrechnungskontrolle gegenüber der Spitzenorganisation der deutschen Filmwirtschaft. Bedeutsam sind dabei nicht die Bilder, sondern die Stimmigkeit der daraus resultierenden Belegungszahlen.

Eine Beeinträchtigung des Schutzes der Daten der Kinobesucher kommt nur dann in Betracht, wenn bei dem Vorgang personenbezogene Daten verarbeitet werden.

Ein Personenbezug ist erst dann gegeben, wenn durch die Bildaufnahmen eine Individualisierbarkeit von Personen ermöglicht wird, also einzelne Personen erkennbar sind oder durch Bildbearbeitung erkennbar gemacht werden können, wenn beispielsweise Gesichtszüge sichtbar sind, oder sonstige Begleitumstände eine Identifizierung der Person ermöglichen.

Übersichtsaufnahmen oder Bildaufnahmen, die so unscharf sind oder in so geringer Auflösung erstellt werden, dass eine Identifizierung der einzelnen Personen – auch mittels Aufnahmesteuerung oder Bildbearbeitung – ausgeschlossen ist, sind keine personenbezogenen oder personenbeziehbaren Daten.

Bei einer Prüfung der verwendeten Anlage hat die LDI NRW festgestellt, dass aufgrund der Auflösung des Standbilds und der damit verbundenen Unschärfe in der Regel keine Personen identifiziert oder ihr Kriterien zur Identifizierung zugeordnet werden können.

Allerdings ist nicht völlig auszuschließen, dass Personen, die beispielsweise schräg zu ihrem Nachbarn gelehnt sitzen, mit ihrem Kopf bzw. Gesicht „aus dem Rahmen heraus fallen“ und somit möglicherweise erkannt werden könnten.

Soweit also in Einzelfällen doch relevante Daten erhoben werden, ist diese Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO zulässig, wenn sie zur Wahrung der berechtigten Interessen des Kinobetreibers erforderlich ist, sofern nicht die Interessen der Kinobesucher überwiegen.

Eine Datenverarbeitung würde dann nur in Ausnahmefällen stattfinden. Unter Berücksichtigung der Interessen des Kinobetreibers an einer ordnungsgemäßen Abrechnung und an der Verhinderung von Betrug ist das Ticketkontrollsystem als zulässig anzusehen, wenn die folgenden Maßgaben von dem Kinobetreiber eingehalten werden, um den Eingriff in die Rechte und Freiheiten der Betroffenen möglichst gering zu halten:

- Die erzeugten Standbilder werden unmittelbar nach durchgeführter Prüfung der Sitzplatzbelegung gelöscht, da sich die Zahl der verkauften Tickets dann allein aus den im System generierten Belegungszahlen ergibt.
- Die Rahmen der Sitzplatzbelegung sollten deutlich größer gezogen werden, damit eine Identifizierung von Personen in jedem Fall ausgeschlossen ist.

Zwecks Umsetzung der Informations- und Transparenzpflichten nach Art. 13 DS-GVO ist durch deutlich sichtbare und leicht erreichbare Hinweistafeln an den Kassen, den Kinoeingängen und auch im Onlinebestellsystem darauf hinzuweisen, dass zum Zweck der Ticketbelegprüfung Übersichtsstandbilder erstellt und unmittelbar nach erfolgter Prüfung gelöscht werden. Empfohlen wird, die auf der Internetseite der LDI NRW veröffentlichten Muster für die Hinweisbeschilderung und ein Informationsblatt zu verwenden (www.ldi.nrw.de). Dabei sollte darauf hingewiesen werden, dass ein Personenbezug zwar nicht beabsichtigt ist, jedoch im Einzelfall nicht ausgeschlossen werden kann.

Diese Hinweise können auch dazu beitragen, dass „Schwarzseher“ abgehalten werden.

Der Betreiber hat die Maßgaben der LDI NRW umgesetzt.

Nach Abwägung der berechtigten Interessen des Kinobetreibers und der Interessen von betroffenen Kinobesuchern im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO wurde eine für beide Seiten vertretbare Lösung gefunden, die sowohl der erforderlichen Belegungskontrolle als auch datenschutzrechtlichen Erfordernissen Rechnung trägt.

## 7.3 Prüfung von Videoüberwachung bei Großbäckereien

**Videoüberwachung wird bei Großbäckereien sowohl in den Produktionsstätten, in Filialen als auch an den Verwaltungsstandorten eingesetzt. Dabei werden sehr unterschiedliche Zwecke verfolgt. Betroffen von der Videoüberwachung sind hauptsächlich die Beschäftigten. In einigen Fällen könnte der verfolgte Zweck auch erreicht werden, ohne die Beschäftigten einer Videoüberwachung auszusetzen.**

Zu den Aufgaben der Datenschutz-Aufsichtsbehörden gehört es auch, Untersuchungen über die Anwendung der DS-GVO durchzuführen (Art. 57 Abs. 1 Buchstabe h DS-GVO).

Vor dem Hintergrund einer Reihe von Eingaben in den letzten Jahren aus diesem Umfeld haben wir uns veranlasst gesehen, den Einsatz von Videoüberwachung in Großbäckereien zu überprüfen.

In der zweiten Hälfte des Jahres 2019 wurden daher stichprobenartig sieben Großbäckereien daraufhin überprüft, ob sie Videoüberwachungsanlagen betreiben. Stellten wir dies fest, haben wir die Videoüberwachung im jeweiligen Unternehmen auf ihre Vereinbarkeit mit den Vorschriften der DS-GVO überprüft. Dazu gehörten auch Vor-Ort-Kontrollen in den Verwaltungen der Großbäckereien sowie in Bäckerei-Filialen. Die Kontrollen vor Ort erfolgten zum Teil ohne vorherige Ankündigung.

Soweit Videoüberwachung eingesetzt wurde, hat sich unsere Prüfung auf folgende Bereiche erstreckt:

- Videoüberwachung in den Filialen,
- Videoüberwachung am Verwaltungsstandort,
- Videoüberwachung in den Produktionsstätten.

**Videoüberwachung in den Filialen**

Insbesondere bei der Prüfung von Filialen haben wir unser Augenmerk auf die Beschäftigten gelegt. Filialen waren teilweise mit mehreren Kameras ausgestattet. In einigen Fällen waren die Erfassungsbereiche der jeweiligen Kameras so eingestellt, dass eine nahezu komplette Übersicht über den Arbeitsplatz möglich war. Eine Videoüberwachung der Verkaufstheke und des Bereichs dahinter greift besonderes stark in die Rechte und Freiheiten der Verkäuferinnen und Verkäufer ein, da diese sich fast während ihrer gesamten Arbeitszeit in diesem kleinen Bereich aufhalten.

Teilweise waren auch Räume videoüberwacht, die sich an den Verkaufsbereich anschließen, wie etwa Lagerräume. Allerdings halten sich in den von uns geprüften Filialen die Beschäftigten hier in der Regel nur kurz auf.

Die Zwecke, die mit einer Videoüberwachung in Bäckerei-Filialen verfolgt wurden, waren zum Beispiel:

- Abschreckung gegen Einbruch oder Überfälle,
- Wahrnehmung des Hausrechts,
- Optimierung der Warenpräsentation.

Zwar wurde in keinem Fall als Zweck die Überwachung der Beschäftigten angegeben; trotzdem sind diese davon betroffen. Eine gezielte Videoüberwachung

von Beschäftigten ist nach den Regelungen des Beschäftigtendatenschutzes grundsätzlich unzulässig und unverzüglich einzustellen.

Sofern der Zweck der Videoüberwachung nicht die Überwachung der Beschäftigten ist, beurteilt sich die Zulässigkeit in der Regel nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO. Nach dieser Vorschrift ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, und sofern nicht die Interessen, die Grundrechte oder die Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Es ist also in jedem Einzelfall festzustellen, ob für die Wahrung der von dem verantwortlichen Unternehmen ins Feld geführten Zwecke eine Videoüberwachung in dem vorgefundenen Umfang erforderlich ist. Bei der Interessenabwägung ist ferner zu prüfen, ob die Interessen des verantwortlichen Unternehmens an der Durchführung einer Videoüberwachung so schwer wiegen, dass sie das Interesse der Beschäftigten, an ihrem Arbeitsplatz unbeobachtet zu sein, überwiegen.

Als weitere Rechtsgrundlage für eine Datenverarbeitung in Form der Videoüberwachung kommt grundsätzlich auch eine Einwilligung des Betroffenen in Betracht (Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO).

Eine Einwilligung muss allerdings freiwillig erfolgen. Für die Beurteilung der Freiwilligkeit der Einwilligung sind insbesondere die im Beschäftigtenverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen (§ 26 Abs. 2 BDSG).

Ein Unternehmen ging davon aus, eine schriftliche Einwilligung der Beschäftigten in die Überwachung ihres Arbeitsplatzes reiche als Rechtsgrundlage für die Videoüberwachung aus.

Dies ist allerdings aus den genannten Gründen grundsätzlich nicht möglich, weil die von den Verkäuferinnen und Verkäufern erteilten Einwilligungen in Anbetracht der Gesamtumstände nicht als freiwillig im Sinne des Datenschutzrechtes anzusehen sind. Arbeitgeber sollten auch bedenken, dass eine Einwilligung jederzeit widerrufen werden kann.

Neben dem Grundsatz der Rechtmäßigkeit der Datenverarbeitung stellt die DS-GVO in Art. 5 Abs. 1 weitere Grundsätze auf, zu deren Einhaltung der Betreiber einer Videoüberwachungsanlage verpflichtet ist.

Beispielsweise haben wir mehrmals einen Verstoß gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c DS-GVO) festgestellt. Danach müssen personenbezogene Daten dem Zweck angemessen, erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Daten sind „erheblich“, wenn ihre Verarbeitung

geeignet ist, den festgelegten Zweck zu fördern (Vgl. Herbst, in: Kühling/Buchner: Datenschutz-Grundverordnung/BDSG Kommentar, C. H. Beck Verlag, 2. Auflage, München 2018, Art. 5 DS-GVO, Rn. 57).

In einem Fall haben wir die Videoaufnahmen beanstandet, weil sie diesen Grundsätzen nicht entsprachen; sie waren nämlich lediglich zum Zweck der Optimierung der Warenpräsentation angefertigt worden. Die Kameras waren keineswegs nur auf die Auslage gerichtet, sondern erfassten den gesamten Bereich hinter der Theke bis hin zu einer Wand, an der ebenfalls Ware ausgelegt war. Die Arbeitsplätze der Verkäuferinnen und Verkäufer wurden also komplett erfasst.

Soll festgestellt werden, ob Ware den Anweisungen der Unternehmensleitung entsprechend in der Auslage präsentiert wird, so sind ausschließlich Bilder der Auslage erforderlich. Es ist nicht erforderlich, auch Personen zu erfassen. Das erklärte Ziel kann also ohne eine Verarbeitung personenbezogener Daten (und damit durch eine Datenverarbeitung außerhalb des Anwendungsbereichs der DS-GVO) erreicht werden.

In allen geprüften Fällen waren die Beschäftigten in Bäckerei-Filialen zwar auf den Umstand der Videoüberwachung hingewiesen worden. Allerdings hatten die Beschäftigten nicht immer die Informationen erhalten, die nach Art. 13 Abs. 1 DS-GVO mitzuteilen sind.

So war Beschäftigten teilweise nicht bekannt, wer Einsicht in die Videoaufnahmen hat, die an ihrem Arbeitsplatz entstehen bzw. wer Zugriff auf das Bildmaterial hat.

**Videoüberwachung am Verwaltungsstandort**

Die meisten Unternehmen, die wir geprüft haben, betrieben Videoüberwachungsanlagen auch an ihren Verwaltungsstandorten. Zweck war die Aufklärung von Einbrüchen, Diebstählen sowie Sachbeschädigungen. Verstöße gegen die DS-GVO haben wir in diesem Bereich insbesondere bei den Hinweis- und Informationspflichten festgestellt.

In einem Unternehmen wurde zwar durch Piktogramme unübersehbar auf den Umstand der Videoüberwachung hingewiesen. Allerdings entsprachen die Informationsschilder nicht den Anforderungen des Art. 13 DS-GVO. Zum Beispiel war der Datenschutzbeauftragte mit seinen Kontaktdaten nicht genannt. Vielmehr war eine andere Stelle des Verantwortlichen angegeben. Von dieser Stelle wären Anfragen, nach einer Vorprüfung, an den Datenschutzbeauftragten weitergeleitet worden. Damit wurde nicht nur gegen den Grundsatz der Transparenz (Art. 5 Abs. 1 Buchstabe a DS-GVO) sowie gegen Art. 13 Abs. 1 DS-GVO, der die Pflichtangaben enthält, verstoßen. Wir haben hierin auch einen Verstoß gegen Art. 38 Abs. 4 DS-GVO gesehen. Nach dieser Vorschrift können betroffene Personen den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und zu mit der Wahrnehmung ihrer Rechte gemäß der DS-GVO im Zusammenhang stehenden Fragen zu Rate ziehen. Es ist sicherzustellen, dass der Datenschutzbeauftragte

für die betroffenen Personen direkt erreichbar ist. An ihn adressierte Post muss zum Beispiel ungeöffnet an ihn weitergeleitet werden oder E-Mails nur vom Datenschutzbeauftragten oder seinen hiermit beauftragten Mitarbeiterinnen und Mitarbeitern gelesen werden können. (Vgl. Bergt, in: Kühling/Buchner: Datenschutz-Grundverordnung/BDSG Kommentar, C. H. Beck Verlag, 2. Auflage, München 2018, Art. 38, Rn. 35.) Unter anderem hierauf haben wir das verantwortliche Unternehmen hingewiesen. Außerdem haben wir auf das Muster zur Erfüllung der Hinweis- und Informationspflichten aufmerksam gemacht, das die Datenschutzkonferenz (DSK) beschlossen hat und unserer Homepage www.ldi.nrw.de abrufbar ist.

**Videoüberwachung in den Produktionsstätten**

In Produktionsstätten sind wir mehrmals auf Videoüberwachungsanlagen an sog. Hygieneschleusen gestoßen. Lebensmittelverarbeitende Unternehmen sind gesetzlich zur Einhaltung bestimmter Hygienestandards verpflichtet. Deshalb sind am Eingang zum Produktionsbereich zum Beispiel Hygieneschleusen eingerichtet. Bei diesen handelt es sich um Stationen, an denen vor dem Passieren eines Drehkreuzes insbesondere die Hände zu waschen sind und Schuhsohlen automatisch gereinigt werden. Diese Hygieneschleusen werden mit Videokameras überwacht. Bei einem Vorfall, zum Beispiel einer Reklamation wegen Verunreinigungen der Backware, soll festgestellt werden können, wer unbefugt den Produktionsbereich betreten oder wer die Hygienevorschriften nicht beachtet hat. In den von uns geprüften Unternehmen erfolgte kein Monitoring. Zwar wurden die Hygieneschleusen fortlaufend gefilmt. Die Bilder wurden aber nicht in Echtzeit auf einen Monitor übertragen und somit das Geschehen an der Hygieneschleuse nicht permanent beobachtet. Auch wenn eine Echtzeitübertragung technisch möglich war, wurden die Aufnahmen nur von einem beschränkten Personenkreis eingesehen, wenn ein Vorfall gemeldet wurde (Black-Box-Verfahren).

Bei der Prüfung der Rechtmäßigkeit dieser Videoüberwachung hatten wir zu berücksichtigen, dass die Einhaltung von Hygienestandards ein gewichtiges Interesse des Unternehmens ist. Demgegenüber steht das Interesse der Beschäftigten, nicht einer Videoüberwachung am Arbeitsplatz ausgesetzt zu sein. Allerdings beschränkt sich der Erfassungsbereich der Kameras ausschließlich auf die Hygieneschleusen. Das Black-Box-Verfahren bedeutet einen geringeren Eingriff in die Rechte und Freiheiten der Betroffenen als das Monitoring. Zudem werden Beschäftigte sich nur kurz, nämlich für den Reinigungsvorgang, im Erfassungsbereich der Kameras aufhalten. Wir haben in diesem Fall die Erforderlichkeit der Videoüberwachung und ein überwiegendes Interesse des Unternehmens bejaht.

In allen Bereichen sind wir bei Vor-Ort-Kontrollen auf Kameras gestoßen, mit denen die Überwachung von wertvollen Gegenständen oder Gebäudeteilen bezweckt war. Einige dieser Kameras konnten ihren Zweck nur zeitweise erfüllen. Sie waren an Stellen montiert, die einen großen Erfassungsbereich ermöglichten. Der Erfassungsbereich war derart groß, dass – unbeabsichtigt und unnötigerweise – auch identifizierbare Personen, in der Regel Beschäftigte, aufgenommen

wurden. Außerdem wurden regelmäßig Objekte zwischen Kamera und zu überwachendem Gegenstand platziert, zum Beispiel im Außenbereich ein Lkw oder im Innenbereich ein Regalwagen. So war die Sicht auf den überwachten Gegenstand zeitweise versperrt. Der Zweck der Videoüberwachung wurde hier verfehlt. Wir haben dazu geraten, die Kameras so zu platzieren, dass es gar nicht zu Videoaufnahmen von Personen kommt. Gleichzeitig könnte der Zweck der Videoüberwachung auf diese Weise auch besser erfüllt werden.

In den geprüften Fällen haben die Unternehmen in der Folge unserer Prüfung und Beratung die Verfahren für die Zukunft datenschutzkonform umgestaltet. In Einzelfällen wurden wegen festgestellter Verstöße nach Art. 58 Abs. 2 Buchstabe b DS-GVO Verwarnungen ausgesprochen.

Wir erwarten, dass die stichprobenartige Kontrolle einiger Bäckereibetriebe eine Signalwirkung zur Verbesserung in der Branche insgesamt nach sich ziehen wird, und somit auch einen Rückgang entsprechender Beschwerden bewirken dürfte.

Mitarbeiter werden nur selten ordnungsgemäß über die Videoüberwachung informiert. Videoüberwachung, die zur Einhaltung von Hygienevorschriften eingesetzt wird, lässt sich in der Regel mit dem Datenschutzrecht in Einklang bringen. Oftmals wird der Grundsatz der Datenminimierung nicht beachtet. Dadurch kommt es zu Videoaufnahmen von identifizierbaren Personen. Diese Aufnahmen sind oft überflüssig. Das verfolgte Ziel lässt sich in diesen Fällen ohne die Verarbeitung personenbezogener Daten erreichen, sodass die DS-GVO nicht zur Anwendung kommt.

# 8. Vereine und Parteien

## 8.1 Spielberichterstattung und Liveticker über Wettkämpfe von Sportvereinen im Internet

**Auch bei der Veröffentlichung von Spielberichten und Livetickern über ein Internetportal durch Sportvereine muss das Datenschutzrecht beachtet werden. Das gilt insbesondere wenn die Spielerinnen und Spieler Kinder sind.**

Anlässlich einer Eingabe sind wir darauf hingewiesen worden, dass Sportvereine im laufenden Ligabetrieb Spielberichte und Liveticker im Internet einstellen. Im konkreten Fall waren auch Daten von Kindern betroffen.

In Sportvereinen werden bei Liga- und Freundschaftsspielen auch elektronische Spielberichte gefertigt, die nicht nur intern zur Abwicklung eines ordnungsgemäßen Spielbetriebes genutzt werden. Die Berichte werden über Internetportale anderen Interessierten zur Verfügung gestellt. Ebenso wird die Möglichkeit eröffnet, durch Liveticker zeitnah das Spielgeschehen zu verfolgen.

Veröffentlichungen von Spielberichten und Livetickern können auf Grundlage einer Interessenabwägung (Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO) auch ohne Einwilligung der betroffenen Personen ins Internet eingestellt werden.

Das gilt jedenfalls grundsätzlich für erwachsene Teilnehmerinnen und Teilnehmer der Sportveranstaltung. Beim Spielbetrieb von Kindern und Jugendlichen ist allerdings deren besondere Schutzbedürftigkeit zu beachten. Dabei sind die Interessen der Betroffenen umso schutzbedürftiger, je jünger die minderjährigen Teilnehmerinnen und Teilnehmer sind. In der Regel ist bei Kindern eine Veröffentlichung von Spielberichten und Livetickern durch einen Verein oder Verband nur mit Einwilligung der Erziehungsberechtigten zulässig. Bei Jugendlichen kommt es auf die Einsichtsfähigkeit an.

Die zulässige Dauer der Veröffentlichung von Spielberichten und Livetickern hängt von der Bedeutung des Ereignisses und dem daraus abgeleiteten Informationsinteresse der Öffentlichkeit ab: So ist etwa die Deutsche Meisterschaft bedeutender als ein Freundschaftsspiel. Bei Livetickern, die zu aktuell relevanten Sportveranstaltungen in kurzen Zeitabständen neue Informationen veröffentlichen, wird im Hinblick auf den Zweck der Verarbeitung und deren Aktualität nur ein kurzer Veröffentlichungszeitraum in Betracht kommen.

Die Veröffentlichung der Spielerdaten sind auf Vornamen, Namen, Vereinszugehörigkeit und eventuell in begründeten Ausnahmefällen den Geburtsjahrgang zu begrenzen. Auch Strafen wie beispielsweise Verwarnungen einschließlich Zeitstrafen oder Platzverweise von Spielerinnen und Spielern dürfen übermittelt werden, wenn das Informationsinteresse daran entsprechend hoch ist und entgegenstehende Interessen der Betroffenen nicht überwiegen. Hier bedarf es einer sorgfältigen Prüfung.

Spielberichte und Liveticker können grundsätzlich auch ohne Einwilligung der Spielerinnen und Spieler ins Internet eingestellt werden. Bei Kindern ist regelmäßig eine Einwilligung der Erziehungsberechtigten einzuholen bzw. bei Jugendlichen auf die Einsichtsfähigkeit abzustellen. Der Umfang der Daten und der Zeitraum der Veröffentlichung sind zu beschränken.

## 8.2 Zugangskontrollen im Vorfeld von Parteiveranstaltungen

**Die Anforderung von Personalausweisdaten und Fotos zum Zwecke des Personenschutzes im Vorfeld von Informationsveranstaltungen politischer Parteien ist unzulässig.**

Im Rahmen einer Beschwerde ist die LDI NRW darauf aufmerksam gemacht worden, dass eine politische Partei im Vorfeld von Informationsveranstaltungen die Übermittlung von Personalausweisdaten und Fotos per E-Mail als Voraussetzung für die Einladung bzw. Teilnahme an der Veranstaltung einfordert.

Zweck dieser Datenverarbeitung sollte der Personenschutz von Politikern, Rednern, Gaststättenbetreibern und auch der Besucherinnen und Besucher selbst sein. In der Vergangenheit seien Politiker der Partei angegriffen und Gaststättenbetreiber bedroht worden.

Unsere Prüfung hat ergeben, dass die von der Partei geplanten Maßnahmen nicht auf eine rechtliche Grundlage gestützt werden konnten, da es sich hierbei nicht um das mildeste Mittel handelte. Zu Identifizierungszwecken und auch zu Zwecken der Akkreditierung hätte die Vorlage des Ausweises beim Einlass zu der Veranstaltung ausgereicht. Die Beurteilung einer Gefährdungslage einer Veranstaltung und deren Absicherung fallen zudem nicht in die Zuständigkeit des Veranstalters, sondern in die der staatlichen Sicherheitsbehörden.

Die anwaltlich vertretene Partei wurde auf die Unzulässigkeit der beabsichtigten Datenverarbeitung nachdrücklich hingewiesen. Zudem wurde die Erwartung geäußert, dass der Kreisverband sich im Hinblick auf zukünftige Veranstaltungen entsprechend der Ausführungen der LDI NRW verhalten werde. Bisher sind hier keine weiteren Beschwerden bekannt.

Das Einfordern von Personalausweisdaten und Fotos im Vorfeld von Informationsveranstaltungen von Parteien ist regelmäßig unzulässig.

# 9. Gesundheit und Soziales

## 9.1 Gerichtsentscheidungen

**Bundessozialgericht zur Speicherung von Fotos nach Erstellung der elektronischen Gesundheitskarte**

Lange Zeit war umstritten, ob gesetzliche Krankenkassen das Foto der versicherten Person weiterhin speichern dürfen, wenn die elektronische Gesundheitskarte erstellt wurde. Das Bundessozialgericht hat in dieser Frage nunmehr für Klarheit gesorgt. Siehe hierzu unter 9.3.

**Bundesverwaltungsgericht zur Videoüberwachung in öffentlich zugänglichen Bereichen von Arztpraxen**

Das Bundesverwaltungsgericht hat über die Anforderungen an eine zulässige Videoüberwachung in Arztpraxen entschieden. Siehe hierzu unter 9.5.

## 9.2 Bedeutung der Patienteninformation zum Datenschutz und der Einwilligung in die Weitergabe von Gesundheitsdaten

**Trotz der Erstellung zahlreicher Informationsblätter und Mustertexte der Heilberufekammern zur Umsetzung der DS-GVO und der umfangreichen Beratung unsererseits gibt es in der Praxis immer noch Schwierigkeiten bei der Umsetzung der Vorgaben für die erforderliche Patienteninformation und für eine wirksame Einwilligungserklärung.**

Wie die vielen Anfragen und Beschwerden von Petentinnen und Petenten zeigen, bereitet die praktische Umsetzung der gesetzlichen Vorgaben im Praxisalltag Schwierigkeiten:

- Patientinnen und Patienten können wegen unübersichtlicher Formulare nicht zwischen Patienteninformation und Einwilligungserklärung unterscheiden.
- Die verwendeten Formulare entsprechen nicht den Vorgaben der DS-GVO.
- Den Patientinnen und Patienten wird die Behandlung verweigert, falls sie die Patienteninformation und/oder eine Einwilligungserklärung nicht unterschreiben.

**Patienteninformationen**

Die DS-GVO gibt keine konkreten Maßgaben vor, mittels derer den Betroffenen die verpflichtenden Informationen nach Art. 12 ff. DS-GVO mitgeteilt werden sollen. Vielmehr enthält sie lediglich die Anforderung, dass die Informationen in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu übermitteln sind. Die Wahl des Mittels ist damit grundsätzlich dem Verantwortlichen überlassen. Allerdings werden in den Art. 13 und 14 DS-GVO in zwei umfangreichen Katalogen die Informationen aufgeführt, die der betroffenen Person mindestens genannt werden müssen, damit diese als informiert angesehen werden kann.

In vielen Eingaben an die Datenschutzaufsichtsbehörden wurde geschildert, dass Ärztinnen und Ärzte die Behandlung verweigerten, wenn Patienten die Unterschrift unter die Patienteninformation ablehnten.

Daher fasste die Datenschutzkonferenz schon im Jahr 2018 dazu einen Beschluss, der klarstellt, dass sich aus der Verweigerung der Akzeptanz der Datenschutzinformationen kein Grund für eine Ablehnung der Behandlung ergibt (Siehe Beschluss der DSK „Ablehnung der Behandlung durch Ärztinnen und Ärzte bei Weigerung der Patientin oder des Patienten, die Kenntnisnahme der Informationen nach Art. 13 DSGVO durch Unterschrift zu bestätigen“ vom 5. September 2018).

**Einwilligungserklärung**

Die Verarbeitung von Gesundheitsdaten als besondere Kategorie von Daten muss den Grundsätzen des Art. 9 DS-GVO genügen.

Ausnahmen von dem grundsätzlichen Verbot der Verarbeitung von Gesundheitsdaten sind in Art. 9 Abs. 2 DS-GVO

abschließend geregelt. Die Übermittlung der Gesundheitsdaten darf unter anderem auf der Grundlage einer Einwilligungserklärung erfolgen (Art. 9 Abs. 2 Buchstabe a DS-GVO).

Für den Fall, dass keine anderen Ausnahmen nach Art. 9 Abs. 2 DS-GVO vorliegen, dürfen Datenübermittlungen an andere Ärzte oder externe Abrechnungsstellen nicht erfolgen, wenn keine wirksame Einwilligungserklärung der Patientin oder des Patienten vorliegt.

Nach Art. 7 DS-GVO muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat, sofern die Verarbeitung auf einer Einwilligung beruht. Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Stillschweigen oder Untätigkeit der betroffenen Person reichen daher nicht aus.

Darüber hinaus darf die Erfüllung eines Vertrags nach Art. 7 Abs. 4 DS-GVO nicht von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig gemacht werden, wenn die Datenverarbeitung für die Erfüllung des Vertrags nicht erforderlich ist (sog. Koppelungsverbot). Beispielhaft ist hier die Abrechnung von Behandlungsleistungen zu nennen: Zur Erfüllung des Behandlungsvertrages ist eine Einverständniserklärung zur Weitergabe der Patientendaten an ein externes Abrechnungsunternehmen nicht erforderlich, da die Abrechnung der Behandlungsleistungen im Falle einer fehlenden Einwilligung alternativ vom Arzt selber durchgeführt werden kann.

Im Praxisalltag kommt der Patienteninformation und der rechtswirksamen Einwilligungserklärung eine hohe Bedeutung zu, weil es um besonders geschützte Gesundheitsdaten geht.

Aufgrund der Dokumentations- und Nachweispflicht seitens des Verantwortlichen sind hierfür jeweils eigenständige Formulare vorzusehen. Entsprechende Mustertexte wurden in Abstimmung mit uns von den Heilberufekammern erstellt.

## 9.3 Grundsätzlich keine weitere Speicherung des Lichtbildes nach Erstellung der elektronischen Gesundheitskarte

**Lange Zeit war umstritten, ob gesetzliche Krankenkassen das Foto der versicherten Person weiterhin speichern dürfen, wenn die elektronische Gesundheitskarte erstellt wurde. Das Bundessozialgericht hat in dieser Frage nunmehr für Klarheit gesorgt.**

Nach § 291 Abs. 2 Satz 4 Fünftes Buch Sozialgesetzbuch ist die elektronische Gesundheitskarte mit einem Lichtbild der bzw. des Versicherten zu versehen. Dieses Lichtbild wurde bisher bei den Krankenkassen auch nach Anfertigung der Gesundheitskarte weiterhin gespeichert. Diese Vorgehensweise wurde damit begründet, dass das Lichtbild benötigt werde, um zum Beispiel bei Verlust der Gesundheitskarte eine Ersatzkarte auszustellen. Eine Löschung des Fotos könne erst nach Beendigung der Mitgliedschaft erfolgen.

Nachdem diese Auffassung zunächst vor dem Sozialgericht Konstanz und dem Landessozialgericht Baden-Württemberg Bestand hatte, bekam das Bundessozialgericht die Gelegenheit, sich zu dieser Frage zu positionieren. Mit Urteil vom 18. Dezember 2018 (Az. B 1 KR 31/17 R) gab es dem klagenden Krankenkassenmitglied Recht: Sobald die elektronische Gesundheitskarte ausgestellt ist, muss das Foto bei der Krankenkasse gelöscht werden. Die Speicherung des Fotos dient allein dem Zweck, die Karte auszustellen, wobei die „Ausstellung“ ein zeitlich abgrenzbarer Vorgang und gerade kein Dauerzustand ist. Die Befugnis zur Speicherung des Fotos bezieht sich nur auf eine einzige konkrete Gesundheitskarte.

Eine unserer Aufsicht unterstehende Krankenkasse haben wir auf deren Anfrage darüber unterrichtet, dass wir die Rechtsprechung des Bundessozialgerichts unserer Beratungs- und Kontrolltätigkeit zugrunde legen.

Nach unserer Auffassung lässt das Urteil des Bundessozialgerichts dennoch Raum für eine Einwilligungslösung. Wenn es im eigenen Interesse der versicherten Person liegt, das Lichtbild für die Ausstellung einer Ersatzkarte zu speichern (zum Beispiel um sich Arbeitsaufwand zu ersparen), sollte ihr die Möglichkeit eingeräumt werden, hierzu ihre Einwilligung zu erteilen. Die Einwilligung muss ausdrücklich, freiwillig und informiert sowie zweckgebunden erfolgen und soll nach § 67b Abs. 2 Satz 1 Zehntes Buch Sozialgesetzbuch schriftlich oder elektronisch erteilt werden. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Grundsätzlich müssen gesetzliche Krankenkassen das Foto der versicherten Person löschen, sobald ihr die elektronische Gesundheitskarte zur Verfügung gestellt wurde. Nur wenn die bzw. der Versicherte wirksam einwilligt, ist auch darüber hinaus die Speicherung des Lichtbildes zulässig.

## 9.4 Technische und organisatorische Maßnahmen in Arztpraxen

**Es liegen zahlreiche Beschwerden über mangelhafte technische und organisatorische Maßnahmen in Arztpraxen vor. Es ist den Verantwortlichen anzuraten, eine Prüfung der in diesem Beitrag aufgeführten Anforderungen und Maßnahmen durchzuführen und sensibel auf die Hinweise von Patientinnen und Patienten einzugehen.**

Beschwerden werden uns insbesondere dann vorgetragen, wenn auf persönliche oder postalische Hinweise Betroffener nicht oder nicht angemessen reagiert wird. Im Zuge einer Auswertung dieser Beschwerden zeigten sich wiederholt die folgenden Mängel:

**Fehlende Vertraulichkeit im Bereich der Anmeldung**
Insbesondere aufgrund von schwer veränderlichen baulichen Gegebenheiten, liegen Fälle vor, in denen keine ausreichende Trennung zwischen der Anmeldung und dem Wartebereich gegeben war. Patienten sind somit dem Risiko ausgesetzt, dass Wartende die Daten der Person und den Grund für den Arztbesuch aus dem Wartebereich im Detail erfahren können. Dies auch in der Weise, dass Bildschirminhalte auf den IT-Systemen der Anmeldung durch die Wartenden einsehbar sind. Den Verantwortlichen ist eine Prüfung anzuraten, sowohl optisch als auch akustisch für einen hinreichenden Schutz vor der Kenntnisnahme durch Dritte zu sorgen.

**Aktenaufbewahrung angrenzend zum Wartebereich**
In einigen Fällen waren Warteplätze auf dem Flur in der Nähe von Aktenschränken eingerichtet, die dem Personal der Anmeldung einen leichten Zugriff auf die Papierakten ermöglichen. Im Alltagsgeschäft kann schnell vergessen werden, diese Schränke wieder sicher zu verschließen, was eine Schutzverletzung darstellt. Der Verantwortliche muss in Bezug auf den Inhalt des Aktenschranks prüfen, ob Vertraulichkeit und Verfügbarkeit hinreichend sichergestellt sind.

**Möglichkeit des unbefugten Zugriffs auf Daten im Behandlungszimmer**
Sofern eine Patientin oder ein Patient allein im Behandlungszimmer wartet, ergibt sich in dieser Zeitspanne häufig die Möglichkeit, in Notizen, etwaige offenliegende Akten oder in angezeigte Bildschirminhalte Einsicht zu nehmen oder aktiv auf die IT-Systeme zuzugreifen. Je nach Aktualität des Systems genügt bereits das Einführen eines USB-Sticks, um das Betriebssystem zu kompromittieren und somit Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden. Neben der Sicherstellung der Aktualität der IT-Systeme ist ggf. der Arbeitsablauf entsprechend diesem Risiko so zu gestalten, dass solche Risiken vermieden werden.

**Fehlende SSL/TLS-Verschlüsselung der Webseite**
Die Webauftritte der Arztpraxen ermöglichen nicht selten auch eine Kontaktaufnahme zu Termin- oder Behandlungszwecken. Sofern personenbezogene Daten übermittelt werden, muss der Schutz

der Vertraulichkeit, Integrität und Authentizität, regelmäßig durch Einsatz von SSL/TLS, sichergestellt sein. Stichprobenartige Prüfungen zeigen hier schon deutliche Verbesserungen, da immer mehr Verantwortliche eine SSL/TLS-gesicherte Verbindung mit dem Webserver ermöglichen.

Betreiber von Arztpraxen haben Sorge zu tragen, dass der Datenschutz durch geeignete technische und organisatorische Maßnahmen sichergestellt wird. Hierzu zählt ebenfalls, dass das eingesetzte Personal auf die Entgegennahme von Hinweisen und einen sensiblen Umgang mit personenbezogenen Daten geschult ist.

## 9.5 Videoüberwachung in öffentlich zugänglichen Bereichen von Arztpraxen

**Das Bundesverwaltungsgericht hat mit seinem Urteil vom 27. März 2019 (Az. 6 C 2/18) über die Anforderungen an eine zulässige Videoüberwachung in Arztpraxen entschieden.**

Das Urteil beruhte zwar auf der Rechtslage vor Inkrafttreten der DS-GVO und berücksichtigte somit noch nicht die besonderen Regelungen des Art. 9 DS-GVO bei der Verarbeitung von Gesundheitsdaten. Dennoch enthält die Entscheidung wichtige Vorgaben für die Frage, wann eine Videoüberwachung in Arztpraxen zulässig ist und ist somit auch für die heutige Rechtslage von Bedeutung.

Allein das Anbringen von Hinweisschildern kann die Videoüberwachung nicht legitimieren. Als Rechtsgrundlage für die Videoüberwachung kommt eine Einwilligung der betroffenen Besucher der Praxis in Betracht. Voraussetzung für das Vorliegen einer rechtswirksamen Einwilligung ist aber, dass diese auf einer freien Entscheidung der betroffenen Personen beruht, und dass die Einwilligung durch eine eindeutige bestätigende Handlung erfolgt. Dem wird durch das bloße Anbringen von Hinweisschildern allerdings nicht genügend Rechnung getragen.

Die Aufnahme von Personen mittels Videoüberwachung beim Aufenthalt in einer Arztpraxis stellt nach der bisherigen wie nach der neuen Rechtslage die Verarbeitung von Gesundheitsdaten dar. So lassen sich zum Beispiel allein anhand der Tatsache, dass ein bestimmter Arzt aufgesucht wird, Rückschlüsse auf eine mögliche Krankheit der Person ziehen. Zudem sind manche Krankheiten so offensichtlich, dass sie einem Patienten quasi „ins Gesicht geschrieben stehen“. Ebenso ist es unerheblich, wenn unter der Mehrzahl der Besucher der Praxis auch solche sind, die selber keine Patienten sind, sondern die Praxis aus anderen Gründen aufsuchen. Denn es reicht schon aus, dass nur eine Person von den Besuchern aus gesundheitlichen Gründen die Praxis aufsucht, um die Videoüberwachung rechtlich insgesamt als Erhebung von Gesundheitsdaten zu bewerten. Die Verarbeitung von Gesundheitsdaten ist ohne Vorliegen eines Ausnahmetatbestandes nach Art. 9 Abs. 2 DS-GVO grundsätzlich unzulässig. Häufig geben Ärzte und Ärztinnen an, sich vor möglichen Straftaten schützen zu wollen, da die Videoüberwachung eine abschreckende Funktion besitzt. Dies stellt jedoch nach der neuen Rechtslage keinen zulässigen Ausnahmetatbestand nach Art. 9 Abs. 2 DS-GVO dar. Daher kommt in Praxisräumen eine Videoüberwachung nur restriktiv und nur in Einzelfällen in direktem Zusammenhang mit Maßnahmen der Gesundheitsvorsorge bzw. konkreten gesundheitlichen Behandlungen in Betracht. Denkbar wäre zum Beispiel eine Videoüberwachung eines abgetrennten Raumes oder Teilbereichs zur Beobachtung von Patienten mit besonderen Risiken. Dabei ist jedoch ein strenger Maßstab an die Erforderlichkeit der Videoüberwachung anzulegen. Zu prüfen wäre demnach vorrangig, ob das Wohl der Patienten nicht durch andere Maßnahmen sichergestellt werden kann, beispielsweise durch eine Überwachung durch

medizinisches Personal oder einen Notrufschalter.

Die Überwachung von öffentlich zugänglichen Bereichen in Arztpraxen ist in der Regel ohne das Vorliegen einer wirksamen Einwilligung unzulässig. Ärztinnen und Ärzte sind gut beraten, die Voraussetzungen für eine zulässige Videoüberwachung in ihrer Praxis genau zu überprüfen.

## 9.6 Prüfaktion zur Nutzung von Internethandelsplattformen durch Apotheken

**Die Nutzung der Internethandelsplattform „Amazon Market Place“ durch Apotheken wird stichprobenartig auf Einhaltung der datenschutzrechtlichen Vorgaben geprüft.**

Auch im Gesundheitsbereich wird die Nutzung moderner Internethandelsplattformen wie „Amazon Market Place“ immer beliebter. Dies gilt auch für Apotheken, die mittels dieser Plattform als unabhängige Verkäufer eigene Arzneimittel bewerben und anbieten. Bei dieser Nutzung müssen datenschutzrechtliche Vorgaben eingehalten werden.

Da bei dem Kauf- bzw. Anmeldeprozess besonders zu schützende Gesundheitsdaten im Sinne von Art. 9 DS-GVO verarbeitet werden, muss sichergestellt sein, dass die Kunden vorab rechtswirksame Einwilligungen zur Verarbeitung ihrer Gesundheitsdaten erteilt haben.

Mit unserer stichprobenartigen Prüfung wollen wir den Sachverhalt beleuchten und die Apotheken sowie deren Kundinnen und Kunden sensibilisieren. So wurden bereits zwölf Apotheken, die Medikamente auf der Plattform von Amazon Market Place anbieten, unter datenschutzrechtlichen Gesichtspunkten zur Stellungnahme aufgefordert. Die Verfahren sind noch nicht abgeschlossen.

Soweit wir feststellen, dass die Verfahren insbesondere vor dem Hintergrund der aktuellen Rechtsprechung nicht rechtskonform gestaltet sind, werden wir angemessene Maßnahmen ergreifen.

Mit einer Prüfung der Praxis von Apotheken beim Einsatz von Internethandelsplattformen soll kontrolliert werden, ob dabei der besondere Schutz von Gesundheitsdaten gewährleistet wird.

## 9.7 Überprüfung privatärztlicher Abrechnungsunternehmen

**Die Abrechnungspraxis von privatärztlichen Abrechnungsunternehmen wird stichprobenartig unter dem Gesichtspunkt der Einhaltung der datenschutzrechtlichen Vorgaben geprüft.**

Der Einsatz von privatärztlichen Abrechnungsunternehmen stellt eine langjährige Praxis der Ärzteschaft dar. Dabei besteht die besondere Konstellation darin, dass die die Einwilligung zur Datenverarbeitung nicht durch die datenverarbeitende Stelle – also das Abrechnungsunternehmen – eingeholt wird, sondern durch den behandelnden Arzt bzw. die Ärztin. Je nach Fallgestaltung erfolgt die Datenverarbeitung nicht nur zu Abrechnungszwecken, sondern umfasst auch die Einholung von Bonitätsauskünften oder die Weiterabtretung an ein Kreditinstitut.

Aufgrund von Eingaben zu dieser Praxis wollen wir die Verfahren der Unternehmen näher untersuchen und dabei unser Augenmerk auf die Rahmenbedingungen bei der Einholung von Einwilligungen legen. In NRW wurden bereits sieben privatärztliche Abrechnungsunternehmen datenschutzrechtlich überprüft. Eine länderübergreifende Abstimmung zwischen den Aufsichtsbehörden unter Beteiligung betroffener Akteure – wie die Bundesärztekammer – soll dazu führen, dass einheitliche Vorgaben erarbeitet werden.

Sowohl die Unternehmen als auch Ärzte und Patienten sollen für die rechtlichen Probleme des Verfahrens sensibilisiert werden. Als Folge der Prüfung werden die Verfahren bei Bedarf den rechtlichen Vorgaben entsprechend anzupassen sein.

Mit der stichprobenartigen Überprüfung privatärztlicher Abrechnungsunternehmen wollen wir die Einhaltung datenschutzrechtlicher Vorgaben bei diesen Abrechnungen kontrollieren und sicherstellen.

# 10. Innere Sicherheit und Justiz

## 10.1 Gerichtsentscheidungen

**Bundesverfassungsgericht zu Kennzeichenerfassungen durch Polizeibehörden**

Das Bundesverfassungsgericht stellt in seiner Entscheidung vom 18. Dezember 2019 (Az. 1 BvR 142/15) ausdrücklich fest: Ein Kfz-Kennzeichen ist ein personenbezogenes Datum, dessen Verarbeitung immer einer Rechtsgrundlage bedarf. Es führt dazu aus, dass bereits jede Erfassung eines Kfz-Kennzeichens einen Grundrechtseingriff darstellt, unabhängig davon, ob im Weiteren eine Speicherung erfolgt, der Abgleich in den polizeilichen Dateien zu einer Übereinstimmung führt und/oder ggf. weitere polizeiliche Maßnahmen ausgelöst werden. Damit korrigiert das Bundesverfassungsgericht eine vielzitierte eigene Entscheidung aus dem Jahr 2008. Hintergrund der aktuellen Entscheidung war der automatische Abgleich von Kennzeichen zu Fahndungszwecken in Bayern.

**Verwaltungsgerichtsbarkeit Niedersachsen zur Verkehrsüberwachung mittels abschnittsbezogener Geschwindigkeitskontrolle („Section Control“)**

„Section Control“ ist eine in Deutschland neuartige Methode zur Feststellung und Ahndung von Geschwindigkeitsverstößen. Im Unterschied zu herkömmlichen punktuellen Geschwindigkeitsmessungen wird dabei auf einer definierten Strecke die Durchschnittsgeschwindigkeit der Fahrzeuge errechnet. Die Verwaltungsgerichtsbarkeit Niedersachsen hat im Jahr 2019 in verschiedenen Entscheidungen festgestellt, dass Verkehrsüberwachungen mittels „Section Control“ durch die Polizei – und zwar auch schon während einer Pilotphase – einer ausdrücklichen Rechtsgrundlage bedürfen. Bestehende Vorschriften des Bundes und des Landes Niedersachsen seien nicht ausreichend (vgl. Verwaltungsgericht Hannover, Beschluss vom 12. März 2019, Az. 7 B 850/19, sowie bestätigend Oberverwaltungsgericht Lüneburg, Beschluss vom 10. Mai 2019, Az. 12 ME 68/19). Vielmehr bedürfe es einer bereichsspezifischen, präzisen und normenklaren Rechtsgrundlage. Dies gilt in Anlehnung an die oben genannte Entscheidung des Bundesverfassungsgerichts zur Zulässigkeit automatisierter Kennzeichenkontrollen auch für Fälle, in denen die erhobenen Daten mangels Vorliegen einer Geschwindigkeitsüberschreitung sofort nach Abschluss der Messung wieder gelöscht werden.

Eine mögliche Rechtsgrundlage stellt nach Auffassung des Oberverwaltungsgerichts Lüneburg die nunmehr neu geschaffene Regelung in § 32 Abs. 7 Niedersächsisches Sicherheits- und Ordnungsgesetz dar (vgl. Oberverwaltungsgericht Lüneburg, Beschluss vom 03. Juli 2019, Az. 12 MC 93/19).

## 10.2 Strategische Fahndung: Umfangreiche Datenverarbeitung, kein messbarer Erfolg zur Gefahrenabwehr

**Der erste Einsatz des neuen polizeilichen Mittels der sog. „Strategischen Fahndung“ hat zu tausenden Kontrollen von Passantinnen und Passanten inklusive deren Identitätsfeststellungen geführt, ohne den angestrebten polizeilichen Erfolg zu erreichen.**

Im Frühjahr 2019 wurde in NRW erstmals das mit der Reform des Polizeigesetzes NRW (PolG NRW – siehe 24. Bericht unter 9.1) geschaffene Instrument der „Strategischen Fahndung“ eingesetzt. § 12a PolG NRW erlaubt der Polizei, bei Vorliegen bestimmter Voraussetzungen für einen Zeitraum von zunächst bis zu 28 Tagen in einem festgelegten Gebiet Personenkontrollen und Identitätsfeststellungen durchzuführen sowie Einsicht in Fahrzeuge zu nehmen. Diese polizeigesetzliche Vorschrift dient der Gefahrenabwehr. Mit der Maßnahme sollen also Gefahren, wozu auch bevorstehende Straftaten gehören, verhindert werden. Die Verfolgung von begangenen Straftaten oder Ordnungswidrigkeiten ist hiervon dagegen nicht umfasst. Für diese repressiven Zwecke stehen der Polizei die Mittel der Strafprozessordnung zur Verfügung.

Mehrere Sachverständige hatten schon im Gesetzgebungsverfahren das zu befürchtende Missverhältnis von Anzahl und Ausmaß der mit der Maßnahme einhergehenden Grundrechtseingriffe bei unbeteiligten Personen zu den zu erwartenden Erfolgen der Maßnahme kritisiert. Auch wir hatten uns in unserer Stellungnahme an den Landtag vom 30. Mai 2018 unter anderem zu dieser Vorschrift kritisch geäußert (vgl. Landtag-Stellungnahme 17/645; 24. Bericht unter 9.1). Diese Befürchtungen haben sich in der Anwendungspraxis nunmehr bestätigt.

Die konkret durchgeführte erste „Strategische Fahndung“ sollte der Bekämpfung des Wohnungseinbruchsdiebstahls dienen. Die Kontrollen wurden in Gebieten und zu Zeiten durchgeführt, in denen nach der Statistik verhältnismäßig viele Wohnungseinbrüche begangen werden. Die Polizei erhoffte sich von der Maßnahme Hinweise auf bevorstehende oder durchgeführte Wohnungseinbrüche. Zu diesem Zweck wurden über mehrere Wochen insgesamt über 5.000 Personen und über 2.000 Fahrzeuge kontrolliert.

Das Ergebnis kann aus polizeilicher Sicht nur als ernüchternd betrachtet werden: Die gesamte Maßnahme hat nicht einen konkreten Hinweis auf einen geplanten oder begangenen Wohnungseinbruchsdiebstahl ergeben, und auch die Anzahl der Wohnungseinbrüche hat sich im Zeitraum der Maßnahme gegenüber dem Vorjahreszeitraum nicht zum Positiven verändert.

Aus datenschutzrechtlicher Sicht ist das Ergebnis katastrophal: Die Daten tausender Personen sind polizeilich verarbeitet worden, ohne dass diese hierzu einen Anlass gegeben hätten. Dies allein ist schon äußerst kritisch zu sehen. Diese so zahlreichen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen wiegen jedoch besonders schwer, wenn die

Maßnahme – wie hier – nicht zum angestrebten polizeilichen Erfolg der Gefahrenabwehr geführt hat.

Einschließlich des von uns stichprobenhaft geprüften Falls gab es laut Bericht des Innenministeriums im Innenausschuss des Landtages am 12. Dezember 2019 (Ausschussprotokoll 17/856) bis dato insgesamt 44 angeordnete Maßnahmen der „Strategischen Fahndung“ in NRW.

Eine abschließende Bewertung der „Strategischen Fahndung“ ist sicherlich noch verfrüht. Der von uns geprüfte Fall bestätigt jedoch zunächst die Kritik an der Regelung im Vorfeld ihres Inkrafttretens.

## 10.3 Zentrales Fahndungsportal der Polizei NRW mit Startschwierigkeiten

**Das neue zentrale Online-Fahndungsportal der Polizei NRW ist ein wichtiges Instrument zur Erhöhung der Reichweite von Suchanzeigen im Rahmen von Öffentlichkeitsfahndungen. Allerdings wurden dort im Anfangszeitraum mehr Daten eingestellt, als für die Aufgabenerfüllung erforderlich waren.**

Nachdem eine im Jahr 2012 gestartete erste Version für ein zentrales Online-Fahndungsportal kurz nach dem Start aus sicherheitstechnischen Gründen eingestellt worden war, nahm die Polizei NRW im November 2018 ein neues Online-Fahndungsportal in Betrieb. Alle Kreispolizeibehörden sind gehalten, Öffentlichkeitsfahndungen nach gesuchten Straftäterinnen und -tätern oder vermissten Personen in diesem Portal zu veröffentlichen. Durch mediale Berichterstattung wurde allerdings kurz nach seiner Inbetriebnahme bekannt, dass insbesondere bei Suchaufrufen nach vermissten oder verdächtigen Personen in mehreren Einzelfällen mehr Daten in der Suchanzeige aufgeführt waren, als für die Suche oder zum Schutz der Bevölkerung sowie von hinweisgebenden Personen erforderlich waren. Hierbei handelte es sich teils um sehr sensible Angaben, zum Beispiel zur Gesundheit oder zu Minderjährigen.

Bei der der Medienberichterstattung nachgelagerten Prüfung stellten wir fest, dass die polizeiinternen Abläufe zwischenzeitlich überarbeitet und verschiedene Verbesserungen initiiert worden waren: Die Polizei überprüfte vorsorglich alle damals veröffentlichten Vermisstenanzeigen, bereinigte sie ggf. und löschte zum Beispiel konkrete Namensangaben. Die beteiligten Kreispolizeibehörden wurden nochmals sensibilisiert, ausschließlich erforderliche Daten in die Fahndungsanzeige aufzunehmen. Zudem findet inzwischen vor der Veröffentlichung eine abschließende zentrale Qualitätsprüfung der Anzeigen seitens der Polizei statt.

Im Ergebnis konnte somit festgestellt werden, dass das Verfahren der Erstellung und Veröffentlichung von Suchanzeigen im zentralen Online-Fahndungsportal nunmehr datenschutzgerecht ausgestaltet ist. Dabei erhöht die zentrale Vorhaltung des Systems zudem sogar die Gewähr für einheitliche, qualitätsgeprüfte Fahndungsanzeigen.

Nach anfänglichen Auffälligkeiten in mehreren Einzelfällen wurden seitens der Polizei korrigierende Maßnahmen getroffen. Die Beschränkung der Anzeigeninhalte auf erforderliche Daten wurde inzwischen sichergestellt.

# 11. Verwaltung

## 11.1 Beratung öffentlicher Stellen

Wegen der anhaltend hohen Nachfrage wurde die in Kooperation mit den kommunalen Spitzenverbänden durchgeführte Veranstaltungsreihe rund um diverse Themen der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) sowie der Anwendung des novellierten Datenschutzgesetzes NRW fortgesetzt. Der Schwerpunkt lag hierbei weiterhin auf Fragen und Hilfestellungen zur Anwendung der neuen Rechtsvorschriften in der kommunalen Praxis. Um diese Themen ging es auch im Erfahrungsaustausch mit einem kommunalen Datenschutzbeauftragten, der Konzepte zur Umsetzung der europarechtlichen und nordrhein-westfälischen Vorschriften in seiner Kommune erstellt hatte. Fortgesetzt wurden auch die bereits seit vielen Jahren etablierten Erfahrungsaustauschrunden mit den behördlichen Datenschutzbeauftragten der nordrhein-westfälischen Hochschulen und mit dem Justizministerium NRW. Erfreulicherweise konnten darüber hinaus einige zusätzliche Vortragsbitten erfüllt werden.

- So hielten wir einen Vortrag mit anschließender Diskussion beim Ambulanten Sozialen Dienst (ASD) zur neuen Systematik der Datenschutzvorschriften sowie zu den spezifischen Rechtsgrundlagen für die Datenverarbeitung durch den ASD.
- Eine Präsentation nebst Diskussion beim Arbeitskreis Denkmalschutz des Städtetages hatte die Datenschutzanforderungen im Zusammenhang mit digitalen Denkmallisten zum Gegenstand.
- Bei einer Veranstaltung der Kommunalagentur NRW ging es für uns darum, in einem Vortrag mit anschließender Diskussion die datenschutzrechtlichen Vorschriften im Vergabeverfahren der öffentlichen Auftraggeber mit dem Schwerpunkt Erstellung von Vergabeunterlagen zu erläutern.
- Eher allgemeine Grundlagen zu den Anforderungen und zur Umsetzung der DS-GVO sowie des DSG NRW wurden auf Wunsch des Arbeitskreises der Hochschuljuristinnen und -juristen für Drittmittel dargelegt.

Gerne würden wir unsere Vortragstätigkeit noch weiter verstärken und noch mehr Einladungen annehmen, allerdings stoßen wir dabei – insbesondere auch angesichts der vielen anderen wichtigen Aufgaben der LDI NRW – immer wieder an unsere Kapazitätsgrenzen.

## 11.2 Auskunft nach Art. 15 DS-GVO bei öffentlichen Stellen

**Der Auskunftsanspruch nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) hat gerade bei öffentlichen Stellen des Landes NRW zu einigen Unsicherheiten geführt. Gelegentlich sind die gesetzlichen Anforderungen dort noch nicht hinreichend bekannt oder die Auskunftssuchenden haben unzutreffende Vorstellungen über Voraussetzungen und Grenzen dieses Anspruchs.**

Seit einigen Monaten wenden sich vermehrt Bürgerinnen und Bürger an uns, die bei einer öffentlichen Stelle eine Auskunft nach Art. 15 DS-GVO beantragt haben und mit der Bearbeitung unzufrieden sind. Folgende Fallgestaltungen treten dabei schwerpunktmäßig auf:

**Einwohnerinnen und Einwohner einer Kommune bitten die Stadtverwaltung um umfassende Auskunft zu allen personenbezogenen Daten, die über sie bei der Kommune gespeichert sind.**
Zu Recht kann hier die Kommune verlangen, dass die Antragstellenden ihren Auskunftsanspruch auf bestimmte Ämter oder Sachverhalte konkretisieren. Das Recht auf Auskunft nach Art. 15 DS-GVO kann vom nationalen Gesetzgeber unter den Voraussetzungen des Art. 23 Abs. 1 und 2 DS-GVO beschränkt werden. Der nordrhein-westfälische Gesetzgeber hat mit § 12 Datenschutzgesetz NRW (DSG NRW) von dieser Möglichkeit Gebrauch gemacht. Dort heißt es in Abs. 1 Sätze 1 und 2: „Soweit der Verantwortliche große Mengen von Informationen über die betroffene Person verarbeitet, kann er bei einem Auskunftsersuchen verlangen, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht. Das Auskunftsrecht setzt voraus, dass die betreffende Person Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglicht."

Zu berücksichtigen ist, dass es bei einer Kommune in aller Regel gerade keine übergreifende Datenbank zur Auffindung von Datensätzen gibt. Es müsste vielmehr in jedem Amt nachgeforscht werden, ob dort Daten zu einer betroffenen Person vorliegen. Gerade das wollte der nationale Gesetzgeber vermeiden. Aus diesem Grund ist es auch nicht erforderlich, zunächst festzustellen, dass tatsächlich eine große Menge an Daten über die betroffene Person verarbeitet wird; § 12 Abs. 1 Satz 2 DSG NRW gilt unabhängig von Satz 1. Die Auskunftssuchenden müssen ihre Anfragen deshalb hinreichend konkretisieren, um eine Bearbeitung zu ermöglichen.

**Die öffentliche Stelle erteilt die Auskunft erst nach Ablauf eines Monats oder entschuldigt sich nach dieser Zeit dafür, dass noch keine Auskunft erfolgt ist, und stellt diese zeitnah in Aussicht.**
Gemäß Art. 12 Abs. 3 DS-GVO muss die öffentliche Stelle die Auskunft unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags erteilen. Diese Frist kann unter Berücksichtigung der Komplexität und der Anzahl von Anträgen um zwei Monate verlängert werden. Darüber muss die öffentliche Stelle jedoch innerhalb der Monatsfrist

informieren. Sie muss dabei auch die Gründe für die Verlängerung angeben.

**Die öffentliche Stelle übersendet als Auskunft ein Datenblatt, in dem aufgeführt wird, welche Kategorien von Daten über die betroffene Person in den einzelnen Ämtern vorliegen.**
Zunächst reicht es nicht, nur anzugeben, welche Kategorien von Daten über die betroffene Person gespeichert sind. Die öffentliche Stelle muss diese Daten vielmehr auch konkret benennen, damit die betroffene Person sie kontrollieren und ggf. berichtigen lassen kann.

Weiterhin sind nach Art. 4 Nr. 1 DS-GVO personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Daher unterfallen diesem Begriff nicht nur (Stamm-)Daten wie zum Beispiel Adresse, Kontaktdaten, Geburtsdatum, Kontoverbindungen, Kfz-Kennzeichen oder Mülltonnengröße, sondern auch Schriftstücke wie Bescheide, Beschwerdeschreiben der Person, Stellungnahmen der öffentlichen Stelle zu den Beschwerden, Vermerke, (behördeninterne) E-Mails und ähnliches, da solche Dokumente Aussagen enthalten, die sich auf eine identifizierbare natürliche Person beziehen. Nicht umfasst sind aber beispielsweise abstrakte Rechtsgutachten (diesbezüglich kommt aber ggf. ein informationsfreiheitsrechtlicher Anspruch in Betracht) oder Ablichtungen von Kommentaren.

**Die öffentliche Stelle hat eine grundsätzlich datenschutzkonforme Auskunft erteilt, die betroffene Person bemängelt diese jedoch als unvollständig.**
In dieser Fallkonstellation stößt die Aufsichtstätigkeit der LDI NRW vielfach an ihre Grenzen. Dies liegt daran, dass wir letztendlich nicht überprüfen können, ob eine öffentliche Stelle eine Auskunft tatsächlich vollständig erteilt hat oder ob dort noch weitere Daten über die betroffene Person vorhanden sind. Solche Beschwerden können wir daher nur bis zu einem bestimmten Grad und auch nur dann bearbeiten, wenn die Antragstellenden konkret benennen, welche Daten in der Auskunft fehlen.

Bei der Erteilung von Auskünften nach der DS-GVO besteht bei öffentlichen Stellen noch Klärungsbedarf.

## 11.3 Prüfaktion zu Datenschutzbeauftragten bei Jobcentern der Kommunen in NRW

**Jobcenter der Kommunen sind datenschutzrechtlich eigenständige Verantwortliche und müssen sämtliche Pflichten des Datenschutzrechts umsetzen, zu denen auch die Pflicht zur Benennung von Datenschutzbeauftragten gehört. Dazu haben wir im Jahr 2019 eine Prüfung durchgeführt.**

Gegenstand der Prüfaktion war die Frage, ob die Jobcenter in den Kommunen eigene Datenschutzbeauftragte benannt und deren Kontaktdaten an geeigneter Stelle veröffentlicht haben, sowie ob diese der LDI NRW gemäß Art. 37 Abs. 7 Datenschutz-Grundverordnung (DS-GVO) gemeldet worden sind. Dabei haben wir alle kommunalen Jobcenter in NRW geprüft. Für Jobcenter, die als gemeinsame Einrichtungen von Kommunen und Agentur für Arbeit betrieben werden, ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig.

Durch die DS-GVO ist die Stellung von Datenschutzbeauftragten gestärkt worden. Sie nehmen nicht mehr nur eine interne Beratungs- und Kontrollfunktion wahr, sondern dienen nunmehr auch bei Behörden als direkter Ansprechpartner sowohl für die betroffenen Personen außerhalb der Behörde als auch für die Aufsichtsbehörde (vgl. Art. 38 Abs. 4, Art. 39 Abs. 1 Buchstaben d, e DS-GVO). Um diese Funktion auch sinnvoll wahrnehmen zu können, müssen die Kontaktdaten von Datenschutzbeauftragten leicht auffindbar sein. Der LDI NRW müssen die Kontaktdaten mitgeteilt werden (Art. 37 Abs. 7 DS-GVO).

Nach Art. 37 Abs. 1 Buchstabe a DS-GVO benennen Verantwortliche und Auftragsverarbeiter auf jeden Fall Datenschutzbeauftragte, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird.

Für Behörden und öffentliche Stellen gilt nach der DS-GVO somit europaweit eine generelle Pflicht zur Benennung von Datenschutzbeauftragten.

Stellen mit Aufgaben nach dem Sozialgesetzbuch (SGB), wie etwa Jobcenter, stellen eigenständige Verantwortliche dar und sind insoweit von der Gemeinde als Verantwortliche im Sinne des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) zu unterscheiden.

Dies macht die Regelung des § 67 Abs. 4 Zehntes Buch Sozialgesetzbuch (SGB X) deutlich:

*„Werden Sozialdaten von einem Leistungsträger im Sinne von § 12 des Ersten Buches verarbeitet, ist der Verantwortliche der Leistungsträger. Ist der Leistungsträger eine Gebietskörperschaft, so sind der Verantwortliche die Organisationseinheiten, die eine Aufgabe nach einem der besonderen Teile dieses Gesetzbuches funktional durchführen.“*

Nach § 67 Abs. 4 Satz 2 SGB X kommt es demnach darauf an, welche Organisationseinheit die Aufgaben funktional wahrnimmt.

Das bedeutet, dass diese Stellen, wie etwa Jobcenter, als eigenständige Verantwortliche auch sämtliche Pflichten des

Datenschutzrechts umsetzen müssen, zu denen auch die Pflicht zur Benennung von Datenschutzbeauftragten gehört.

Als Datenschutzbeauftragte können geeignete Personen innerhalb oder außerhalb des Verantwortlichen bzw. des Auftragsverarbeiters benannt werden. Behörden oder öffentliche Stellen haben ferner die Möglichkeit, für mehrere Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe gemeinsame Datenschutzbeauftragte zu benennen (Art. 37 Abs. 3 DS-GVO). So ist beispielsweise denkbar, dass Datenschutzbeauftragte der Kommunen zugleich als Datenschutzbeauftragte für Jobcenter benannt werden können. Hierzu bedarf es allerdings eines gesonderten Benennungsaktes.

Der Bezug auf Organisationsstruktur und Größe bedeutet auch, dass Verantwortliche und Auftragsverarbeiter sicherstellen müssen, dass gemeinsame Datenschutzbeauftragte in der Lage sind, die Aufgaben zu erfüllen, welche ihnen in Bezug auf sämtliche Behörden oder öffentlichen Stellen übertragen wurden.

Der Schwerpunkt der Prüfaktion lag bei der Frage, ob die Jobcenter ihre Pflicht zur Benennung von Datenschutzbeauftragten erfüllt haben. Dazu haben wir zunächst die öffentlich zugänglichen Informationen ausgewertet, insbesondere die Internetseiten der Kommunen. In der Regel mussten weitere Informationen per Fragebogen eingeholt werden. Insgesamt haben wir 12 Kreise, 6 kreisfreie Städte und 78 kreisangehörige Gemeinden überprüft.

Die Prüfung hatte folgendes Ergebnis:

Die Jobcenter der kreisangehörigen Gemeinden sahen sich überwiegend nicht in der Pflicht, eigene Datenschutzbeauftragte zu benennen, sondern verwiesen auf die Datenschutzbeauftragten der jeweiligen Kreise. Ein ebenfalls großer Teil der Kommunen hielt den eigenen kommunalen Datenschutzbeauftragten automatisch auch für zuständig für die Jobcenter-Aufgaben, die von den Kreisen übertragen wurden.

Bei einem Teil der kreisfreien Städte war nicht erkennbar, ob der gemeldete kommunale Datenschutzbeauftragte auch eigens für das jeweilige Jobcenter benannt wurde.

Die LDI NRW hat die Jobcenter darauf hingewiesen, dass es nach § 67 Abs. 4 Satz 2 SGB X darauf ankommt, welche Organisationseinheit die Aufgabe funktional wahrnimmt. Nimmt der Kreis oder die kreisfreie Stadt die Aufgabe des Jobcenters wahr, ist die entsprechende Organisationseinheit des Kreises bzw. der kreisfreien Stadt der Verantwortliche. Ist die Aufgabe auf eine kreisangehörige Gemeinde ausgelagert, ist deren entsprechende Organisationseinheit der Verantwortliche. Das bedeutet, dass kommunale Datenschutzbeauftragte oder Datenschutzbeauftragte des Kreises, der die Aufgabe übertragen hat, nicht automatisch auch Datenschutzbeauftragte des Jobcenters sind.

In der Praxis muss demnach grundsätzlich das Jobcenter als Verantwortlicher eine Datenschutzbeauftragte oder einen

Datenschutzbeauftragten benennen. Idealerweise geschieht dies auf schriftlichem Wege.

Möglich ist auch, dass der Bürgermeister (im Fall der Auslagerung der Aufgabe des Jobcenters auf die kreisangehörige Gemeinde) bzw. der Landrat (im Fall, dass die Aufgabe des Jobcenters nicht auf die kreisangehörigen Gemeinden ausgelagert wurde) die Benennung von Datenschutzbeauftragten für Jobcenter vornimmt. Hierzu kann eine bereits für die Kommune bestehende Benennungsurkunde so ergänzt werden, dass die bzw. der Datenschutzbeauftragte auch für das Jobcenter benannt wird. Es handelt sich dann um gemeinsame Datenschutzbeauftragte. In diesem Fall ist auf eine explizite Nennung des Jobcenters zu achten, da es sich bei dem Jobcenter um einen eigenständigen Verantwortlichen handelt.

Da Jobcenter sensible Daten verarbeiten, ist datenschutzrechtliche Expertise dort besonders wichtig. Mit der Prüfaktion haben wir die kommunalen Jobcenter dafür sensibilisiert, dass sie datenschutzrechtlich eigenständige Verantwortliche sind. Wir haben insbesondere darauf hingewirkt, dass die Vorgaben zur Benennung von Datenschutzbeauftragten eingehalten werden, damit die datenschutzrechtliche Expertise für die Aufgabe sichergestellt wird.

# 12. Datensicherheit

## 12.1 Änderung bei der Meldung von Datenpannen

**Mit einem Webformular können Verantwortliche der Landesbeauftragten ab März 2020 Verletzungen des Schutzes personenbezogener Daten melden.**

Die mit Art. 33 und 34 Datenschutz-Grundverordnung (DS-GVO), gegebenenfalls in Verbindung mit § 59 Datenschutzgesetz NRW, eingeführten Melde- und Benachrichtigungspflichten von Verletzungen des Schutzes personenbezogener Daten (auch als Datenpannen bezeichnet) können durch diese neue Form der Meldung sowohl für die Meldepflichtigen als auch für die Aufsichtsbehörde (LDI NRW) einfacher und schneller abgewickelt werden.

Zur Entwicklung der Eingangszahlen siehe unter 2.

Das Meldeformular wurde im Jahr 2019 entwickelt, um die Abwicklung der großen Zahl der Meldungen von Datenpannen zu optimieren.

Es stellt den zentralen Kommunikationsweg für Meldungen von Verletzungen des Schutzes personenbezogener Daten an die LDI NRW dar.

Das interaktive Webformular ersetzt die bisher zur Verfügung gestellten Formulare „Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33 DS-GVO)" und „Information über die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art. 33 Abs. 3 Buchstabe d, Art. 34 DS-GVO)".

Es kann direkt im Webbrowser ausgefüllt und an uns übermittelt werden. Daraufhin erhält die meldende Person eine automatische Eingangsbestätigung, die per E-Mail versandt wird und das Aktenzeichen der Meldung enthält. Dieses Aktenzeichen kann zusammen mit dem Eingangsdatum der Meldung genutzt werden, um zu einem späteren Zeitpunkt ergänzende Meldungen zur Datenpanne abzugeben. Zu Dokumentationszwecken können sich Meldende zusätzlich eine PDF-Datei zur übermittelten Meldung erzeugen lassen. Die in der Meldung angegebene Anlaufstelle für weitere Informationen wird von uns über den Status der Bearbeitung informiert und bei Rückfragen kontaktiert.

Das Webformular für Meldungen von Datenpannen steht als der zentrale Kommunikationsweg für Meldungen nach Art. 33 DS-GVO und Informationen über Benachrichtigungen nach Art. 34 DS-GVO an die LDI NRW zur Verfügung. Wir erwarten dadurch eine Verbesserung der Servicequalität bezogen auf die Einreichung und Bearbeitung der Meldungen.

## 12.2 Unsichere Passwortspeicherung bei Verantwortlichen

**Auskünfte von Verantwortlichen zeigen, dass weiterhin veraltete Hashverfahren zur Speicherung von Passwörtern in Onlinesystemen verwendet werden – hier müssen Verantwortliche regelmäßig nachbessern. Aufgrund der aktuellen Entwicklungen im Bereich der Kryptowährungen muss auch der Einsatz aktueller Hashverfahren kritisch geprüft werden.**

Die Verwendung eines Hashverfahrens um die Vertraulichkeit eines Passwortes sicherzustellen, ist gängige Praxis. Dabei wird aus dem Passwort eine Zeichenfolge gebildet, die anstelle des Passworts im Klartext als eine Art „Fingerabdruck“, dem so genannten Hashwert, gespeichert wird. Auf diese Weise wird die Vertraulichkeit des originären Passwortes sichergestellt, da der Hashwert so gebildet wird, dass aus diesem der Klartext des Passworts nicht rekonstruiert werden kann. Sofern eine Passwortprüfung erforderlich ist, wird aus der Benutzereingabe ein Hashwert gebildet und mit dem gespeicherten Wert verglichen.

Im Zuge von Auskunftsersuchen zeigt sich regelmäßig, dass Verantwortliche technische Verfahren zur Passwortspeicherung angeben, die nicht mehr dem Stand der Technik entsprechen. In diesen Fällen werden die Passwörter mit Hashalgorithmen wie MD5 oder SHA-1 verarbeitet. Vom Einsatz von MD5 (Message-Digest Algorithm 5) wird für eine Mehrzahl von Verfahren bereits seit 2009 vom BSI abgeraten. Der Wechsel von SHA-1 (Secure Hash Algorithm) auf SHA-2 oder SHA-3 wird seit Anfang 2018 vom BSI empfohlen. In Bezug auf die Anwendung kryptografischer Verfahren ist insbesondere die Technische Richtlinie „BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ zu berücksichtigen.

Die derzeitigen Entwicklungen zeigen allerdings, dass auch die aktuellen Hashverfahren für diesen Einsatzzweck kritisch hinterfragt werden müssen. Zwar lassen sich Hashwerte nicht zurückrechnen, allerdings ist es denkbar, das zu einem Hashwert gehörige Passwort durch Berechnung der Hashwerte für alle möglichen Passwörter zu ermitteln. Bislang standen diesem Vorgehen nur der erhebliche Ressourcenaufwand und die damit verbundenen Kosten entgegen. Die Entwicklungen im Bereich der Kryptowährungen haben zu einer Änderung der Ausgangslage geführt.

Die Hashwertberechnung ist für viele Kryptowährungen, wie etwa dem Bitcoin, von zentraler Bedeutung. So erfordert das „Schürfen“ neuer Bitcoins extrem viele Hashwert-Berechnungen. Das Interesse und die Wertsteigerung des Bitcoins haben zu einer Entwicklung von Spezialhardware geführt, die die oben genannten Voraussetzungen erfüllen und extrem viele Hashwerte berechnen können. Somit stehen nun vergleichsweise günstige Hardwarekomponenten zur Verfügung, die ein achtstelliges Passwort (Groß- und Kleinschreibung, Zahlen und Sonderzeichen) in unter zwei Minuten berechnen können.

Das Risiko lässt sich durch mehrfache Anwendung von Hashverfahren reduzieren, wie es zum Beispiel mit PBKDF2 (Password-Based Key Derivation Function) vorgesehen ist. Verfahren wie bcrypt oder Argon2 erreichen eine höhere Resistenz durch den Bedarf von Arbeitsspeicher – eine Ressource, die aus Kostengründen in dieser Spezialhardware nicht zur Verfügung steht und eine vollständige Passwortsuche erschwert.

Sofern alte Hash-Verfahren im Einsatz sind, ist in Abhängigkeit vom Risiko der Verarbeitung eine Aktualisierung auf Verfahren wie bcrypt oder Argon2 vorzunehmen.

## 12.3 Erhebung personenbezogener Daten über Webformulare

**Viele Firmen bieten zur bequemen Kontaktaufnahme Webformulare an. Aus datenschutzrechtlicher Sicht ist eine Verschlüsselung erforderlich, wenn personenbezogene Daten abgefragt werden. Eingaben an die LDI NRW zeigen, dass diese Absicherung nicht immer vorliegt.**

Kontaktformulare ermöglichen es, die zur Bearbeitung einer Anfrage erforderlichen Informationen strukturiert zu erfassen. Anfragen können anhand der Angaben vorsortiert werden. Solche Anfragen können gestellt werden ohne die Webseite zu verlassen. Webformulare sind daher sehr beliebt und in vielen Bereichen verbreitet. Außer zur allgemeinen Kontaktaufnahme werden sie unter anderem von Arztpraxen zur Terminvereinbarung bereitgestellt.

Der Verantwortliche hat, wenn er über ein Webformular personenbezogene Daten erhebt, nach Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen zum Schutz dieser Daten zu treffen.

Die Datenübermittlung im World Wide Web erfolgt traditionell unverschlüsselt. Werden vom Verantwortlichen keine Maßnahmen ergriffen, erfolgt eine unverschlüsselte Übermittlung. Somit können Dritte die eingegebenen Daten einsehen oder verändern. Bereits seit einigen Jahren ist eine transportverschlüsselte Übertragung verfügbar und gilt inzwischen als Stand der Technik. Werden über Webformulare personenbezogene Daten erhoben, ist eine Transportverschlüsselung erforderlich.

Aufgrund mehrerer Eingaben haben wir festgestellt, dass weiterhin unverschlüsselte Webformulare eingesetzt werden. Die LDI NRW hat daraufhin die Verantwortlichen auf diesen Missstand hingewiesen und auf eine datenschutzkonforme Verarbeitung hingewirkt.

In einigen Fällen haben Verantwortliche über Webformulare personenbezogene Daten erhoben, ohne geeignete technische und organisatorische Maßnahmen zu treffen. Nach dem Eingreifen der LDI NRW haben die Verantwortlichen die Defizite beseitigt und ihre Webformulare datenschutzkonform gestaltet.

## 12.4 Unsachgemäße Lagerung und Entsorgung von Papierunterlagen

**Die unsachgemäße Lagerung und Entsorgung von Papierunterlagen mit personenbezogenen Daten stellt grundsätzlich einen Verstoß gegen Art. 32 DS-GVO dar und kann mit Bußgeldern sanktioniert werden.**

Bei der LDI NRW sind mehrere Beschwerden über Arztpraxen und Rechtsanwaltskanzleien eingegangen, die Papierunterlagen unsachgemäß gelagert oder entsorgt haben. Dabei wurden auch sensible Unterlagen wie Patienten- und Mandantenakten an offen zugänglichen Orten wie Hausfluren oder gemeinschaftlich genutzten Tiefgaragen gelagert oder – ohne diese geeignet zu vernichten – in öffentlich zugänglichen Containern oder Mülltonnen entsorgt. Darüber hinaus stellt sich im Einzelfall die Frage, ob die Unterlagen nicht schon vor Jahren hätten vernichtet werden müssen.

Durch diese Formen der unsachgemäßen Lagerung bzw. Entsorgung war es Dritten potentiell möglich, die teilweise sehr sensiblen und umfangreichen personenbezogenen Daten einzusehen und zu entwenden, ohne dass der Verantwortliche dies hätte feststellen bzw. nachvollziehen konnte. Mit der unbefugten Kenntnisnahme oder Nutzung dieser Daten durch Dritte sind mitunter hohe Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden.

Auch in Papierform müssen personenbezogene Daten nach Art. 32 DS-GVO mit geeigneten technischen und organisatorischen Maßnahmen insbesondere vor unbefugten Zugriffen, Veränderungen und Verlust geschützt werden. Sie müssen unter Berücksichtigung der Risiken für die Rechte und Freiheiten der betroffenen Personen so gelagert werden, dass nur befugte Personen Zugang zu diesen erhalten. Nachdem die Verarbeitung der Papierunterlagen nicht mehr erforderlich ist und ggf. bestehende Aufbewahrungsfristen abgelaufen sind, sind die Papierdokumente geeignet zu vernichten. Die Dokumente sind so zu vernichten, dass die Wahrscheinlichkeit, dass Dritte Kenntnis über den Inhalt der vernichteten Dokumente erhalten, soweit reduziert wird, dass ein angemessenes Schutzniveau für die betroffenen Personen erreicht wird. Es wird empfohlen, sich dabei an der DIN 66399 zu orientieren.

Insbesondere bei sensiblen Daten ist eine ordnungsgemäße Lagerung und Vernichtung von Papierdokumenten zwingend erforderlich. In einzelnen Fällen, die wir derzeit untersuchen, ziehen wir weitere Maßnahmen, wie Bußgeldverfahren, in Erwägung.

## 12.5 Einbrüche in Kindertagesstätten

**Verletzungen des Schutzes personenbezogener Daten sind nach Art. 33 Datenschutz-Grundverordnung (DS-GVO) unter gewissen Voraussetzungen an die zuständige Aufsichtsbehörde zu melden. Auffällig viele Meldungen betreffen Datenverluste durch Einbruchdiebstähle in Kindertagesstätten.**

Art. 4 Nr. 12 DS-GVO fasst verschiedene Kategorien von Datenpannen unter dem Oberbegriff „Verletzungen des Schutzes personenbezogener Daten“ zusammen. Hierzu zählen Fälle, in denen Dritte unbefugt in den Besitz personenbezogener Daten gelangen, und Fälle, in denen der Verantwortliche den Zugriff auf die Daten verliert. Zu den personenbezogenen Daten zählen neben Stammdaten wie Name und Anschrift, beispielsweise auch Gutachten oder Fotografien.

Eine solche Datenpanne ist nach Art. 33 DS-GVO an die Aufsichtsbehörde zu melden, es sei denn, sie birgt voraussichtlich kein bzw. nur ein geringes Risiko für die Rechte und Freiheiten der betroffenen Personen.

Uns wurden im Jahr 2019 viele Fälle gemeldet, in denen in Kindertagesstätten oder ähnlichen Einrichtungen eingebrochen und dabei personenbezogene Daten entwendet wurden. Regelmäßig waren die Daten auf Laptops gespeichert oder befanden sich noch auf den Speicherkarten entwendeter Kameras.

Der LDI NRW liegen keine Anhaltspunkte dafür vor, dass die auf den Geräten gespeicherten Daten das eigentliche Ziel des Einbruchs waren. Der Einbruch gilt in der Regel den Geräten. Dennoch sind von einer Kindertagesstätte erstellte Fotoaufnahmen von Kindern für manche Tätergruppen ein durchaus attraktives Ziel. Dies ist bei der Auswahl der technischen und organisatorischen Maßnahmen zu berücksichtigen.

In den uns bekannten Fällen hätten die Risiken für die betroffenen Personen, insbesondere für die Kinder, deren Fotoaufnahmen entwendet wurden, ohne viel Aufwand erheblich verringert werden können. So sollten Fotoaufnahmen unverzüglich von der Speicherkarte auf einen verschlüsselten Datenträger kopiert und anschließend sicher von der Speicherkarte gelöscht werden

Diese einfachen Maßnahmen schließen weitgehend aus, dass bei einem Diebstahl der Geräte Unbefugte Zugriff auf die auf ihnen gespeicherten Daten nehmen können.

Auch Einrichtungen, die sich aufgrund nicht vorhandener Wertgegenstände nicht als lohnendes Ziel betrachten, können jederzeit Opfer von Einbrüchen werden. Umso wichtiger ist es, personenbezogene Daten nur so zu speichern, dass Einbrecher keinen Zugriff erlangen können. Eine konsequente Datenträgerverschlüsselung und das sichere Löschen sensibler Daten von unverschlüsselten Speichermedien kann hierzu beitragen.

# Anhang

# Veröffentlichungen der Datenschutzkonferenz 2019

Neben den hier abgedruckten Entschließungen und Beschlüssen der Datenschutzkonferenz sind alle weiteren Veröffentlichungen auf der Homepage der Datenschutzkonferenz www.datenschutzkonferenz-online.de abrufbar.

## Entschließungen der Datenschutzkonferenz 2019

Mit Entschließungen nimmt die Datenschutzkonferenz zu datenschutzpolitischen Fragen öffentlich Stellung. Entschließungen werden sowohl in den Konferenzen, als auch zwischen den Konferenzen gefasst.

## 97. Konferenz vom 3./4. April 2019

### ▪ Hambacher Erklärung zur Künstlichen Intelligenz – Sieben datenschutzrechtliche Anforderungen

Systeme der Künstlichen Intelligenz (KI) stellen eine substanzielle Herausforderung für Freiheit und Demokratie in unserer Rechtsordnung dar. Entwicklungen und Anwendungen von KI müssen in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen. Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Das gilt in besonderem Maße für den Einsatz von selbstlernenden Systemen, die massenhaft Daten verarbeiten und durch automatisierte Einzelentscheidungen in Rechte und Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

**I. Künstliche Intelligenz und Datenschutz**

„Künstliche Intelligenz“ (auch „KI“ oder „Artificial Intelligence“ – „AI“) wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland an die Weltspitze der Entwicklung von KI zu bringen. „AI made in Germany“ soll gleichzeitig dafür sorgen, dass auch bei weitreichendem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der EU gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, „technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu „lernen“ […].“ Fußnote: KI-Systeme werden beispielsweise bereits in der Medizin unterstützend in Forschung und Therapie eingesetzt. Schon heute sind neuronale Netze in der Lage, automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen. In den falschen Händen jedoch, kann es auch missbraucht werden.

Auch zur Bewertung von Bewerbungsunterlagen wurde bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Allerdings hatte das Unternehmen bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das KI-System Frauen sehr viel schlechter, obwohl das Geschlecht nicht nur kein vorgegebenes Bewertungskriterium, sondern dem System sogar unbekannt war. Dies offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern verfestigt werden.

Anhand dieser Beispiele wird deutlich, dass mit KI-Systemen häufig personenbezogene Daten verarbeitet werden und diese Verarbeitung Risiken für die Rechte und Freiheiten von Menschen birgt. Sie zeigen auch, wie wichtig es ist, Entwicklung und Einsatz von KI-Systemen politisch, gesellschaftlich und rechtlich zu begleiten. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder verstehen die folgenden Anforderungen als einen konstruktiven Beitrag zu diesem zentralen gesellschaftspolitischen Projekt.

## II. Datenschutzrechtliche Anforderungen an Künstliche Intelligenz

Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, beinhaltet die Datenschutz-Grundverordnung (DS-GVO) wichtige rechtliche Vorgaben. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Auch für KI-Systeme gelten die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO). Diese Grundsätze müssen gemäß Art. 25 DS-GVO durch frühzeitig geplante technische und organisatorische Maßnahmen von den Verantwortlichen umgesetzt werden (Datenschutz durch Technikgestaltung).

### 1. KI darf Menschen nicht zum Objekt machen

Die Garantie der Würde des Menschen (Art. 1 Abs. 1 GG, Art. 1 GRCh) gebietet, dass insbesondere im Fall staatlichen Handelns mittels KI der Einzelne nicht zum Objekt gemacht wird. Vollständig automatisierte Entscheidungen o-

der Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 DS-GVO nicht allein der Maschine überlassen werden. Wenn der Anwendungsbereich des Art. 22 DS-GVO nicht eröffnet ist, greifen die allgemeinen Grundlagen des Art. 5 DS-GVO, die insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zurechenbarkeit und Fairness die Rechte des Einzelnen schützen. Betroffene haben auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

**2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben**

Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO). Zweckänderungen sind mit Art. 6 Abs. 4 DS-GVO klare Grenzen gesetzt. Auch bei KI-Systemen müssen erweiterte Verarbeitungszwecke mit dem ursprünglichen Erhebungszweck vereinbar sein. Das gilt auch für die Nutzung personenbezogener Daten zu Trainingszwecken von KI-Systemen.

**3. KI muss transparent, nachvollziehbar und erklärbar sein**

Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO). Dies erfordert insbesondere eine transparente Verarbeitung, bei der die Informationen über den Prozess der Verarbeitung und ggf. auch über die verwendeten Trainingsdaten leicht zugänglich und verständlich sind (Art. 12 DS-GVO). Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DS-GVO ist dafür auch über die involvierte Logik ausreichend aufzuklären. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DS-GVO).

**4. KI muss Diskriminierungen vermeiden**

Lernende Systeme sind in hohem Maße abhängig von den eingegebenen Daten. Durch unzureichende Datengrundlagen und Konzeptionen kann es zu Ergebnissen kommen, die sich als Diskriminierungen auswirken. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar. Sie verstoßen u.a. gegen bestimmte Anforderungen der Datenschutz-Grundverordnung, etwa den Grundsatz der Verarbeitung nach

Treu und Glauben, die Bindung der Verarbeitung an legitime Zwecke oder die Angemessenheit der Verarbeitung.

Diese Diskriminierungsneigungen sind nicht immer von vornherein erkennbar. Vor dem Einsatz von KI-Systemen müssen deshalb die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

**5. Für KI gilt der Grundsatz der Datenminimierung**

Für KI-Systeme werden typischerweise große Bestände von Trainingsdaten genutzt. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO). Die Verarbeitung personenbezogener Daten muss daher stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

**6. KI braucht Verantwortlichkeit**

Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten. Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Art. 5 DS-GVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Art. 12 ff DS-GVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern. Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich sein.

**7. KI benötigt technische und organisatorische Standards**

Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisatorische Maßnahmen gem. Art. 24 und 25 DS-GVO zu treffen, wie z.B. Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Prac-

tice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

### III. Die Entwicklung von KI bedarf der Steuerung

Die Datenschutzaufsichtsbehörden überwachen die Anwendung des Datenschutzrechts, setzen es durch und haben die Aufgabe, bei der Weiterentwicklung für einen effektiven Grundrechtsschutz einzutreten. Angesichts der hohen Dynamik in der Entwicklung der Technologien von künstlicher Intelligenz und der vielfältigen Einsatzfelder zeichnen sich die Grenzen der Entwicklung noch nicht ab. Gleichermaßen sind die Risiken der Verarbeitung personenbezogener Daten in KI-Systemen nicht pauschal einzuschätzen. Auch ethische Grundsätze sind zu beachten. Wissenschaft, Datenschutz-aufsichtsbehörden, die Anwender und besonders die Politik sind gefordert, die Entwicklung von KI zu begleiten und im Sinne des Datenschutzes zu steuern.

## ▪ Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten![1]

Unternehmen haften im Rahmen von Art. 83 Datenschutz-Grundverordnung (DS-GVO) für schuldhafte Datenschutzverstöße ihrer Beschäftigten, sofern es sich nicht um einen Exzess handelt. Dabei ist nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen.

Diese Haftung für Mitarbeiterverschulden ergibt sich aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) besagt, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist. Erwägungsgrund 150 der DS-GVO weist für die Verhängung von Geldbußen wegen Datenschutzverstößen gegen Unternehmen klarstellend darauf hin. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten sämtlicher ihrer Beschäftigten. Eine Kenntnis der Geschäftsführung eines Unternehmens von dem konkreten Verstoß oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können („Exzesse“), sind ausgenommen.

[1] Die Entschließung wurde gegen die Stimmen von Bayern und Baden-Württemberg gefasst.

Die alten nationalen Haftungsregeln wurden bisher nicht europarechtskonform der neuen Rechtslage angepasst. Unzutreffend verweist § 41 Abs. 1 des neuen Bundesdatenschutzgesetzes (BDSG) auf zurechnungseinschränkende Regelungen im OWiG. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben bereits im Rahmen des Gesetzgebungsverfahrens zum neuen Bundesdatenschutzgesetz darauf aufmerksam gemacht, dass diese Bestimmungen den Vorgaben der DS-GVO zur Verantwortlichkeit für Datenschutzverstöße widersprechen.

Die DSK begrüßt insoweit, dass der Koalitionsvertrag vorsieht, das Sanktionsrecht für Unternehmen generell im deutschen Recht so zu ändern, dass „die von Fehlverhalten von Mitarbeiterinnen und Mitarbeitern profitierenden Unternehmen stärker sanktioniert werden“. Diese gebotene Modernisierung des deutschen Unternehmenssanktionsrechts entspräche dann auch dem europäischen Kartellrecht und dem etablierten internationalen Standard.

Die DSK fordert den Bundesgesetzgeber daher nochmals auf, in den Beratungen des Entwurfs des Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 die §§ 30, 130 OWiG klarstellend vom Anwendungsbereich auszunehmen und damit dem europäischen Recht anzupassen.

## ▪ 23.04.2019 – Keine Abschaffung der Datenschutzbeauftragten

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) spricht sich gegen eine Abschaffung oder Verwässerung der die Datenschutzgrundverordnung ergänzenden nationalen Regelungen der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten aus.

Nach § 38 Bundesdatenschutzgesetz müssen z. B. Unternehmen und Vereine Datenschutzbeauftragte benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Diese Pflicht hat sich seit vielen Jahren bewährt und ist deshalb auch bei der Datenschutzreform im deutschen Recht beibehalten worden.

Die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten. Dies hat sich ganz besonders bei der Umstellung auf die Datenschutz-Grundverordnung bewährt.

Auch beim Wegfall der nationalen Benennungspflicht von Datenschutzbeauftragten bleiben die Pflichten des Datenschutzrechts bestehen. Verantwortliche verlieren jedoch interne Beraterinnen und Berater zu Fragen des Datenschutzes. Der Wegfall mag kurzfristig als Entlastung empfunden werden. Mittelfristig geht interne Kompetenz verloren.

Eine Aufweichung dieser Benennungspflicht, insbesondere für kleinere Unternehmen und Vereine, wird diese daher nicht entlasten, sondern ihnen mittelfristig schaden.

## ▪ 12.09.2019 – Digitalisierung der Verwaltung datenschutzkonform und bürgerfreundlich gestalten!

Die Bundesregierung will die in der Verwaltung geführten Register modernisieren und plant in diesem Zusammenhang einen einfacheren Zugriff auf dort gespeicherte personenbezogene Daten. Nach Auffassung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) darf dieses Vorhaben nicht zur Einführung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren führen. Vielmehr muss der Schutz der Grundrechte und Grundfreiheiten, insbesondere das Recht auf Schutz personenbezogener Daten, Priorität haben. Ebenso wichtig ist es, den Bürgerinnen und Bürgern die besseren Dienstleistungen verbunden mit einer deutlich höheren Transparenz anzubieten.

**Bundesregierung nimmt Modernisierung der Register in Angriff**
Die Bundesregierung hat mit dem Onlinezugangsgesetz ein umfangreiches Digitalisierungsprogramm für die Verwaltung in Deutschland gestartet. Bund und Länder sind verpflichtet, ihre Verwaltungsleistungen künftig auch elektronisch über Verwaltungsportale anzubieten. Es sollen Nutzerkonten bereitgestellt werden, über die sich Nutzende für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können.

In diesem Zusammenhang hat sich der Nationale Normenkontrollrat (NKR) für eine Modernisierung der deutschen Registerlandschaft ausgesprochen und empfohlen, dass bestimmte Basisdaten von Bürgern und Unternehmen nur einmal mitgeteilt werden müssen („Once Only"-Prinzip). Der NKR hat darüber hinaus angeregt, datenschutzkonforme Identifikationsnummern für Personen, Unternehmen sowie Gebäude, Wohnungen und Flurstücke zu schaffen und zu nutzen und ein „Datencockpit" einzurichten, bei dem die Bürgerinnen und Bürger alle staatlichen Datenflüsse im Auge haben können.

Die Einführung solcher Identifikationsnummern für Personen wird aktuell unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI) von der Bundesregierung verfolgt. Der IT-Planungsrat hat in seiner 28. Sitzung am 12. März 2019 den vom BMI vorgelegten „Leitlinien für eine Modernisierung der Registerlandschaft" zugestimmt sowie den „Vorschlag für die Verbesserung des Identitätsmanagements als Teil der Registermodernisierung" zur Kenntnis genommen und das angestrebte Vorhaben begrüßt.

**Datenschutzfreundliche und transparente Gestaltung für Bürgerinnen und Bürger**
Bereits die Schaffung einheitlicher und verwaltungsübergreifender Personenkennzeichen bzw. Identifikatoren und einer entsprechenden Infrastruktur zum Datenaustausch

bergen die Gefahr, dass personenbezogene Daten in großem Maße leicht zusammengetragen, verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden könnten. Die Datenschutzkonferenz weist darauf hin, dass das Bundesverfassungsgericht schon seit Jahrzehnten der Einführung und Verarbeitung derartiger Personenkennzeichen sehr enge Schranken auferlegt, da sie massiv in den Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffener Bürgerinnen und Bürger eingreifen. Bereits die Möglichkeit einer umfassenden Katalogisierung von Bürgerinnen und Bürgern durch den Staat gefährdet das Persönlichkeitsrecht, da sie bei den Menschen zu einer vorauseilenden Anpassung ihres Verhaltens führen kann. Auch die Grundsätze der europäischen Datenschutz-Grundverordnung und deren Regelungen zur datenschutzgerechten Gestaltung setzen einheitlichen und verwaltungs-übergreifenden Personenkennzeichen enge Grenzen und verlangen geeignete Garantien für die Wahrung der Rechte und Freiheiten der betroffenen Personen.

Insbesondere im Hinblick auf die geplante Verwendung modernisierter Register für zukünftige Zensus-Erhebungen und geplante/modernisierte Zugriffsrechte der Sicherheitsbehörden bedarf es eines besonderen Schutzes der betroffenen Personen. Den hohen Risiken für das Recht auf informationelle Selbstbestimmung muss in einem umfassenden regulatorischen, vor allem aber technischen und organisatorischen Konzept begegnet werden. Nur so können die vom deutschen und europäischen Verfassungsrecht geforderten Garantien gewahrt werden.

Die Modernisierung der Register muss zwingend von Beginn an auch dafür genutzt werden, den Bürgerinnen und Bürgern die Nutzung der im Online-Zugangsgesetz vorgesehenen Dienstleistungen durch Nutzung einmal hinterlegter Daten zu erleichtern. Von besonderer Bedeutung ist es darüber hinaus, den Bürgerinnen und Bürgern ein im Vergleich zur gegenwärtigen Situation deutlich höheres Maß an Transparenz zu gewährleisten. Ein „Datencockpit“, wie es der NKR bereits vorgeschlagen hat, muss es den Bürgerinnen und Bürgern erlauben, jederzeit nachzuvollziehen, welches Register welche Daten über sie vorhält, welche Behörden darauf zugegriffen haben und mit welchen anderen Daten diese verknüpft wurden. Gleichzeitig muss gewährleistet sein, dass ausschließlich den betroffenen Bürgerinnen und Bürgern der Zugriff möglich ist. Auf dieser Grundlage muss die Digitalisierung der Verwaltung dazu genutzt werden, das informationelle Machtgefälle zwischen Staat und Bürgerinnen und Bürgern weitgehend aufzuheben und ihnen die Inanspruchnahme ihrer Rechte deutlich zu erleichtern.

Dazu muss nach Auffassung der Datenschutzkonferenz die dezentrale Registerstruktur erhalten bleiben. Die Nutzung von einheitlichen, verwaltungs-übergreifenden Personenkennzeichen bzw. Identifikatoren zur direkten Identifizierung von Bürgerinnen und Bürgern lehnt die Datenschutzkonferenz ab. Sie fordert alternative Methoden zur eindeutigen Identifizierung. Neben Abgleichen über den jeweiligen Datensatz des Registers kämen dafür allenfalls sektorspezifische Personenkennziffern in Betracht, die eine eindeutige Identifizierung erlauben, einseitigen staatlichen Abgleich von Daten verhindern, ein

Höchstmaß an Transparenz beispielsweise durch ein Datencockpit ermöglichen, das Risiko von Missbrauch und Kompromittierung verringern und die Eindeutigkeit von Registern gewährleisten.

## 98. Konferenz vom 6./7. November 2019

### ▪ Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

Auf der Grundlage der Hambacher Erklärung vom 03.04.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem Positionspapier Anforderungen an KI-Systeme erarbeitet, deren Umsetzung die DSK für eine datenschutzkonforme Gestaltung von KI-Systemen empfiehlt. Die in der Hambacher Erklärung festgelegten rechtlichen Rahmenbedingungen werden damit im Hinblick auf technische und organisatorische Maßnahmen konkretisiert, die auf die unterschiedlichen Phasen der Lebenszyklen von KI-Systemen bezogen sind.

Die Phasen des Lebenszyklus eines KI-Systems – Designs des KI-Systems, Veredelung von Rohdaten zu Trainingsdaten, Training der KI-Komponenten, Validierung der Daten und KI-Komponenten sowie des KI-Systems, Einsatz des KI-Systems und die Rückkopplung von Ergebnissen – werden am Maßstab von Gewährleistungszielen untersucht. Um aus rechtlichen Anforderungen KI-spezifische technische und organisatorische Maßnahmen abzuleiten und zu systematisieren, werden die Gewährleistungsziele Transparenz, Datenminimierung, Nichtverkettung, Intervenierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit verwendet.

Für die Verarbeitung von personenbezogenen Daten, bei der KI-Systeme zum Einsatz kommen, gelten die in der DS-GVO formulierten Grundsätze. Mit dem Positionspapier wird Verantwortlichen im Umfeld von KI ein Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gegeben, an dem sie sich bei der Planung und dem Betrieb von KI-Systemen orientieren können. Das Positionspapier soll verdeutlichen, dass der Einsatz von KI-Systemen und der Datenschutz keine zwingenden Gegensätze sind. Die Chancen und neuen Möglichkeiten des Einsatzes von KI-Systemen werden durch einen modernen Datenschutz nicht verhindert. Das Positionspapier soll die Entwicklung und den Einsatz von KI auch unter Nutzung personenbezogener Daten konstruktiv begleiten. Damit wird Handlungssicherheit gesteigert und sichergestellt, dass die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere das Recht auf informationelle Selbstbestimmung, auch in dem dynamischen, von KI-Systemen geprägten Umfeld gewahrt werden.

Die DSK legt dieses Positionspapier auch vor, um den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen auf dieser Grundlage weiter zu intensivieren.

Hinweis: Das Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen vom 06.11.2019 ist auf unserer Internetseite abrufbar.

## ▪ Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten

Die Datenschutzkonferenz weist nachdrücklich darauf hin, dass die Sicherheit von Patientendaten in der medizinischen Behandlung nach der Datenschutz-Grundverordnung flächendeckend gewährleistet sein muss. Der effektive Schutz von Gesundheitsdaten darf nicht von der Größe der Versorgungseinrichtung abhängen.

In der jüngeren Vergangenheit häufen sich Vorfälle, in denen der Schutz von Patientendaten in der stationären Versorgung gefährdet ist. So wurden im Juli 2019 eine Reihe von Einrichtungen eines Trägers in Rheinland-Pfalz und dem Saarland Opfer eines Befalls mit Schadsoftware. Die durch diese erfolgte Verschlüsselung von Daten im IT-Verbund der Trägergesellschaft hat zu weitreichenden Beeinträchtigungen des Krankenhausbetriebs geführt. Im September 2019 wurde bekannt, dass weltweit mehr als 16 Millionen Datensätze, darunter 13.000 von in deutschen Gesundheitseinrichtungen behandelten Patienten, offen im Internet zugänglich waren. Ursache hierfür waren nach den bislang bekannt gewordenen Informationen insbesondere unzureichende technische und organisatorische Vorkehrungen zum Schutz dieser Daten.

Der Einsatz von Informations- und Kommunikationstechnik in der Gesundheitsversorgung ist im Zeitalter der digitalisierten Medizin unabdingbar. Allerdings müssen die in diesem Zusammenhang rechtlich gebotenen und nach dem Stand der Technik angemessenen Vorkehrungen zu einem effektiven Schutz der Daten von Patientinnen und Patienten flächendeckend getroffen werden. Dazu sind alle in diesem Zusammenhang tätigen Einrichtungen unabhängig von ihrer Größe aufgrund der Datenschutz-Grundverordnung verpflichtet.

Die Datenschutzkonferenz fordert vor dem Hintergrund einer zunehmenden Digitalisierung der Gesundheitsversorgung und angesichts der damit einhergehenden Gefährdungen ausdrücklich dazu auf, auch in finanzieller Hinsicht sicherzustellen, dass alle Einrichtungen des Gesundheitswesens die zum Schutz der Patientendaten nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können.

## ▪ Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte!

Mit zunehmender Sorge beobachtet die Datenschutzkonferenz, dass Betreiber von Gesundheitswebseiten und Gesundheits-Apps auch sensible personenbezogene Daten der Nutzerinnen und Nutzer ohne erkennbare Verarbeitungsgrundlage an Dritte weiterleiten. Unter anderem geschieht dies durch Tracking - und Analyse-Tools (also Programme, die das Surfverhalten beobachten und analysieren), von deren Einsatz die betroffenen Personen keine Kenntnis haben.

So wurde im September 2019 durch die Studie einer Nichtregierungsorganisation bekannt, dass zahlreiche Betreiber von Gesundheitswebseiten, die ihren Besuchern Informationen zu Depression und anderen psychischen Krankheiten anbieten, personenbezogene Nutzungsdaten ohne adäquate Einbindung der Nutzerinnen und Nutzer an andere Stellen weitergeleitet haben sollen. Teilweise soll dabei sogar die Teilnahme an Depressions-Selbsttests erfasst worden sein. Auch von 44 analysierten deutschen Webseiten besäßen weit über die Hälfte solche integrierten Bausteine, die dies ermöglicht hätten. Im Oktober 2019 wurden Recherchen veröffentlicht, wonach eine in Deutschland ansässige Diagnostik-App ebenfalls Tracking- und Analyse-Dienste nutze und in diesem Zusammenhang sensible Gesundheitsdaten wie z.B. körperliche Beschwerden ohne vorherige Information und Legitimation der Nutzer an Dritte weiterleite.

Zu den Datenempfängern gehören häufig neben sonstigen Tracking-Dienstleistern große Unternehmen wie Facebook, Google und Amazon, die vorrangig eigene Geschäftsinteressen verfolgen. Die Verknüpfung der weitergeleiteten Daten mit anderen Informationen begründet das Risiko, dass für jede Nutzerin und jeden Nutzer ein personenbezogenes Gesundheitsprofil entsteht, von dessen Existenz und Umfang die betroffenen Personen nichts wissen.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder prüfen im Rahmen ihrer Aufgaben und Möglichkeiten derartige Hinweise und werden Datenschutzverletzungen gegebenenfalls sanktionieren. Zugleich ist der Gesetzgeber aufgerufen, im Zusammenhang mit der bevorstehenden Einführung digitaler Gesundheitsanwendungen in die Regelversorgung den Schutz der Vertraulichkeit sensibler Gesundheitsdaten sicherzustellen. Beispielsweise wäre es nicht hinzunehmen, wenn die Nutzung einer von der Regelversorgung erfassten Gesundheits-App zwingend an gesetzlich nicht vorgesehene Weiterleitungen von Gesundheitsdaten gekoppelt würde.

Die Datenschutzkonferenz fordert die Betreiber von Gesundheitswebseiten und Gesundheits-Apps auf, die berechtigten Vertraulichkeitserwartungen ihrer Nutzerinnen und Nutzer zu respektieren. Unabhängig von den allgemeinen datenschutzrechtlichen Anforderungen an die Weitergabe personenbezogener Gesundheitsdaten sind dabei insbesondere folgende Anforderungen zu beachten:

- Leiten Betreiber von Gesundheitswebseiten und Gesundheits-Apps personenbezogene Nutzungsdaten an andere Stellen weiter, sind sie für diese Datenweitergabe verantwortlich, selbst wenn sie – wie etwa bei der Einbindung von Social Plugins - keinen eigenen Zugriff auf die weitergeleiteten Daten haben.
- Als Verantwortliche sind Betreiber insoweit verpflichtet, die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu beachten. Die eingangs beschriebene Weiterleitung von Gesundheitsdaten kann nach Art. 9 Abs. 1, 2 Buchst. a Datenschutz-Grundverordnung ausnahmsweise nur auf Grundlage einer vor der Datenverarbeitung eingeholten ausdrücklichen Einwilligung zulässig sein, die auch den übrigen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung genügen muss.
- Insbesondere unterliegt die Einwilligung in die Verarbeitung von Gesundheitsdaten strengen Transparenzanforderungen: Unter anderem muss sie konkret benennen, wer für die Verarbeitung verantwortlich ist und welche Kategorien personenbezogener Daten, wie beispielsweise Gesundheitsdaten, Informationen über die sexuelle Orientierung oder zum Sexualleben verarbeitet werden. Auch die Zwecke der Datenverarbeitung und die Empfänger von weitergeleiteten Daten sind konkret zu benennen. Diese Informationen müssen die Nutzerinnen und Nutzer in die Lage versetzen, sich über die Konsequenzen ihrer erteilten Einwilligung bewusst zu werden.
- Im Rahmen der Regelversorgung wäre die einwilligungsbasierte Weiterleitung von Nutzerdaten an Tracking- oder Analyse-Dienstleister oder sonstige Dritte, die nicht Teil der Gesundheitsversorgung sind, allenfalls zulässig, wenn dies gesetzlich geregelt würde. Gegen eine solche gesetzliche Regelung bestünden allerdings im Hinblick auf das Erfordernis der freiwilligen Einwilligung erhebliche Bedenken.

Im Übrigen weist die Datenschutzkonferenz darauf hin, dass sich aus dem dargestellten Sachverhalt erneut die dringende Notwendigkeit ergibt, möglichst zeitnah eine ePrivacy-Verordnung zu verabschieden. Darin müssen die Bedürfnisse des elektronischen Datenverkehrs mit den Erfordernissen der Grundrechte auf Privatheit und auf Datenschutz in Einklang gebracht werden. Es sind insbesondere Regelungen erforderlich, die einen hohen Schutz sensibler Daten effektiv sicherstellen.

## ▪ Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke!

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist auf den Missstand hin, dass seit einiger Zeit eigentlich für Zwecke der polizeilichen Gefahrenabwehr eingerichtete automatisierte Kennzeichenerfassungssysteme auch für Zwecke der Strafverfolgung eingesetzt werden. Sie erfassen dabei massenhaft und teilweise längerfristig Kfz-Daten unabhängig von der Beschuldigteneigenschaft der betroffenen Personen.

Im Rahmen der Gefahrenabwehr fahndet die Polizei auf Grundlage des jeweiligen Landespolizeigesetzes nach einzelnen Kraftfahrzeugkennzeichen. Nur im Fall einer Übereinstimmung von Kennzeichen und gesuchtem Fahrzeug kommt es zu einer Speicherung des einzelnen Kraftfahrzeugkennzeichens. Kfz-Kennzeichen, nach denen nicht polizeilich gefahndet wird, werden nach ihrer Erfassung unverzüglich gelöscht.

Demgegenüber wird im Bereich der Strafverfolgung – gestützt auf gerichtliche Beschlüsse oder staatsanwaltliche Anordnungen – nicht nur nach einzelnen Kraftfahrzeugen punktuell gefahndet. Vielmehr werden teilweise zusätzlich die Kennzeichen sämtlicher Fahrzeuge, die eine Straße mit einem Erfassungsgerät passieren, über einen längeren Zeitraum hinweg unterschiedslos erfasst und langfristig gespeichert. Als Rechtsgrundlage für solche Strafverfolgungsmaßnahmen wird in der Regel § 100h der Strafprozessordnung (StPO) herangezogen. Dieser erlaubt zwar, zur Observation beschuldigter Personen bestimmte technische Mittel einzusetzen, sofern Gegenstand der Strafverfolgung eine Straftat von erheblicher Bedeutung ist. Gegen andere Personen sind solche Maßnahmen nur ausnahmsweise zulässig. Eine umfassende Datenverarbeitung, wie sie die Aufzeichnung der Kennzeichen aller ein Erfassungsgerät passierender Kraftfahrzeuge über einen längeren Zeitraum bedeutet, führt jedoch dazu, dass sämtliche Verkehrsteilnehmende im Erfassungsbereich Ziel von Ermittlungsmaßnahmen sind und insoweit Bewegungsprofile entstehen können. Eine Ausweitung des Betroffenenkreises in dieser Größenordnung ist durch keinerlei Tatsachen begründbar und nicht zu rechtfertigen. Sie kann deshalb insbesondere nicht auf § 100h StPO gestützt werden.

Angesichts einer fehlenden Rechtsgrundlage sieht die DSK in der geschilderten exzessiven Nutzung von Kennzeichenerfassungssystemen für die Zwecke der Strafverfolgung einen Verstoß gegen das Grundgesetz und eine Verletzung der Bürgerinnen und Bürger in ihrem Recht auf informationelle Selbstbestimmung. Die DSK fordert die Polizeibehörden und Staatsanwaltschaften auf, die umfassende und unterschiedslose Erfassung, Speicherung und Auswertung von Kraftfahrzeugen durch Kennzeichenerfassungssysteme für Zwecke der Strafverfolgung zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen.

Die DSK lehnt Vorschläge ab, die auf die Schaffung einer neuen Rechtsgrundlage für derartige strafprozessuale Maßnahmen abzielen. Nach verfassungsgerichtlicher Rechtsprechung stellen bereits die automatisierten Kfz-Kennzeichen-Kontrollen zur Fahndung nach Personen oder Sachen einen Eingriff von erheblichem Gewicht dar, selbst wenn die Kfz-Kennzeichen unverzüglich spurenlos gelöscht werden. Eine längerfristige Aufzeichnung sämtlicher Kennzeichen begründet demgegenüber einen deutlich schwerwiegenderen Grundrechtseingriff.

# Beschlüsse der Datenschutzkonferenz

Beschlüsse der Datenschutzkonferenz sind Positionen, die die Auslegung datenschutzrechtlicher Regelungen bzw. entsprechende Empfehlungen betreffen.

## 97. Konferenz vom 3./4. April 2019

### ▪ 03.04.2019 – Positionierung der DSK zum datenschutzkonformen Einsatz von Windows 10

Datenschutzrisiken moderner Betriebssysteme wurden bereits mehrfach in der DSK beraten. Die 90. DSK hat im Herbst 2015 die Entschließung zu Cloud-unterstützten Betriebssystemen verabschiedet.

Im Jahr 2017 hat das LDA Bayern auf Grundlage der alten Rechtslage des BDSG a.F. einen Prüfbericht zu Windows 10 im Unternehmensumfeld veröffentlicht. Dabei wurde unter anderem die Frage formuliert, „ob Microsoft auf die Kritik der Nutzer und anderer europäischer Datenschutzbehörden, die Windows 10 Home und Professional prüfen, reagiert und bei der Fortentwicklung von Windows 10 datenschutzrechtliche Verbesserungen vorsehen wird“.

Auch das BSI hat sich im November 2018 intensiv mit Sicherheitsmängeln von Windows 10 befasst (BSI-Studie SiSyPHuS). Ein Schwerpunkt der Untersuchungen betraf die Analyse der Telemetrie Komponenten. Dabei kommt das BSI zum Ergebnis, dass sich selbst in der höchsten Sicherheitsstufe (Telemetrie-Level Security) nicht alle Datenübertragungen an Microsoft unterbinden lassen. Die SiSyPHuS-Win10-Studie des BSI adressieren dabei auch datenschutzrechtliche Risiken.

Die Marktverbreitung der Windows 10 Versionsfamilie ist inzwischen weit fortgeschritten. Im Konsumersektor, in der gewerblichen Wirtschaft sowie auch in weiten Teilen der öffentlichen Verwaltungen von Bund, Ländern und Kommunen - letztere begünstigt durch Rahmenverträge, Architektur- und Beschaffungsentscheidungen (insb. Rahmenvertragsverhandlungen 2018 des Bundes) - sind die verschiedenen Windows-10-Versionen ausgerollt worden. Zahlreiche weitete Migrationen dürften in den Jahren 2019 und 2020 im professionellen Einsatz erfolgen.

Aus technischer Sicht unterscheiden sich sowohl die Betriebssystemarchitektur als auch die Release Strategie von Windows 10 sehr deutlich von den Vorgängerprodukten. Aus daten-schutzrechtlicher Sicht ist dabei auf die folgenden Aspekte ein besonderes Augenmerk zu legen:

- Windows 10 ist nicht mehr ein reines Betriebssystem sondern eine „Systemumgebung“, die neben dem eigentlichen Betriebssystem eine Vielzahl von zusätzlichen Funktionalitäten enthält. Diese können zwar individuell konfiguriert werden, wobei

bei einer Standardinstallation je nach eingesetzter Produktversion nicht die datenschutz-freundlichste Voreinstellung vorhanden ist. Ob dabei das Prinzip „Data Protection by Default“ verletzt wird, ist in jedem Fall zu prüfen.
- Jedes Update (insbesondere Funktionsupdates) kann dazu führen, dass Konfigurationseinstellungen verändert werden und sich der Funktionsumfang ändert. Dies führt dazu, dass ein „neues“ Produkt vorliegt, dessen Einsatz erneut auf die datenschutz-rechtliche Zulässigkeit geprüft werden muss.
- Die Datenübermittlung von Windows 10 an Microsoft kann durch alleinige Einstellungen in Windows 10 nicht vollständig unterbunden werden. Da die Übertragung verschlüsselt an Microsoft erfolgt, ist nicht abschließend festzustellen, ob und wenn ja, welche personenbezogenen Daten an Microsoft übermittelt werden.

Die Datenschutzgrundverordnung (DS-GVO) verlangt von Verantwortlichen beim Einsatz von Windows 10, die datenschutzkonforme Verarbeitung personenbezogener Daten sicherzustellen. Dies bedeutet für die Verantwortlichen derzeit einen erheblichen Aufwand. Er ließe sich minimieren, wenn Microsoft den Verantwortlichen einfache Möglichkeiten insbesondere zur permanenten Deaktivierung aller Datenübermittlungen bereitstellen würde.

Die DSK hat sich entschlossen, dem Arbeitskreis Technik den Auftrag zu erteilen, eine datenschutzrechtliche Positionierung zum Einsatz von Windows 10 zu erarbeiten und diese zur Grundlage eines weitergehenden, vom LDA Bayern zu koordinierenden Dialoges mit Microsoft zu datenschutzrechtlichen Fragestellungen zum Produkt Windows 10 zu machen.

## - 03.04.2019 – Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO

Der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ wird in Erwägungsgrund 33 erwähnt, aber in der Datenschutz-Grundverordnung (DSGVO) nicht näher definiert. Er steht in einem engen inhaltlichen Zusammenhang mit der Zweckbestimmung, wie sie bei der Erteilung von Einwilligungen auszugestalten ist. Nach Art. 4 Nr. 11 DSGVO ist eine Einwilligung stets für den „bestimmten Fall“, in informierter Weise und unmissverständlich abzugeben. Das Erfordernis des „bestimmten Falls“ konkretisiert den Grundsatz der Zweckbindung im Sinne des Art. 5 Abs. 1 Buchst. b DSGVO, wonach personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke zu erheben sind.

In ihrem Arbeitspapier 259 rev 01, S. 33, weist die Artikel-29-Datenschutz-Gruppe überdies darauf hin, dass deswegen der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ von dem weit zu verstehenden Begriff der wissenschaftlichen Forschung in Art.

89 DSGVO zu unterscheiden ist. Dort geht es um den Anwendungsbereich der wissenschaftlichen Forschung, nicht um die Zweckbindung im Rahmen einer konkreten Datenverarbeitung. Demgegenüber ist der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ enger zu verstehen.

Daraus folgt: Nur wenn das konkrete Design des Forschungsvorhabens absehbar bis zum Zeitpunkt der Datenerhebung eine vollständige Zweckbestimmung schlechthin nicht zulässt (vgl. Erwägungsgrund 33, Satz 1), kann beispielsweise der Ansatz der breiten Einwilligung (broad consent) zum Tragen kommen. Bei der einer Datenerhebung zeitlich vorgelagerten Einwilligung können dann unter engen Voraussetzungen Abstriche hinsichtlich der Bestimmtheit des Zwecks hingenommen werden.

Auch der Erwägungsgrund 33 entbindet allerdings nicht von der Pflicht, im Kontext von Forschungsprojekten Mechanismen herauszuarbeiten, nach denen die Verwendung der erhobenen Daten für die betroffene Person nachvollziehbar eingegrenzt wird. Insbesondere wird es nicht als mit dem Erwägungsgrund 33 vereinbar erachtet, wenn die Verwendung der erhobenen Daten pauschal auf bestimmte Forschungsbereiche ausgeweitet wird. Das Gebot einer informierten Einwilligung erfordert zumindest, dass möglichst präzise das jeweilige Forschungsvorhaben und nachfolgend aufgeführte spezifische Sicherungsmaßnahmen von der Einwilligungserklärung erfasst werden.

In den Einzelfällen, in denen das Arbeiten mit breiten Einwilligungen als für das Erreichen des Forschungszwecks zwingend erforderlich erachtet wird, ist deshalb insbesondere mit den folgenden Korrektiven zu arbeiten. Sie dienen der Transparenz, Vertrauensbildung und Datensicherheit, um die abstraktere Fassung des Forschungszwecks zu kompensieren:

**A. Zusätzliche Sicherungsmaßnahmen zur Gewährleistung von Transparenz**

- Verwendung einer für den Einwilligenden zugänglichen Nutzungsordnung oder eines einsehbaren Forschungsplanes, der die geplanten Arbeitsmethoden und die Fragen, die Gegenstand der Forschung sein sollen, beleuchtet
- Ausarbeitung und Dokumentation im Hinblick auf das konkrete Forschungsprojekt, wieso in diesem Fall eine nähere Konkretisierung der Forschungszwecke nicht möglich ist
- Einrichten einer Internetpräsenz, durch die die Studienteilnehmer über laufende und künftige Studien informiert werden

**B. Zusätzliche Sicherungsmaßnahmen zur Vertrauensbildung**

- Positives Votum eines Ethikgremiums vor der Nutzung für weitere Forschungszwecke
- Prüfung, ob das Arbeiten mit einem dynamic consent möglich ist bzw. Einräumung einer Widerspruchsmöglichkeit vor der Verwendung der Daten für neue Forschungsfragen

**C. Zusätzliche Garantiemaßnahmen zur Datensicherheit**

Verstärkter Einsatz von Garantien im Hinblick auf die erhobenen Daten durch technisch-organisatorische Maßnahmen wie:

- Keine Datenweitergabe in Drittländer mit geringerem Datenschutzniveau
- Gesonderte Zusagen zur Datenminimierung, Verschlüsselung, Anonymisierung oder Pseudonymisierung
- Spezifische Vorschriften für die Begrenzung des Zugriffs auf die erhobenen Daten

Das Ergebnis der Prüfung einschließlich der zugrunde liegenden Beweggründe sowie die Sicherstellung der o. g. Sicherungsmaßnahmen sind zu dokumentieren und den zur Prüfung der ethischen und datenschutzrechtlichen Vereinbarkeit des Forschungsvorhabens zuständigen Stellen zusammen mit dem Forschungskonzept vorzulegen.

## ▪ 01.04.2019 – Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit[1]

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich am 5. September 2018 zu dem (Weiter-)Betrieb von Facebook-Fanpages nach dem Urteil des EuGH vom 5. Juni 2018 geäußert. In ihrem Beschluss hat die Konferenz deutlich gemacht, dass Fanpage-Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DSGVO nachweisen können müssen. Dies ergibt sich aus der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO sowie insbesondere in Bezug auf Verpflichtungen nach Art. 24, 25, 32 DSGVO.

Am 11. September 2018 veröffentlichte Facebook eine sog. „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ sowie „Informationen zu Seiten-Insights“. Diese von Facebook veröffentliche „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ erfüllt nicht die Anforderungen an eine Vereinbarung nach Art. 26 DSGVO. Insbesondere steht es im Widerspruch zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO, dass sich Facebook die alleinige Entscheidungsmacht „hinsichtlich der Verarbeitung von Insights-Daten" einräumen lassen will. Die von Facebook veröffentlichten Informationen stellen zudem die Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere Seiten-Insights durchgeführt werden und der gemeinsamen Verantwortlichkeit unterfallen, nicht hinreichend transparent und konkret dar. Sie sind nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung

[1] Unter Enthaltung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit

der personenbezogenen Daten der Besucherinnen und Besucher ihrer Fanpage zu ermöglichen. Vor diesem Hintergrund bekräftigt die Konferenz erneut die Rechenschaftspflicht der Fanpage-Betreiber (unabhängig von dem Grad der Verantwortlichkeit) und stellt fest:

1. Jeder Verantwortliche benötigt für die Verarbeitungstätigkeiten, die seiner Verantwortung unterliegen, eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO und – soweit besondere Kategorien personenbezogener Daten verarbeitet werden – nach Art. 9 Abs. 2 DSGVO. Dies gilt auch in den Fällen, in denen sie die Verarbeitungstätigkeiten nicht unmittelbar selbst durchführen, sondern durch andere gemeinsam mit ihnen Verantwortlichen durchführen lassen.

2. Ohne hinreichende Kenntnis über die Verarbeitungstätigkeiten, die der eigenen Verantwortung unterliegen, sind Verantwortliche nicht in der Lage, zu bewerten, ob die Verarbeitungstätigkeiten rechtskonform durchgeführt werden. Bestehen Zweifel, geht dies zulasten der Verantwortlichen, die es in der Hand haben, solche Verarbeitungen zu unterlassen. Der EuGH führt hierzu aus: „Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien.“ (EuGH, C-210/16, Rn. 40).

3. Im Hinblick auf die Ausführungen zur „Hauptniederlassung für die Verarbeitung von Insights-Daten für sämtliche Verantwortliche“ sowie zur federführenden Aufsichtsbehörde (Punkt 4 in der „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“) weist die Konferenz darauf hin, dass sich die Zuständigkeit der jeweiligen Aufsichtsbehörden für Fanpage-Betreiber nach der DSGVO richtet. Nach Art. 55 ff. DSGVO sind die Aufsichtsbehörden für Verantwortliche (wie z. B. Fanpage-Betreiber) in ihrem Hoheitsgebiet zuständig. Dies gilt unabhängig von den durch die DSGVO vorgesehenen Kooperations- und Kohärenzmechanismen.

Sowohl Facebook als auch die Fanpage-Betreiber müssen ihrer Rechenschaftspflicht nachkommen. Die Datenschutzkonferenz erwartet, dass Facebook entsprechend nachbessert und die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend gerecht werden. Solange diesen Pflichten nicht nachgekommen wird, ist ein datenschutzkonformer Betrieb einer Fanpage nicht möglich.

## ▪ 26.04.2019 – Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen

Zukünftig sollen nach einem Referentenentwurf zur Änderung des Rundfunkbeitragsstaatsvertrags (RBStV) regelmäßig alle vier Jahre Meldedaten sämtlicher volljähriger Personen an die jeweils zuständige Landesrundfunkanstalt zur Sicherstellung der Aktualität des dortigen Datenbestandes übermittelt werden. Gemäß Art. 1 Ziffer 7 dieses Entwurfs des 23. Rundfunkänderungsstaatsvertrages vom 5. Februar 2019 zählen zu den Meldedaten neben Namen und gegenwärtiger und letzter Anschrift insbesondere auch Geburtstag, Titel, Familienstand sowie die genaue Lage der Wohnung.

Bereits der im Jahr 2013 durchgeführte vollständige Meldedatenabgleich war seinerzeit auf erhebliche datenschutzrechtliche Bedenken gestoßen (vgl. Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 11. Oktober 2010). Die DSK stellte ihre Bedenken nur deshalb teilweise zurück, weil lediglich ein einmaliger Meldedatenabgleich vorgenommen werden sollte, um den Start in das neue Beitragsmodell zu erleichtern. Mit der nun vorgesehenen Regelung wären die – bereits damals zweifelhaften – Zusicherungen des Gesetzgebers, dass es sich bei den anlasslosen vollständigen Meldedatenabgleichen aus den Jahren 2013 und 2018 um einmalige Vorgänge handeln würde, endgültig hinfällig.

Gegen die geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs bestehen weiterhin grundlegende verfassungsrechtliche und datenschutzrechtliche Bedenken.

Ein solcher Abgleich stellt einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung dar und gerät in Konflikt mit den Grundsätzen der Datenminimierung und der Erforderlichkeit gemäß Art. 5 Abs. 1 lit. a und c, Art. 6 Abs. 1 der Datenschutz-Grundverordnung (DSGVO).

Bei einem vollständigen Meldedatenabgleich werden in großem Umfang personenbezogene Daten von Betroffenen, die überhaupt nicht beitragspflichtig sind, weil sie entweder in einer Wohnung leben, für die bereits durch andere Personen Beiträge gezahlt werden oder weil sie von der Beitragspflicht befreit sind, an die Rundfunkanstalten übermittelt und von diesen verarbeitet. Zudem werden auch Daten von all denjenigen Einwohnerinnen und Einwohnern erhoben und verarbeitet, die sich bereits bei der Landesrundfunkanstalt angemeldet haben und regelmäßig ihre Beiträge zahlen. Dabei betrifft der geplante Meldedatenabgleich mehr personenbezogene Daten, als die Beitragszahlerinnen und -zahler bei der Anmeldung mitteilen müssen, z.B. Doktorgrad und Familienstand (vgl. § 8 Abs. 4 RBStV). Es sollen also personenbezogene Daten an die Rundfunkanstalten übermittelt werden, die nicht zur Beitragserhebung notwendig sind.

Die Meldedaten-Übermittlungsverordnungen der Länder bieten mit der anlassbezogenen Meldedatenübermittlung an die Rundfunkanstalten bereits eine angemessene und ausreichende Möglichkeit, die Aktualität des Datenbestandes des Beitragsservices auch bei Veränderungen der Meldesituation der Beitragsschuldnerinnen und Beitragsschuldner zu gewährleisten. Auch wenn die Meldebehörden in Einzelfällen eine Änderungsmitteilung unterlassen sollten, würde ein erneuter vollständiger Meldedatenabgleich in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung der Beitragsschuldner eingreifen, ohne dass dies durch andere Gesichtspunkte, etwa das Ziel der Gebührengerechtigkeit, gerechtfertigt wäre.

Die Landesrundfunkanstalten gehen selbst davon aus, dass ein vollständiger Meldedatenabgleich letztlich in weniger als einem Prozent der Fälle zu einer zusätzlichen, dauerhaften Anmeldung von Beitragspflichtigen führt (vgl. Evaluierungsbericht der Länder gem. § 14 Abs. 9a RBStV vom 20. März 2019).

Die geplanten Regelungen berücksichtigen zudem die Maßstäbe der DS-GVO nicht ausreichend. Nationale Datenschutzvorschriften müssen aufgrund des Anwendungsvorrangs europäischer Verordnungen auf eine Öffnungsklausel der DS-GVO gestützt werden können. Art. 85 Abs. 2 DS-GVO ist nicht einschlägig, da die Datenverarbeitung zum Zweck des Einzugs des Rundfunkbeitrags nicht in dem Anwendungsbereich dieser Norm liegt. Bei Regelungen, die auf die Öffnungsklausel nach Art. 6 Abs. 2 und Abs. 3 i. V. m. Art. 6 Abs. 1 lit. e) DS-GVO gestützt werden, sind die Grundsätze der Datenminimierung und Erforderlichkeit zu beachten. Mitgliedstaatliche Regelungen für die Erfüllung von Aufgaben, die im öffentlichen Interesse liegen, dürfen danach eingeführt werden, wenn diese die DS-GVO zwar präzisieren, nicht aber deren Grenzen überschreiten. Regelungen, die sich auf diese Öffnungsklausel beziehen, müssen sich folglich in dem Rahmen halten, den die DS-GVO vorgibt. Hier bestehen erhebliche Bedenken im Hinblick auf die Grundsätze der Datenminimierung und der Erforderlichkeit.

Positiv hervorzuheben ist zwar, dass die bisherige Vermieterauskunft im Hinblick auf Mietwohnungen aus § 9 Abs. 1 Satz 2 und 3 RBStV gestrichen werden soll. Ebenso soll der Ankauf von Adressdaten von Privatpersonen ausdrücklich ausgeschlossen werden. Beide Datenverarbeitungen sind aus Sicht des Datenschutzes kritisch zu sehen und ihre Streichung ist zu begrüßen. Dabei darf jedoch nicht übersehen werden, dass mit dem geplanten regelmäßigen vollständigen Meldedatenabgleich eine weitaus umfassendere, datenschutzrechtlich ebenfalls sehr bedenkliche Möglichkeit der Datenerhebung geschaffen werden soll, die das praktische Bedürfnis der Vermieterauskunft und des Ankaufs privater Adressen ohnehin entfallen lässt.

**Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert, den geplanten regelmäßigen vollständigen Meldedatenabgleich nicht einzuführen, da gegen die vorgesehenen Regelungen grundlegende verfassungsrechtliche Bedenken bestehen und diese die Maßstäbe der DS-GVO nicht ausreichend berücksichtigen.**

- **13.05.2019 – Beschluss zur Beteiligung der spezifischen Aufsichtsbehörden gem. § 18 Abs. 1 Satz 4 BDSG an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der EU**

1. Die Verpflichtung zur Beteiligung der spezifischen Aufsichtsbehörden nach § 18 Abs. 1 Satz 4 BDSG ist nur dann eröffnet, wenn es sich um Angelegenheiten der Europäischen Union handelt.

2. Liegen die Voraussetzung von Nr. 1 vor, ist eine Betroffenheit in folgenden Konstellationen gegeben:

a) eine spezifische Aufsichtsbehörde ist im Kooperationsverfahren nach Art. 60 DSGVO unmittelbar selbst federführende Behörde im Sinne von § 19 Abs. 1 BDSG (vgl. Art. 56 DSGVO);

b) eine spezifische Aufsichtsbehörde ist für die Bearbeitung einer Eingabe entsprechend § 19 Abs. 2 BDSG (vgl. Art. 4 Nr. 22 Buchst. c DSGVO) zuständig;

c) eine spezifische Aufsichtsbehörde ist in entsprechender Anwendung von § 40 Abs. 2 BDSG in der Rolle als betroffene Behörde (vgl. Art. 4 Nr. 22 Buchs. a DSDGVO) zuständig;

d) eine spezifische Aufsichtsbehörde ist in den Verfahren nach Art. 60 DSGVO in der Konstellation des Art. 4 Nr. 22 Buchst. b DSGVO betroffen, wenn sich die erheblichen Auswirkungen nur im Rahmen der ausschließlichen Zuständigkeiten der spezifischen Aufsichtsbehörde bewegen;

e) ein Verfahren der Amtshilfe nach Art. 61 DSGVO oder gemeinsame Maßnahmen spielen sich unmittelbar im Zuständigkeitsbereich einer spezifischen Aufsichtsbehörde ab.

3.

a) Im Kohärenzverfahren nach Art. 64 DSGVO, ggf. zusätzlich im Verfahren der verbindlichen Streitbeilegung nach Art. 65 DSGVO (bei unmittelbarer Zuständigkeit siehe oben 2);

und

b) bei der Erarbeitung von Stellungnahmen und der Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren i. S. v. Art. 70 DSGVO

liegt nur dann eine Betroffenheit vor, wenn spezifische Fragen der Verarbeitung personenbezogener Daten durch die der Aufsicht der spezifischen Aufsichtsbehörden unterliegenden Stellen betroffen sind.

> Erläuterung: Spezifische Betroffenheit bedeutet, dass gerade die spezifische Aufsichtsbehörde in einer Weise von der Angelegenheit betroffen sein muss, die über eine allgemeine Mitbetroffenheit hinausgeht. Ist sie lediglich in gleicher Weise betroffen wie die staatlichen Aufsichtsbehörden, liegt keine spezifische Betroffenheit vor und die Beteiligungspflicht wird nicht ausgelöst. Dabei kommt es nicht nur darauf an, dass bspw. Kirchen, Religionsgemeinschaften oder Medien-/Rundfunkveranstalter ausdrücklich Gegenstand einer Angelegenheit sind. Eine spezifische Betroffenheit ist vielmehr auch dann anzunehmen, wenn der Gegenstand einer Angelegenheit in besonderer Weise den Zuständigkeitsbereich der spezifischen Aufsichtsbehörden berührt.

4. Die Aufsichtsbehörden des Bundes und der Länder können für alle weiteren Fälle eine Beteiligung vorsehen.

5. Die Verpflichtungen zur Beteiligung nach § 18 Abs. 1 Satz 4 BDSG sind erfüllt, wenn die spezifischen Aufsichtsbehörden frühzeitig mit allen zweckdienlichen Informationen versorgt sind und ihnen frühzeitig Gelegenheit zur Stellungnahme gegeben wird. Die Betroffenheit einer spezifischen Aufsichtsbehörde wird von der Aufsichtsbehörde geprüft, die die Herstellung einer Positionsbestimmung in europäischen Angelegenheiten initiiert. Die Beteiligung der spezifischen Aufsichtsbehörden wird über die Zentrale Anlaufstelle sichergestellt. Die Aufsichtsbehörden des Bundes und der Länder berücksichtigen die Stellungnahmen der spezifischen Aufsichtsbehörden. Eine abweichende Stellungnahme ändert aber weder etwas an einem sonst unter den Aufsichtsbehörden von Bund und Ländern bestehenden Einvernehmen noch hat dies Auswirkungen auf Abstimmungen nach § 18 Abs. 2 BDSG.

6. Bei § 18 Abs. 1 Satz 4 BDSG handelt es sich um eine Verfahrensregelung, deren Nichteinhaltung keine rechtlichen Folgen für das Verfahren hat.

7. Die spezifischen Aufsichtsbehörden werden durch die Aufsichtsbehörden des Bundes und der Länder regelmäßig über die Entwicklungen auf europäischer Ebene informiert.

8. Gemeinsam mit dem BfDI lädt der Vorsitz der Datenschutzkonferenz Vertreter der spezifischen Aufsichtsbehörden zweimal jährlich zu einem Informations- und Erfahrungsaustausch ein.

9. Religions- und Weltanschauungsgemeinschaften können nach Artikel 91 Absatz 2 DSGVO nur dann eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, einrichten, wenn sie bereits zum Zeitpunkt des Inkrafttretens der DSGVO am 25. Mai 2016 umfassende Datenschutzregelungen i. S. v. Art. 91 Abs. 1 DSGVO angewendet haben. Diese Datenschutzregelungen müssen mit der DSGVO in Einklang gebracht werden.

10. Weitere Erläuterungen ergeben sich aus den Arbeitsergebnissen der 9. Sitzung des AK Grundsatz, die die DSK am 29. Januar 2019 zustimmend zur Kenntnis genommen hat.

## ▪ 24.05.2019 – Asset Deal – Katalog von Fallgruppen

Unter Ablehnung der Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie des Sächsischen Datenschutzbeauftragten.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich auf einen Katalog von Fallgruppen verständigt, die im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f i.V.m. Abs. 4 DS-GVO bei einem Asset Deal zu berücksichtigen sind. Die Fallgruppen lauten:

**1. Kundendaten bei laufenden Verträgen**

Hier bedarf der Vertragsübergang zivilrechtlich einer Genehmigung der Kundin oder des Kunden (§ 415 BGB / Schuldübernahme). In dieser zivilrechtlichen Genehmigung wird als Minus auch die datenschutzrechtliche Zustimmung zum Übergang der erforderlichen Daten gesehen. Damit sind die Gegeninteressen der Kundin oder des Kunden gewahrt.

2. **Bestandskunden ohne laufende Verträge und letzter Vertragsbeziehung älter als 3 Jahre[1]**

Daten von Bestandskundinnen und -kunden, bei denen die letzte aktive Vertragsbeziehung mehr als 3 Jahre zurückliegt, unterliegen bei einer erwerbenden Stelle einer Einschränkung der Verarbeitung. Diese Daten dürfen zwar übermittelt, aber eben nur wegen gesetzlicher Aufbewahrungsfristen genutzt werden.

Denkbare Alternative ist, dass entsprechende Kundendaten nicht übertragen werden, sondern beim Alt-Unternehmen verbleiben. Ist ein Insolvenzverwalter eingeschaltet, bemüht dieser sich um einen aus der Masse zu finanzierenden Dienstleister, der die Alt-Daten für einen bestimmten Zeitraum aufbewahrt.

[1] Die 3-Jahresfrist berücksichtigt die regelmäßige Anspruchsverjährung. Zudem haben erfahrungsgemäß nichtaktive Kundendaten älter als 3 Jahre für die erwerbende Stelle keine Bedeutung mehr und sind veraltet.

**3. Daten von Kundinnen und Kunden bei fortgeschrittener Vertragsanbahnung; Bestandskundinnen und -kunden ohne laufende Verträge und letzter Vertragsbeziehung jünger als 3 Jahre[1]**

Daten solcher Kundinnen und Kunden werden nach Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO im Wege der Widerspruchslösung (Opt-out-Modell) mit einer ausreichend bemessenen Widerspruchsfrist (z. B. 6 Wochen) übermittelt. Diese Vorgehensweise ist für die Unternehmen aufwandsschonend und berücksichtigt durch die großzügige Widerspruchsfrist auch die Interessen der Kundinnen und Kunden. Viele Kundinnen und Kunden sind bei einer Aufforderung zu einer ausdrücklichen Einwilligung eher überrascht. Auch sollte darauf geachtet werden, den Widerspruch einfach auszugestalten – z.B. im Online-Verfahren durch Klick auf ein Kästchen.

Die Bankdaten (IBAN) sind jedoch vom Übergang per Widerspruchslösung ausgenommen und nur nach ausdrücklicher Einwilligung des Kunden zu übermitteln. Darunter fällt nicht das Zahlungsverhalten.

**4. Kundendaten im Falle offener Forderungen**

Die Übertragung offener Forderungen gegen Kundinnen und Kunden richtet sich zivilrechtlich nach den §§ 398 ff. BGB (Forderungsabtretung). In diesem Zusammenhang stehende Daten darf der Zedent (Alt-Gläubiger/Alt-Unternehmen) an den Zessionar (Neu-Gläubiger/Neu-Unternehmen) – gestützt auf Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO – (früher § 28 Abs. 1 Satz 1 Nr. 2 oder Abs. 2 Nr. 2 lit. a BDSG a.F.) übermitteln. Überwiegende Gegeninteressen bestehen allerdings dann, wenn die Abtretung durch Vereinbarung ausgeschlossen ist (§ 399 2. Alt. BGB, § 354a HGB).

**5. Kundendaten besonderer Kategorie nach Art. 9 Abs. 1 DS-GVO**

Solche Daten können nur im Wege der informierten Einwilligung nach Art. 9 Abs. 2 lit. a), Art. 7 DS-GVO übergeleitet werden.

## ▪ 12.08.2019 – Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu spezifischen Aufsichtsbehörden

Nach der Sonderregelung des Artikel 91 Absatz 1 der Europäischen Datenschutz-Grundverordnung (DSGVO) dürfen Kirchen, religiöse Vereinigungen oder Gemeinschaften, die zum Zeitpunkt des Inkrafttretens der DSGVO umfassende Regelungen zum

[1] Die 3-Jahresfrist berücksichtigt die regelmäßige Anspruchsverjährung. Zudem haben erfahrungsgemäß nichtaktive Kundendaten älter als 3 Jahre für die erwerbende Stelle keine Bedeutung mehr und sind veraltet.

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten anwenden, diese weiter anwenden, sofern sie mit den Vorschriften der DSGVO in Einklang gebracht werden.

Grundsätzlich unterliegen auch die Kirchen, religiösen Gemeinschaften oder Vereinigungen, die bereits zum Zeitpunkt des Inkrafttretens der DSGVO am 25. Mai 2016 umfassende Datenschutzregelungen i. S. v. Artikel 91 Absatz 1 DSGVO angewendet haben, nach Artikel 91 Absatz 2 DSGVO der Aufsicht durch eine unabhängige Aufsichtsbehörde. Artikel 91 Absatz 2 DSGVO erlaubt ihnen jedoch, eine unabhängige Aufsichtsbehörde spezifischer Art einzurichten.

Für Religionsgemeinschaften, die erst nach dem Inkrafttreten der DSGVO umfassende Datenschutzvorschriften erlassen (haben), ist der sachliche Anwendungsbereich der DSGVO uneingeschränkt eröffnet und es gilt die allgemeine Datenschutzaufsicht.

Bei Artikel 91 handelt es sich um eine Bestandsschutzregelung für die Datenschutzvorschriften derjenigen Kirchen und religiösen Vereinigungen oder Gemeinschaften, die zum Zeitpunkt des Inkrafttretens der DSGVO bereits ein umfassendes, in sich abgeschlossenes Datenschutzrecht etabliert hatten. Solche Religionsgemeinschaften sollen nicht gezwungen sein, ihr unter dem alten Recht bereits etabliertes Recht abschaffen zu müssen.

Die bestehenden Datenschutzregelungen müssen allerdings mit der DSGVO in Einklang gebracht worden sein. Dadurch soll trotz der Privilegierung dieser Regelungen ein einheitliches Niveau staatlichen und kirchlichen Datenschutzrechts erreicht werden.

Die „spezifischen“ Aufsichtsbehörden müssen darüber hinaus die in Kapitel VI der DSGVO für die unabhängigen Aufsichtsbehörden niedergelegten Voraussetzungen erfüllen. Das betrifft u.a. die Unabhängigkeit, Artikel 52 DSGVO, und die in Artikel 58 DSGVO geregelten Befugnisse.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sind gemäß § 18 Absatz 1 Satz 4 Bundesdatenschutzgesetz (BDSG) verpflichtet, diese spezifischen Aufsichtsbehörden bei der Zusammenarbeit in europäischen Angelegenheiten zu beteiligen, soweit sie betroffen sind.

Durch Anpassung des jeweils bereits vor dem 25. Mai 2016 bestehenden Gesetzes über den Kirchlichen Datenschutz sowie des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland an die DSGVO unterfallen zumindest die römisch-katholische Kirche bzw. die Adressaten des EKD-Datenschutzgesetzes grundsätzlich der durch Artikel 91 DSGVO ermöglichten Privilegierung.

## ▪ 12.09.2019 – Datenschutzrechtliche Verantwortlichkeit innerhalb der Telematik-Infrastruktur

Die Datenschutzkonferenz vertritt zur Frage der datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematik-Infrastruktur nach § 291a Abs. 7 SGB V folgende Auffassung:

Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) ist

a) datenschutzrechtlich alleinverantwortlich für die zentrale Zone der TI („TI-Plattform Zone zentral“) sowie

b) "b) im Sinne des Artikel 26 DSGVO datenschutzrechtlich mitverantwortlich für die dezentrale Zone der TI („TI-Plattform Zone dezentral“). Der Umfang der Verantwortung der gematik für die dezentrale Zone der Telematik-Infrastruktur bedarf einer gesetzlichen Regelung. Die gematik ist verantwortlich für die Verarbeitung, insbesondere soweit sie durch die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt ist."

## ▪ 12.09.2019 – Sachliche Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste

Auf Basis des Urteils des EuGH vom 13. Juni 2019 (Az. C – 193/18) zur Auslegung des Begriffs des „Telekommunikationsdienstes“ gelten für die Zuständigkeitsverteilung zwischen dem BfDI und den Aufsichtsbehörden der Länder vorbehaltlich einer Änderung der gesetzlichen Zuständigkeitsregelungen folgende Grundsätze:

1. Webmaildienste sind keine Telekommunikationsdienste i.S.d. Telekommunikationsgesetzes (TKG) in der derzeit geltenden Fassung. Dies gilt für reine Webmaildienste und für E-Maildienste, die zusammen mit einem Internetzugang angeboten werden, wenn die E-Mails (zumindest auch) über einen Webmailer abgerufen werden können. Daraus folgt, dass für die Datenschutzaufsicht mangels anderer besonderer Zuständigkeitsvorschriften allein die jeweiligen Landesdatenschutzaufsichtsbehörden zuständig sind. Die bisher beim Bundesbeauftragten für den Datenschutz (BfDI) geführten Verfahren werden an die jeweils zuständigen Landesaufsichtsbehörden zur Bearbeitung zuständigkeitshalber abgegeben.

2. Messenger-Dienste, die in einem geschlossenen System operieren, d.h. bei denen die Nutzer/innen nur unter sich und nicht mit Nutzer/innen anderer Dienste kommunizieren können, können auch nach der genannten Entscheidung des EuGH als Telekommunikationsdienste i.S.d. TKG angesehen werden

mit der Folge, dass für diese Dienste weiterhin der BfDI aufsichtsrechtlich zuständig ist (§ 115 Abs. 4 TKG).

## ▪ 25.09.2019 – Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu verhaltensbasierter Werbung

Am 04.06.2019 legte das Netzwerk Datenschutzexpertise bei einigen deutschen Datenschutzaufsichtsbehörden eine Beschwerde wegen der Datenverarbeitung im Rahmen personalisierter Online-Werbung ein. Die Unterzeichner der Beschwerde sind allesamt Vorsitzende von Menschenrechts- und Digitalrechtsorganisationen und bezeichnen sich ausdrücklich als Beschwerdeführer.

In der Beschwerde wird die Datenverarbeitung durch Google sowie weitere Anbieter, die Mitglieder des IAB Europe sind, gerügt.

Die Beschwerde umfasst eine detaillierte Beschreibung der Datenverarbeitung von Werbenetzwerken und weist auf mögliche Verstöße gegen die DS-GVO hin.

Die Beschwerde richtet sich allgemein gegen die Datenverarbeitung von Werbenetzwerken und umfasst nicht nur die Verarbeitung durch Google. Weitere Anbieter bzw. Akteure werden jedoch nicht ausdrücklich genannt, sodass sich die Beschwerde zunächst nur gegen Google richtet.

Vor diesem Hintergrund fasst die Datenschutzkonferenz den folgenden Beschluss:

I. Die Beschwerde erfüllt die Anforderungen gem. Art. 77 DSGVO, da sie

1. von natürlichen Personen als betroffenen Personen eingelegt wurden (die 4 Unterzeichner);

2. sich gegen einen konkreten Verantwortlichen richtet (Google) und

3. die betroffenen Personen beschwerdebefugt sind, da sie umfassend erläutern, dass die Datenverarbeitung bei der personalisierten Online-Werbung gegen die DS-GVO verstößt und sie dadurch in ihren Rechten verletzt werden.

II. Beschwerdegegner ist zunächst nur Google. Soweit sich die Beschwerde gegen dieses Unternehmen richtet, ist sie zunächst an den Hamburgischen Beauftragten weiterzuleiten.

IV. Das IAB Europe ist kein Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO, da es sich beim IAB Europe lediglich um einen Interessenverband von Unternehmen aus dem Bereich Programmatic Advertising handelt.

V. Sofern eine Aufsichtsbehörde der Auffassung ist, die Beschwerde sei dahingehend auszulegen, dass sich die Beschwerde gegen die jeweiligen Mitgliedsunternehmen des IAB Europe richtet, so ist mit der Beschwerde entsprechend Ziff. III. zu verfahren.

# Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO – November 2019

**Einleitender Überblick**

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) hat den folgenden Bericht über die Erfahrungen bei der Anwendung der DS-GVO erarbeitet und auf der 98. DSK am 06. November 2019 verabschiedet. Die DSK möchte damit die Erfahrungen der in ihr vertretenen deutschen Aufsichtsbehörden aus der praktischen Anwendung seit Geltungsbeginn der DS-GVO in den Evaluierungsprozess nach Art. 97 DS-GVO einbringen und daran anknüpfend in einigen Punkten auch Vorschläge für Verbesserungen unterbreiten, um einen optimalen Vollzug der DS-GVO zu gewährleisten.

Nach einem Jahr der Geltung der DS-GVO zieht die Europäische Kommission im Juli 2019 zu Recht eine positive Bilanz. Die DS-GVO habe die EU-Bürger zunehmend auf die Datenschutzbestimmungen und ihre Rechte aufmerksam gemacht, die Unternehmen passen ihre Praktiken an, sie erhöhen die Sicherheit ihrer Daten und entwickeln den Datenschutz als Wettbewerbsvorteil. Die Verordnung habe den nationalen Datenschutzbehörden mehr Befugnisse zur Durchsetzung der Vorschriften gegeben. Im ersten Jahr haben die nationalen Datenschutzbehörden diese neuen Befugnisse bei Bedarf wirksam genutzt, sie arbeiten im Rahmen des Kooperationsmechanismus enger zusammen.

Die DSK teilt die Auffassung, dass sich die DS-GVO mit ihrem Regelungskonzept und ihren Zielen im Wesentlichen bewährt. Die Ziele des verbesserten Grundrechtsschutzes und der Schaffung eines einheitlichen digitalen Binnenmarktes erscheinen durch die DS-GVO vorangebracht und auch tatsächlich erreichbar.

Als ein zentraler Aspekt der gesellschaftlichen Wahrnehmung und als Motor zur Entwicklung eines breitangelegten datenschutzrechtlichen Bewusstseins erwies sich, dass bei Verstößen gegen Datenschutznormen erstmals empfindliche Geldbußen drohen. Behörden und Betriebe stellen sich den Anforderungen. Sie agieren aber teilweise unsicher, Umsetzungsdefizite sind zu beobachten. Die Vorgaben an die Verantwortlichen sind vielfältig (die DS-GVO selbst, die Erwägungsgründe, Guidelines), sodass ein umfassendes Datenschutzmanagement des Verantwortlichen geboten ist. Dazu bedarf es einer Interpretation der Vorgaben, die unzählige Datenschutzberater anbieten. Der Bedarf, Orientierung durch die Aufsichtsbehörden zu erhalten ist noch immer sehr hoch. Dieser erhöhten Nachfrage begegneten die Aufsichtsbehörden mit einer intensiven Beratungstätigkeit, deren Kern darin besteht aus einer gestiegenen Anzahl von Rechts- und Informationsquellen einen roten Faden zu wirken, der es erlaubt, den Verantwortlichen pragmatische Handlungsempfehlungen zu geben. Die so gestiegene Akzeptanz

des Datenschutzrechts und der Arbeit der Aufsichtsbehörden muss nunmehr erhalten und ausgebaut werden.

In dieser Hinsicht sind die durch die enorm gestiegene Anzahl von Beschwerden, durch aufwändige grenzüberschreitende Zusammenarbeit (IMI) und intensivierte Beratung gestiegenen Anforderungen an die Aufsichtsbehörden teilweise nicht mit auskömmlicher Aufstockung an Personal und Sachmitteln begleitet worden. Gemäß Art. 52 Abs. 4 DS-GVO hat jeder Mitgliedstaat sicherzustellen, dass seine Aufsichtsbehörde mit den Ressourcen, „die sie benötigt“, ausgestattet wird.

Dies hat u. a. zur Folge, dass von einigen Aufsichtsbehörden anlasslose Kontrollen nicht im erforderlichen Maße durchgeführt werden können, so dass Verantwortliche ein Kontrolldefizit erkennen und in ihren Bemühungen zur Schaffung datenschutzkonformer Zustände nachlassen.

Neben den gesetzlich für die Evaluierung der DS-GVO durch die Kommission festgelegten Themen des Art. 97 Abs. 2 DS-GVO wurde der Fokus des vorliegenden Berichts auf etwaigen Änderungsbedarf aufgrund der Anwendungs-Erfahrungen im ersten Geltungsjahr der DS-GVO gelegt. Dies sowohl bezogen auf bestehende Vorschriften als auch auf die möglicherweise notwendige Schaffung weiterer Regelungen. Auch die Erwägungsgründe wurden in die Überlegungen miteinbezogen.

Die Frage der Befassung mit etwaigen Problemen bei der Umsetzung der DS-GVO in Bundes- und Landesrecht wurde nicht in den Bericht miteinbezogen. Soweit einzelne nationale Umsetzungsnormen problematisch oder kritikwürdig erscheinen, kann sich hieraus allerdings auch ein Änderungsbedarf an Öffnungsklauseln der DS-GVO ergeben.

Grundsätzlich nicht berücksichtigt oder auf essentielle Punkte reduziert wurden außerdem Klarstellungs-, Auslegungs-, Definitions- und Übersetzungsprobleme. Auch strittige Punkte, welche sich bereits im Gesetzgebungsverfahren abgezeichnet und bis heute als in der Anwendung problematisch erwiesen haben, wurden weitestgehend ausgeklammert.

Im Ergebnis haben sich im Zuge der Anwendung der DS-GVO bisher folgende Schwerpunktthemen herausgestellt:

1. Alltagserleichterung & Praxistauglichkeit
2. Datenpannenmeldungen 3. Zweckbindung
3. data protection by design
4. Befugnisse der Aufsichtsbehörden und Sanktionspraxis
5. Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz
6. Direktwerbung
7. Profiling
8. Akkreditierung

Bei den **Informations- und Transparenzpflichten** nach Art. 13 und 14 DS-GVO haben sich in der Praxis Umsetzungsprobleme gezeigt, z. B. bei telefonischer Datenerhebung. Hier geht es insbesondere um die Frage, ob zunächst eine allgemeinere Information an zentraler Stelle ausreicht und konkrete Informationen nur auf Verlangen nachgereicht werden können. Auch Umfang und Inhalt der Informationspflichten könnten möglicherweise praktikabler und bürgerfreundlicher definiert werden. In der Praxis stellt sich teilweise die Frage nach der **Alltagstauglichkeit** der Regelungen der DS-GVO. Möglichkeiten zur erleichterten Anwendung der Informationspflichten, die Pflicht zur Meldung von Datenschutzbeauftragten an die Aufsichtsbehörden sowie das Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO wurden in den Fokus genommen.

Eine allgemein umgreifende Sorge vor den Sanktionsmöglichkeiten der DS-GVO führt nach der Erfahrung der Aufsichtsbehörden dazu, dass viele Datenpannen gemeldet werden, welche tatsächlich gar keine **Datenpannen** sind oder deren Risiken schon längst beseitigt wurden. Daher waren exorbitante Steigerungsraten bei den Meldungen von Datenpannen zu verzeichnen.

Im Bereich der **Zweckbindung** haben sich in der Praxis vor allem Fragen im Hinblick auf die Rechtsgrundlage und die Voraussetzungen der Weiterverwendung der personenbezogenen Daten bei der Zweckänderung ergeben.

**Data protection by design** findet in der Praxis kaum Resonanz, da der Anwendungsbereich der DS-GVO Hersteller gerade nicht erfasst. Die DS-GVO stellt mit data protection by design / by default aber Grundsätze auf, die sich in der Sache an Hersteller richten, nimmt diesen aber nicht als Verantwortlichen in die Pflicht. Daher wird die Frage aufgeworfen, ob auch Hersteller, Lieferanten, Importeure und Verkäufer in die Pflicht genommen werden sollten, so wie es im Produkthaftungsrecht bereits der Fall ist.

Im Schwerpunktthema **„Befugnisse der Aufsichtsbehörden und Sanktionspraxis“** haben sich insbesondere Fragen nach dem Begriff des „Verarbeitungsvorgangs“ aus Art. 58 Abs. 2 lit. b DS-GVO sowie der Zusammenarbeit und des Auskunftsrechts der Aufsichtsbehörden im Bußgeldverfahren als besonders dringlich erwiesen. In einem weiteren in Art. 97 Abs. 2 lit. b DS-GVO aufgeführten Schwerpunkt werden die Erfahrungen der Aufsichtsbehörden mit den Themen **„Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz“** dargestellt.

Bei der **Direktwerbung** stellt sich in unterschiedlichen Konstellationen die Frage der Zulässigkeit, welche durch die Schaffung einer spezifischen Rechtsgrundlage gelöst werden könnte.

Als eine der zentralen datenschutzpolitischen Herausforderungen unserer Zeit wird das **Profiling** angesehen. Trotz vorhandener Begriffsdefinition wird der Prozess der Profilbildung als solcher von den meisten Normen der DS-GVO, etwa zur automatisierten Entscheidungsfindung, nicht erfasst, sodass eine Beurteilung meist nur nach den allgemeinen Tatbeständen des Art. 6 DS-GVO erfolgt. Die DSK fordert eine Verschärfung

des geltenden Rechtsrahmens, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen.

Beim Schwerpunkt **Akkreditierung** könnte durch eine Klarstellung in der DS-GVO eine erhebliche nationale Zuständigkeitsfrage geklärt und die Aufsicht durch die deutschen Datenschutzaufsichtsbehörden sichergestellt werden.

In einer kurzen Liste weiterer Änderungsvorschläge sind konkrete Textänderungen samt Kurzbegründung aufgeführt, welche keinem Schwerpunktthema zuzuordnen sind, aber weitere Erleichterungen in der Anwendung der DS-GVO ermöglichen würden.

Zum aktuell vorherrschenden Thema in der wissenschaftlichen Auseinandersetzung – der Frage des Datenschutzes im Bereich der **Künstlichen Intelligenz** und automatisierten Entscheidungsverfahren – übersendet die DSK außerdem ihre „Hambacher Erklärung zur Künstlichen Intelligenz - Sieben datenschutzrechtliche Anforderungen“ vom 3. April 2019 im Anhang zur Kenntnis. Wenngleich die enthaltenen Forderungen sich auf zukünftige Fall- und Normkonstellationen beziehen, halten die deutschen Datenschutzaufsichtsbehörden die Beachtung dieser Grundsätze in den zukünftigen Evaluierungsprozessen für unerlässlich.

## Schwerpunktthema Nr. 1 – Alltagserleichterung & Praxistauglichkeit

Bei der Beratung, Fallbearbeitung sowie dem Austausch mit Verantwortlichen ist den deutschen Datenschutzaufsichtsbehörden häufig Unverständnis für die Regelungen beziehungsweise den Umfang der Informationspflichten, des Verzeichnisses der Verarbeitungstätigkeiten sowie der Notwendigkeit von Datenschutzfolgenabschätzungen entgegengeschlagen. Vor allem kleine und mittlere Unternehmen (KMU) sowie nicht-gewerbliche Vereine fühlen sich in Deutschland durch die Vorgaben der DS-GVO übermäßig belastet und fordern Ausnahmeregelungen.

### I. Informationspflichten

### 1. Problemaufriss

Die in Art. 13 und 14 DS-GVO geregelten Informations- und Transparenzpflichten sind ein Kernstück der Datenschutz-Grundverordnung. Die deutschen Aufsichtsbehörden erachten das u. a. in Art. 12 Abs. 1 DS-GVO ausgedrückte Anliegen, die betroffene Person in verständlicher und angemessener Form über ihre Datenschutzrechte zu informieren, für eine der wesentlichen Neuerungen durch die DS-GVO.

Teilweise wurde an deutsche Aufsichtsbehörden die Befürchtung herangetragen, die Erfüllung der Informationspflichten sei für Verantwortliche, wie z. B. Vereine und KMU möglicherweise zu aufwändig. Jedoch können auch kleine Einrichtungen Datenverarbeitungen vornehmen, die tiefgreifende Auswirkungen auf die Betroffenen haben.

Einige Verantwortliche haben außerdem gegenüber deutschen Aufsichtsbehörden Probleme adressiert, die bei der Erfüllung der Informationspflichten in bestimmten Kontexten auftreten, wie z. B. bei telefonischer Terminabsprache oder telefonischem Vertragsschluss und der damit verbundenen Datenerhebung.

Als Lösungsansatz wird zum Teil die Einführung einer an Art. 30 Abs. 5 DS-GVO angelehnten Ausnahme für Vereine und KMU mit unter 250 Mitarbeitern vorgeschlagen. Ein weiterer, am Risiko für die Betroffenen orientierter Lösungsansatz ist eine Reduzierung der Informationspflicht in Fällen, in denen die Datenverarbeitung sich in einem sehr engen und für die Betroffenen erwartbaren Rahmen hält.

## 2. Bewertung

Die Aufsichtsbehörden befürworten grundsätzlich einzelne Praxis-Erleichterungen, warnen aber vor generellen Ausnahmen von Verantwortlichen-Pflichten.

Aus den Erfahrungen der Aufsichtsbehörden in der Beratung von Unternehmen, deren Datenverarbeitung hauptsächlich im Rahmen von Kundenbeziehungen stattfindet, ergibt sich für gewisse Fallgestaltungen ein Bedarf an Erleichterungen bei den Informationspflichten. In der Bewertung kann zwischen einer digitalen und einer nicht digitalen Umgebung unterschieden werden.

In einer digitalen Umgebung sind die Informationspflichten regelmäßig gut erfüllbar. Gemäß ErwG 58 Satz 2 DS-GVO können die Informationen grundsätzlich in elektronischer Form zum Zeitpunkt der Erhebung bereitgestellt werden. Sofern der Verantwortliche eine Webseite betreibt, kann von ihm erwartet werden, die erforderlichen Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ anzubieten.

In bestimmten nicht digitalen Sachverhalten führt jedoch das Erfordernis der Information zum Zeitpunkt der Erhebung gemäß Art. 13 DS-GVO zu praktischen Zweifelsfragen. Vor allem bei mündlichen oder telefonischen Kontakten im geschäftlichen Bereich ist es lebensfremd zu erwarten, dass der Verantwortliche, wenn er eine Bestellung aufnimmt, eine Visitenkarte entgegennimmt oder einen Termin notiert, umfassende Informationen gemäß Art. 13 Abs. 1 und 2 DS-GVO erteilt, also die Rechtsgrundlage benennt, über die zuständige Datenschutzaufsichtsbehörde oder über Auskunfts-, Beschwerde- und sonstige Betroffenenrechte und anderes mehr informiert. Eine solche Information würde auch häufig auf das Unverständnis der Betroffenen stoßen und von diesen als störend empfunden werden.

Art. 13 Abs. 4 DS-GVO schließt die Informationspflichten zwar praxisgerecht aus, wenn und soweit die betroffene Person bereits über die Informationen verfügt; gerade im Rahmen von Unternehmen-Kunden-Beziehungen sind dem beauftragenden Kunden viele der informationspflichtigen Daten bereits bekannt. Nicht als bekannt vorausgesetzt werden kann grundsätzlich aber beispielsweise die Rechtsgrundlage der Datenverarbeitung (vgl. Art. 13 Abs. 1 lit. c DS-GVO). Diese ist jedoch nicht bei jeder Auftragserteilung, Terminvereinbarung etc. von Interesse. Betroffene klagten an dieser Stelle häufig über eine Informationsflut. Unter Berücksichtigung des risikobasierten Ansatzes bei der Beauftragung beispielsweise eines Handwerksbetriebs mit risikoarmer Datenverarbeitung würde es hier auch aus Sicht der Betroffenen genügen, wenn sie auf die Auffindbarkeit der Informationen hingewiesen werden.

In Einklang mit dem Working Paper der Art. 29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01), sprechen sich die deutschen Aufsichtsbehörden grundsätzlich dafür aus, die in Art. 13 DS-GVO genannten Informationspflichten in einem gestuften Verfahren erfüllen zu können. In geeigneten Fällen können die notwendigen Informationen beispielsweise auch mit der Übersendung einer Auftragsbestätigung, durch Aushang im Ladengeschäft oder auf ähnliche Weise erteilt werden. Von generellen Ausnahmen sollte allerdings abgesehen werden, um dem Ziel der Vorschrift nicht zuwider zu laufen.

### 3. Konkreter Änderungsvorschlag

Einfügen eines neuen Absatzes in Art. 13 DS-GVO:

> Die Informationen nach den Absätzen 1 und 2 werden nur auf Verlangen der betroffenen Person mitgeteilt, soweit der Verantwortliche Datenverarbeitungen vornimmt, die der Betroffene nach den konkreten Umständen erwartet oder erwarten muss und
>
> 1. sowohl die Offenlegung von Daten gegenüber anderen Stellen als auch die Übermittlung in Drittländer ausgeschlossen sind,
> 2. keine Daten verarbeitet werden, die unter Art. 9 DS-GVO fallen,
> 3. die Daten nicht zu Zwecken der Direktwerbung verarbeitet werden und
> 4. weder Profiling noch automatisierte Entscheidungsfindungen stattfinden.
>
> Die betroffene Person ist auf diese Möglichkeit hinzuweisen.

Außerdem sollte eine Ausnahme von den Informationspflichten zum Zeitpunkt der Erhebung für die Fälle vorgesehen werden, in denen Daten auf der Grundlage von Art. 6 Abs. 1 lit. d DS-GVO verarbeitet werden.

Begründung: Mit diesem Vorschlag soll der risikobasierten Betrachtung bei den Alltagserleichterungen Ausdruck verliehen werden.

## II. Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO

Das Auskunftsrecht nach Art. 15 DS-GVO ist eines der grundlegenden Betroffenenrechte. Ohne Informationen über die Verarbeitung ihrer personenbezogenen Daten können die betroffenen Personen ihre weiteren Rechte, wie z. B. das Recht auf Berichtigung oder Löschung oder das Recht zur Beschwerde bei einer Aufsichtsbehörde nicht effektiv wahrnehmen.

Allerdings ist die Weite des Auskunftsanspruchs umstritten, insbesondere in welchem Umfang Art. 15 Abs. 3 DS-GVO ein „Recht auf Kopie“ einräumt. Ein solches könnte den betroffenen Personen ermöglichen, vom Verantwortlichen die Herausgabe sämtlicher verarbeiteter personenbezogener Daten im Originalkontext zu verlangen. In der Praxis verlangen betroffene Personen zum Teil ohne nähere Konkretisierung Herausgabe aller beim Verantwortlichen vorhandenen Dokumente, die personenbezogene Daten enthalten. Dieser Anspruch kann z. B. auf die Kopie ganzer Verfahrensakten durch eine Behörde gerichtet sein oder auf die Herausgabe des gesamten geschäftlichen E-Mail-Verkehrs eines ehemaligen Mitarbeiters durch ein Unternehmen.

Eine Klarstellung hinsichtlich des Umfangs des von Art. 15 Abs. 3 DS-GVO gewährten Rechts erscheint wünschenswert.

## III. Pflicht zur Meldung von Datenschutzbeauftragten nach Art. 37 Abs. 7 DS-GVO

### 1. Problemaufriss

In Art. 37 Abs. 7 DS-GVO wird derzeit eine Pflicht konstatiert, der Aufsichtsbehörde Kontaktdaten von Datenschutzbeauftragten mitzuteilen. Die Verantwortlichen und Auftragsverarbeiter müssen gewährleisten, dass deren Meldung/en stets auf aktuellem Stand sind. Sie müssen diese nachhalten und ggf. gegenüber der zuständigen Aufsichtsbehörde korrigieren.

Durch die Pflicht, neben der Veröffentlichung der Kontaktdaten diese auch den Aufsichtsbehörden zu melden und beständig zu aktualisieren, entsteht bei den Verantwortlichen ein zusätzlicher Verwaltungsaufwand. Auf Seiten der Aufsichtsbehörden wird hierdurch eine nicht erforderliche Datenverarbeitung in Form einer Entgegennahme von Erst-, Änderungs- und Löschungsmeldungen ausgelöst. Teilweise wird Art. 37 Abs. 7 DS-GVO so interpretiert, dass die Aufsichtsbehörden ein Register der Datenschutzbeauftragten zu führen hätten (inkl. der Verpflichtung, eine Vollständigkeit sicherzustellen und Unstimmigkeiten von Amts wegen zu bereinigen). Eine Vollständigkeit und Richtigkeit kann nur angestrebt, aber nie ganz erreicht werden. Im Hinblick auf die Tatsache, dass im nicht-öffentlichen Bereich ohne nähere Kenntnis der Organisation und des Geschäftsmodells des Verantwortlichen nicht über eine Benennungspflicht entschieden werden kann, sind dafür umfangreiche Datenerhebungen im Rahmen von Anhörungen erforderlich.

### 2. Bewertung

In der Praxis ist das Bereithalten von Kontaktdaten der oder des Datenschutzbeauftragten bei den Aufsichtsbehörden nicht erforderlich, da es eine Veröffentlichungspflicht gibt (Art. 37 Abs. 7 erster Satzteil DS-GVO). Bei Erstkontakten einer Aufsichtsbehörde mit Verantwortlichen könnten ggf. aktuelle Kontaktdaten der oder des Datenschutzbeauftragten mitgeteilt werden.

Zur Entlastung der Verantwortlichen bzw. Auftragsverarbeiter und der Datenschutzaufsichtsbehörden sollte diese Meldepflicht und die nicht erforderliche Datenverarbeitung, die zudem mangels Aktualität der Meldungen ungeeignet ist, entfallen.

### 3. Konkreter Änderungsvorschlag

In Art. 37 Abs. 7 DS-GVO sollte der letzte Halbsatz „und teilt diese Daten der Aufsichtsbehörde mit“ ersatzlos gestrichen werden.

## Schwerpunktthema Nr. 2 – Datenpannenmeldungen

### I. Art. 33 Abs. 1 DS-GVO

### 1. Problemaufriss

Nach Art. 33 Abs. 1 DS-GVO ist grundsätzlich jede Datenschutzverletzung der Aufsichtsbehörde zu melden. Eine Ausnahme besteht nur dann, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Verletzung des Schutzes personenbezogener Daten ist in Art. 4 Nr. 12 DS-GVO als Verletzung der Sicherheit legal definiert, die zu Vernichtung, Verlust, zur Veränderung oder unbefugten Offenbarung führt, und somit mit Art. 5 Abs. 1 lit. f) DS-GVO korrespondiert. Nach dem ErwG 85 DS-GVO kann die Verletzung des Schutzes einen physischen, materiellen oder immateriellen Schaden nach sich ziehen.

Da nach der vorherigen nationalen Rechtslage (§ 42a BDSG aF) eine Meldung nur bei bestimmten Datenarten erfolgen musste, hat sich die Zahl der Meldungen in der Bundesrepublik Deutschland deutlich erhöht. Für die Verantwortlichen besteht darüber hinaus die Schwierigkeit, einzuschätzen, in welchen Fällen kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Häufig dürfte dieses Risiko von Faktoren abhängen, die dem Verantwortlichen nicht bekannt sind. Darüber hinaus melden viele Verantwortliche vermeintliche Verstöße aus Furcht vor hohen Bußgeldern, ohne dass sie eine Risikoabwägung vorgenommen haben. Die sehr weite Fassung des Abs. 1 („voraussichtlich kein Risiko“) führt somit dazu, dass in sehr vielen Trivial- und Bagatellfällen Meldungen erfolgen, die eine hohe Belastung für die Aufsichtsbehörden darstellen und letztlich den Blick auf wirklich relevante Fälle verstellen.

### 2. Bewertung

Ein Risiko für die Rechte und Freiheiten natürlicher Personen kann in der Regel nicht vollkommen ausgeschlossen werden. Die Meldepflicht sollte daher auf Fälle beschränkt werden, die voraussichtlich zu einem mehr als nur geringen Risiko für die Rechte und Freiheiten natürlicher Personen führen.

Darüber hinaus sollte Art. 33 Abs. 1 DS-GVO auf Fälle ausgeweitet werden, bei denen nicht bekannt ist, ob eine Verletzung des Schutzes personenbezogener Daten stattgefunden hat, diese aber zu vermuten ist. Häufig liegt eine Verletzung der Sicherheit von Daten vor, es ist aber nicht bekannt, ob dies zu einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DS-GVO geführt hat.

Beispiel: Eine Dump (eine Kopie) einer umfangreichen Kundendatenbank war über Monate ungesichert über das Web zugänglich, Logfiles, über die ein Zugriff ausgeschlossen werden kann, liegen aber nur für wenige Tage vor. Eine Verletzung im Sinne von Art. 4 Nr. 12 DS-GVO kann (je nach Auslegung des Begriffs „Offenlegen“) hier nicht positiv festgestellt werde.

Hier sollte, wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich ist, eine Meldepflicht bestehen, sofern voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen gegeben ist.

### 3. Änderungsvorschlag

Art. 33 Abs. 1 Satz 1 und 2 DS-GVO neu, der bisherige Satz 2 wird zu Satz 3:

| |
|---|
| Im Falle einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich nicht nur zu geringen Risiken für die Rechte und Freiheiten natürlicher Personen führt, meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Art. 55 zuständigen Aufsichtsbehörde. Darüber hinaus meldet der Verantwortliche einen Verstoß gegen die Anforderungen an die Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 DS-GVO, die wahrscheinlich zur Verletzung des Schutzes personenbezogener Daten geführt hat oder führen wird, unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung der Sicherheit bekannt wurde, sofern im Fall der Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. |

## Schwerpunktthema Nr. 3 – Zweckbindung

### 1. Problemaufriss

Das Prinzip der Zweckbindung ist ein tragendes Prinzip des Datenschutzrechts. Es ist für die betroffenen Personen von praktisch sehr hoher Bedeutung, ob Daten, die sie einem Verantwortlichen zu bestimmten Zwecken preisgegeben haben, für andere Zwecke Verwendung finden dürfen. Die DS-GVO stellt daher besondere Voraussetzungen für die Weiterverarbeitung zu anderen Zwecken auf und sieht bei erlaubten zweckändernden Verarbeitungen eine Informationspflicht des Verantwortlichen vor.

Bei Anwendung des Art. 6 Abs. 4 DS-GVO gibt es Uneinigkeit darüber, ob für die zweckändernde Verarbeitung, die die Voraussetzungen des Art. 6 Abs. 4 DS-GVO an die Vereinbarkeit der Zwecke erfüllt, eine eigene Rechtsgrundlage erforderlich ist. Verantwortliche berufen sich z. B. bei der Weiterverwendung von Daten, die nach dem Gesetz, das ihnen die Datenverarbeitung erlaubt, streng zweckgebunden sind, darauf, dass nach ErwG 50 S. 2 DS-GVO für die zweckändernde Weiterverarbeitung keine eigene Rechtsgrundlage erforderlich sei, wenn der neue Zweck mit dem alten vereinbar ist. Demgegenüber haben jedoch betroffene Personen, die z. B. Daten gegenüber einem Verantwortlichen ohne rechtliche Verpflichtung preisgegeben haben, ein großes Interesse daran, auch vor einer Weiterverwendung zu einem neuen Zweck erneut über die Preisgabe der Daten entscheiden zu können. Deutsche Aufsichtsbehörden haben in derartigen Konflikten unter Berufung auf Art. 5 Abs. 1 lit. a in Verbindung mit Art. 6 Abs. 1 DS-GVO sowie auf ErwG 50 S. 8 DS-GVO gefordert, dass auch die zweckändernde Datenverarbeitung einer Rechtsgrundlage bedarf.

Abgesehen von dieser Frage hat sich in der Praxis die Privilegierung von Wissenschaft und Forschung in Art. 5 Abs. 1 lit. b i.V.m. Art. 6 Abs. 4 DS-GVO als zu weitgehend erwiesen.

## 2. Bewertung

Nach Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 DS-GVO muss jede Datenverarbeitung mindestens eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen erfüllen, um rechtmäßig zu sein. Rechtmäßigkeit (Art. 5 Abs. 1 lit. a DS-GVO) und Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) sind zwei unterschiedliche, nebeneinander stehende Prinzipien der Datenverarbeitung. Die Vorschrift des Art. 6 Abs. 4 DS-GVO betrifft das Prinzip der Zweckbindung. Hätte im Rahmen dieser Vorschrift eine Ausnahme von dem Erfordernis einer Rechtsgrundlage gemacht werden sollen, so hätte dies angesichts der Bedeutung und Konsequenzen einer solchen Ausnahme ausdrücklich im Verordnungstext geregelt werden müssen.

Art. 6 Abs. 4 DS-GVO spricht nur von der Vereinbarkeit der Zwecke. Sein Satz 1 sagt aus, dass bei zweckändernden Verarbeitungen, die nicht auf der Rechtsgrundlage Art. 6 Abs. 1 lit. a DS-GVO oder auf bestimmten Rechtsvorschriften der Union oder Mitgliedstaaten beruhen, die Vereinbarkeit der Zwecke geprüft werden muss. Nach dem Wortlaut bedeutet das nicht, dass bei diesen anderen zweckändernden Verarbeitungen die Prüfung der Vereinbarkeit des Zwecks die Rechtsgrundlage ersetzt, sondern, dass bei

zweckändernden Verarbeitungen, die auf anderen Rechtsgrundlagen beruhen, eine Prüfung der Vereinbarkeit der Zwecke erfolgen muss. Die Regelung impliziert also gerade, dass alle zweckändernden Verarbeitungen auf einer Rechtsgrundlage beruhen müssen.

Insofern irritiert die Aussage in Satz 2 des ErwG 50 DS-GVO, in dem es heißt, es sei bei Vereinbarkeit der Zwecke „keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten".

Auch wenn Satz 8 des gleichen ErwG konstatiert, dass in jedem Fall die in der Verordnung niedergelegten Grundsätze anzuwenden sind, kann dies die Irritation nicht ganz beseitigen, da der Widerspruch zwischen dem nur auf die Rechtsgrundlage bezogenen Satz 2 und dem auf alle Grundsätze der DS-GVO bezogenen Satz 8 des ErwG 50 DS-GVO bestehen bleibt. Zum Teil wird der Verbleib des Satzes 2 in ErwG 50 nach den Trilogverhandlungen als Redaktionsversehen angesehen. In der Praxis führt er zu großen Schwierigkeiten bei der Durchsetzung der Rechtmäßigkeitsanforderungen an zweckändernde Datenverarbeitung und sollte daher gestrichen werden.

### 3. Änderungsvorschläge

| |
|---|
| ErwG 50 Satz 2 DS-GVO wird gestrichen. |

| |
|---|
| Klarstellung in Art. 6 Abs. 4 DS-GVO: Weiterverarbeitungen auf Grundlage dieses Absatzes werden auf solche durch denselben Verantwortlichen beschränkt. |

## Schwerpunktthema Nr. 4 – data protection by design

### 1. Problemaufriss

Es sollten auch Hersteller, Lieferanten, Importeure, Verkäufer usw. in die Pflicht genommen werden, so wie dies im Produkthaftungsrecht (ProdHaftG bzw. RL 85/374/EWG) bereits der Fall ist.

Beim Begriff „Datenschutz durch Technikgestaltung" (data protection by design), der in Art. 25 Abs. 1 DS-GVO für den Verantwortlichen vorgeschrieben ist, stellt sich in der Praxis der Adressatenkreis als nicht weitreichend genug heraus.

Verantwortliche entwickeln in der Regel nicht selbst Hard- und Software. Sie sind weitgehend auf Hardware und Standardbetriebssysteme und -anwendungssoftware angewiesen. Auf Anbieterseite bestehen oft Mono- oder Oligopole, sodass Produkte und Einsatzbedingungen von der Anbieterseite diktiert werden können.

Die DS-GVO stellt mit „data protection by design / data protection by default“ Grundsätze auf, die sich an Hersteller richten, nimmt Hersteller aber nicht als solche in die Pflicht. Die Forderung nach „data protection by design / data protection by default“ läuft, wenn sie ausschließlich an die Verantwortlichen gerichtet wird, häufig ins Leere.

Die DS-GVO sollte daher auch die Hersteller von Software zur Einhaltung dieses datenschutzfördernden Designprinzips verpflichten. In der Praxis trifft dies insb. auf Hersteller von komplexer Software wie z. B. Betriebssystemen, Datenbankmanagementsystemen, Standard-Office-Paketen oder sehr speziellen Fachanwendungen zu.

Hierzu zwei Beispiele:

1. Betriebssysteme

Verantwortliche, die Server, Desktop-Computer, Notebooks, Tablets, Smartphones oder ähnliche Geräte betreiben, müssen eines der wenigen am Markt erhältlichen Betriebssysteme, die auf der jeweiligen Hardware laufen, einsetzen. In der Regel sind diese schon vorinstalliert. Nach derzeitiger Rechtslage ist es die Pflicht dieser Verantwortlichen, etwaige datenschutzrechtlich relevante Schwachstellen, Fehlkonfigurationen, aus ihrer Sicht unerwünschte Funktionen etc. zu finden und abzustellen. Den Hersteller trifft keine Pflicht, seine Produkte ohne diese Fehler auszuliefern.

2. Haustür-Schließzylinder mit App

Es gibt Schließsysteme für Haustüren, die ohne physischen Schlüssel auskommen. Der Berechtigte identifiziert sich mit seinem Smartphone, auf dem eine passende App läuft. Zwischen der App und dem (in einem Drittland ohne angemessenes Datenschutz-Niveau befindlichen) Hersteller findet Datenverkehr statt.

a) Setzt ein Unternehmen derartige Systeme ein, ist es selbst Verantwortlicher und muss Datenverarbeitungen verantworten, die es nicht durchschauen kann. Der Hersteller ist nicht effektiv greifbar.

b) Setzt eine Privatperson im Rahmen privat-familiärer Tätigkeit derartige Systeme ein, ist ein Verantwortlicher im Sinne der DS-GVO schon nicht vorhanden. Die Pflichten der DS-GVO treffen niemanden, gehen also ins Leere. Würde man hier den Importeur, Händler o.ä. in die Verantwortung nehmen können, so wäre für „den Datenschutz“ viel gewonnen.

**2. Bewertung**

Die bisherige Rechtslage widerspricht dem Ansatz von „data protection by design“ bzw. „by default“.

Entgegen ErwG 78 S. 4 DS-GVO werden Hersteller in keiner Weise ermutigt, „das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen“.

Damit bestehen nicht nur erhebliche Lücken im Bereich des Schutzes personenbezogener Daten (und anderer Daten, vgl. Richtlinie (EU) 2016/943), sondern es kommt zu einer Potenzierung von technischem und bürokratischem Aufwand bei dem Versuch, dezentral Mängel zu beseitigen, die zentral verursacht werden. Dies belastet alle Verantwortlichen und Auftragsverarbeiter, wobei KMU überproportional belastet werden.

Die Rechtslage widerspricht so auch allgemeinem Recht. Nach dem über die RL 85/374/EWG harmonisierten Produkthaftungsrecht haften Hersteller für Schäden, die durch ihre Produkte entstehen. Neben Herstellern haften auch Importeure, Lieferanten, etc. Es gilt, diese bereits harmonisierte Rechtslage in den Bereich des Schutzes personenbezogener Daten zu übertragen.

Daher sollte Ziel sein, auch für datenschutzrechtlich relevante Produkte stärker auch die Hersteller in die Verantwortung zu nehmen.

### 3. Änderungsvorschläge

Durch die folgenden Änderungsvorschläge (unterstrichen dargestellt) würde die DS-GVO Pflichten für Hersteller usw. aufstellen, deren Durchsetzung aber dem Verbraucherschutz- und ggf. auch dem Wettbewerbsrecht überlassen.

Art. 4 - Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck…

27. „Hersteller“ den Hersteller im Sinne von Art. 3 der Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte. Nr. 16 Buchstabe a gilt entsprechend. Soweit er über Zwecke und Mittel der Datenverarbeitung entscheidet, ist der Hersteller auch Verantwortlicher im Sinne der Nr. 7.

KAPITEL IV - Verantwortlicher und Auftragsverarbeiter, Hersteller

Abschnitt 1 - Allgemeine Pflichten

Art. 24 - Verantwortung des für die Verarbeitung Verantwortlichen und des Herstellers

(4) Der Hersteller entwickelt und gestaltet seine Produkte, Dienste und Anwendungen unter Berücksichtigung des Rechts auf Datenschutz und des Standes der Technik so,

dass er sicherstellt, dass Verantwortliche und Auftragsverarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen, ohne unzumutbare Änderungen an diesen Produkten, Diensten und Anwendungen vornehmen zu müssen. Er unterstützt sie bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30), bei der Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33) und bei der Benachrichtigung betroffener Personen (Art. 34), indem er ihnen auf Anfrage alle dazu notwendigen Informationen bereitstellt.

Art. 79 - Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche, Auftragsverarbeiter oder Hersteller

(1) Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Art. 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

(2) Für Klagen gegen einen Verantwortlichen, gegen einen Auftragsverarbeiter oder gegen einen Hersteller sind die Gerichte des Mitgliedstaats zuständig, in dem der Hersteller, Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen, dem Auftragsverarbeiter oder dem Hersteller um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

Art. 82 - Haftung und Recht auf Schadenersatz

(7) Beruht der Schaden ganz oder teilweise auf Handlungen oder Versäumnissen des Herstellers, so haftet dieser gegenüber der betroffenen Person neben dem Verantwortlichen oder Auftragsverarbeiter. Er haftet auch gegenüber dem Verantwortlichen und dem Auftragsverarbeiter.

## Schwerpunktthema Nr. 5 – Befugnisse der Aufsichtsbehörden und Sanktionspraxis

### I. Befugnisse

### 1. Problemaufriss

Die Worte „mit Verarbeitungsvorgängen“ in Art. 58 Abs. 2 lit. b DS-GVO führen zu Problemen bei der Anwendung der Vorschrift. Es gibt in der DS-GVO verschiedene Pflichten, die von einer konkreten Verarbeitung unabhängig sind, wie z. B. die Bestellung eines

Datenschutzbeauftragten (Art. 37 DS-GVO) oder Vertreters (Art. 27 DS-GVO) oder die Pflicht zur Führung eines Verarbeitungsverzeichnisses (Art. 30 DS-GVO). Es ist deshalb für die Aufsichtsbehörden fraglich, auf welcher Rechtsgrundlage sie bei derartigen Verstößen eine Verwarnung aussprechen können.

### 2. Bewertung

Die Grundsätze, denen eine Verarbeitung entsprechen muss, sind in Art. 5 DS-GVO niedergelegt und in weiteren Vorschriften der DS-GVO genauer aufgeführt. Es gibt in der DS-GVO Pflichten, die von diesen Verarbeitungsgrundsätzen unabhängig sind. Zumindest für die Bestellung eines Datenschutzbeauftragten oder Vertreters oder für die Pflicht zur Führung eines Verarbeitungsverzeichnisses ist nicht ersichtlich, dass sie einen der in Art. 5 DS-GVO niedergelegten Grundsätze der Verarbeitung ausfüllen. Daher wird durch die Verletzung der genannten Pflichten die einzelne Verarbeitung nicht unzulässig. Es besteht aber ein praktischer Bedarf, auch bei derartigen Verstößen eine Verwarnung aussprechen zu können. Zur Vermeidung von Wertungswidersprüchen sollte diese Möglichkeit bei allen Verstößen gegen die Verordnung bestehen.

Zum Vergleich: Auch die Sanktionen in Art. 83 DS-GVO knüpfen nicht an Verarbeitungsvorgänge, sondern lediglich an „Verstöße gegen diese Verordnung“ (Abs. 1) bzw. „Verstöße gegen die folgenden Bestimmungen“ (Abs. 4, 5) an.

### 3. Änderungsvorschläge

Keine Beschränkung der Befugnisse nach Art. 58 Abs. 2 DS-GVO auf Verarbeitungsvorgänge.

Art. 58

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass ~~beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen~~, er voraussichtlich gegen diese Verordnung verstoßen wird,

b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er ~~mit Verarbeitungsvorgängen~~ gegen diese Verordnung verstoßen hat,

d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, Maßnahmen oder die Erfüllung von Pflichten gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

## II. Art. 83 Abs. 5 lit. e DS-GVO – Sanktionen, Tatbestand für Verstöße gegen Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 1 lit. a DS-GVO

### 1. Problemaufriss

Gemäß Art. 58 Abs. 1 lit. a DS-GVO kann der Verantwortliche / Auftragsverarbeiter von der Aufsichtsbehörde angewiesen werden, „alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind." Dieser behördliche Auskunftsanspruch verpflichtet den Adressaten, auf Anforderung der Behörde zuzuarbeiten.

Nach Art. 58 Abs. 1 lit. e DS-GVO hat die Aufsichtsbehörde darüber hinaus die Befugnis, „Zugang zu allen personenbezogenen Daten und Informationen zu erhalten, die zur Erfüllung ihrer Aufgabe notwendig sind." Das Zugangsrecht erlaubt der Aufsichtsbehörde, über die bereitgestellten Informationen hinaus in interne Unterlagen, Datenbanken und Verfahren Einsicht zu nehmen (z. B. Ehmann/ Selmayr, Datenschutzgrundverordnung Art. 58 RN 16). Nach dieser Abgrenzung muss die Nichtbereitstellung von Informationen oder die Auskunftsverweigerung des Adressaten unter Art. 58 Abs. 1 lit. a DS-GVO subsumiert werden.

Gemäß Art. 83 Abs. 5 lit. e DS-GVO kann nach dem Wortlaut nur das Nichtbefolgen einer Anweisung nach Art. 58 Abs. 2 DS-GVO oder die Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 DS-GVO mit einem Bußgeld geahndet werden. Demgegenüber können Verstöße gegen die Zusammenarbeitspflichten, z. B. die Auskunftsverweigerung nach Art. 83 Abs. 4 lit. a i. V. m. Art. 31 DS-GVO geahndet werden.

### 2. Bewertung

Diese Verortung der fehlenden Informationsbereitstellung oder der Auskunftsverweigerung ist unter den Aufsichtsbehörden umstritten. Zum einen wird Art. 31 DS-GVO von zumindest einem Teil der Kommentarliteratur so verstanden, dass die Zusammenarbeitsverpflichtung von einer Anfrage der Aufsichtsbehörde ausgelöst wird, welche keine Verwaltungsaktqualität haben muss, also eher in Voruntersuchungen zur Sachverhaltsermittlung stattfindet. Eine solche Sachverhaltsermittlung ist jedoch von einer förmlichen Geltendmachung des behördlichen Auskunftsanspruches nach Art. 58 Abs. 1 lit. a DS-GVO zu unterscheiden und in der Folge sind Verstöße gegen die Verpflichtungen auch unterschiedlich zu ahnden.

Zum anderen wird die Inkonsistenz des Auslegungsergebnisses beklagt, da Art. 83 Abs. 4 lit. a DS-GVO i. V. m. Art. 31 DS-GVO einen erheblich niedrigeren Bußgeldrahmen aufweist, als z. B. die Nichtgewährung des Zuganges nach Art. 83 Abs. 5 lit. e DS-GVO i.V.m. Art. 58 Abs. 1 DS-GVO.

Verstöße gegen Art. 58 Abs. 1 lit. a DS-GVO sollten daher wie die Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 lit. e oder f DS-GVO gleichmäßig geahndet

werden. Daher ist im Rahmen des Art. 83 Abs. 5 lit. e DS-GVO ein Tatbestand für Verstöße gegen eine Anweisung nach Art. 58 Abs. 1 lit. a DS-GVO zu schaffen.

### 3. Änderungsvorschlag

Änderung des Art. 83 Abs. 5 lit. e DS-GVO:

| |
|---|
| Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Abs. 2, Nichtbefolgung einer Anweisung, Informationen bereit zu stellen oder Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 Buchstaben a, e und f. |

## Schwerpunktthema Nr. 6 – Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz

### I. Art. 46 Abs. 4 i. V. m. Art. 64 Abs. 2 DS-GVO

### 1. Problemaufriss

Es wird aus dem Gesetzestext nicht klar deutlich, ob bei jeder Verwaltungsvereinbarung, die als Grundlage für internationalen Datentransfer dienen soll und der zuständigen Aufsichtsbehörde gemäß Art. 46 Abs. 3 lit. b DS-GVO zur Genehmigung vorgelegt wird, ein Kohärenzverfahren durchgeführt werden muss. Art. 46 Abs. 4 DS-GVO sieht dies für alle Fälle des Absatzes 3 vor. Art. 64 Abs. 1 DS-GVO erwähnt in lit. e aber nur die Genehmigung von Vertragsklauseln nach Art. 46 Abs. 3 lit. a DS-GVO.

Hintergrund: Seine Stellungnahme zur ESMA/IOSCO Verwaltungsvereinbarung hat der EDSA gemäß Art. 64 Abs. 2 DS-GVO abgegeben. Ob dieses Verfahren in Zukunft für alle Verwaltungsvereinbarungen oder nur für multilaterale Vereinbarungen Anwendung finden soll, wird in der ITES und der COOPESG streitig diskutiert.

### 2. Bewertung

Es bedarf tatsächlich der Klarstellung, ob auch Verwaltungsvereinbarungen nach Art. 46 Abs. 3 lit. b DS-GVO dem Ausschuss vorgelegt werden müssen. Aus deutscher Sicht ist das der Fall. Allerdings soll hier das Kohärenzverfahren nach Art. 64 Abs. 2 DS-GVO angewendet werden, um dem Ausschuss die Möglichkeit zu geben, bei Verwaltungsvereinbarungen, die nicht die Voraussetzungen des Art. 64 Abs. 2 DS-GVO (Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat) erfüllen, den Antrag auf Stellungnahme abzulehnen.

### 3. Änderungsvorschlag

Neufassung des Artikels 46 Absatz 4 DS-GVO

(4) In Fällen gemäß Absatz 3 Buchstabe a wendet die Aufsichtsbehörde das Kohärenzverfahren nach Art. 64 Abs. 1 Satz 2 Buchstabe e an, in Fällen gemäß Absatz 3 Buchstabe b das Kohärenzverfahren nach Artikel 64 Absatz 2.“

## II. Erfahrungen mit Anwendung und Wirkungsweise der Vorschriften zu Kapitel V und Kapitel VII

### 1. Problemaufriss

Als gemäß Art. 97 DS-GVO gesetztes Thema sind die Erfahrungen mit Anwendung und Wirkungsweise der Vorschriften zu Kapitel V und Kapitel VII zu behandeln. Konkret stellen sich hier u. a. die Fragen, ob längere Fristen erforderlich sind.

### 2. Bewertung

Die in der DS-GVO festgelegten Fristen konnten bisher nicht vollumfänglich in der Praxis getestet werden.

Nichtsdestotrotz wurde bereits bei den Anträgen auf Stellungnahme nach Art. 64 Abs. 2 DS-GVO festgestellt, dass eine sachgerechte Behandlung und Diskussion umfangreicherer Themen und schwieriger Einzelfälle durch die Fristen erschwert wird.

### 3. Änderungsvorschlag

Die Frist des Art. 64 Abs. 3 DS-GVO sollte von acht Wochen auf drei Monate und die Frist des Art. 66 Abs. 4 DS-GVO von zwei auf vier Wochen verlängert werden. Entsprechend müsste dann auch geprüft werden, ob die Geltungsdauer einstweiliger Maßnahmen (Art. 66 Abs. 1 DS-GVO) verlängert wird. Mindestens aber sollte im Kooperations- und Kohärenzverfahren eine Verlängerung aller Fristen um 50 % in Betracht gezogen werden.

## III. Art. 64 Abs. 7 DS-GVO

### 1. Problemaufriss

Die DS-GVO schreibt in Art. 64 Abs. 7 DS-GVO bisher lediglich vor, dass die zuständige Aufsichtsbehörde dem EDSA aufgrund dessen Stellungnahme einen geänderten Beschlussentwurf zur Verfügung stellt (oder mitteilt, dass sie den Beschluss nicht ändern wird). Darauf ist aber keine weitere Rückmeldung des EDSA an die federführende Aufsichtsbehörde mehr vorgesehen.

Zuerst identifiziert wurde dieses Thema im Zusammenhang mit den Kohärenzverfahren zu DSFA-Listen (Art. 64 Abs. 1 lit. a DS-GVO). Vielen Anwendern dieser DSFA-Listen war nicht klar, ob diese nun verbindlichen Charakter haben, nachdem sie gemäß Art. 64 Abs. 7 DS-GVO an die Stellungnahme des EDSA angepasst wurden. Mittlerweile äußert es sich als großes Problem bei Kohärenzverfahren zu BCR (Binding Corporate Rules), da dort auch Externe (die antragstellenden Unternehmen) betroffen sind. Fällt also eine Stellungnahme des EDSA zunächst negativ aus bzw. werden dort Änderungsbedarfe aufgeführt und ändert das Unternehmen daraufhin seine BCR-Unterlagen (Teil des Genehmigungsentwurfs der federführenden Behörde), erhalten federführende Behörde und Unternehmen keine abschließende Rückmeldung mehr, ob damit den Bedenken des EDSA Genüge getan wurde und ob in der Folge der geänderte Beschlussentwurf verbindlich geworden ist.

Dies ist mittlerweile ein erheblicher Diskussionspunkt mit dem EDSA-Sekretariat. Daher wäre hier eine ergänzende Regelung in Art. 64 DS-GVO für einen vollständigen Abschluss von Kohärenzverfahren erforderlich.

**2. Bewertung**

Es scheint in der Tat eine Regelungslücke zu bestehen, welches Verfahren ein geänderter Beschlussentwurf nach sich zieht.

**3. Änderungsvorschlag**

Ergänzung eines zweiten Satzes in Art. 64 Abs. 7 DS-GVO:

| |
|---|
| Der Ausschuss gibt binnen vier Wochen eine Stellungnahme zu dem geänderten Beschlussentwurf ab.<br><br>Äußert sich der Ausschuss nicht binnen vier Wochen, so gilt dies als Zustimmung. |

**Schwerpunktthema Nr. 7 – Direktwerbung**

**1. Problemaufriss**

Mit der DS-GVO sind konkrete Regelungen im nationalen Recht entfallen, die insbesondere Gewichtungen von Interessen vorgesehen haben. Die DS-GVO gibt nur im ErwG 47 DS-GVO einen Anhaltspunkt für die Abwägung: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“ In der Praxis stellen sich Fragen, die mit konkreteren Vorgaben des Gesetzgebers besser lösbar wären, z. B.:

Ist die Weitergabe von Kundendaten an Dritte zu Werbezwecken zulässig?

Ist es zulässig, listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen-, oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken (keine Telefon- und Faxnummern, E-Mail-Adresse, Geburtsdatum) für Werbezwecke vorzuhalten und zu nutzen?

Ist die Werbung für wohltätige Zwecke im Ergebnis anders zu bewerten als für wirtschaftliche Zwecke?

### 2. Bewertung

Direktwerbung betrifft viele Wirtschaftsbereiche und viele betroffene Personen.

Die Traditionen in den Mitgliedstaaten sind unterschiedlich, so dass auch die Erwartungen der Betroffenen, die bei der Interessenabwägung zu berücksichtigen sind, unterschiedlich sein können. Für eine europaweit einheitliche Anwendung sollte der Gesetzgeber deshalb detailliertere Regelungen schaffen.

### 3. Änderungsvorschlag

Für Direktwerbung sollte der europäische Gesetzgeber in der DS-GVO gesetzliche Vorgaben schaffen, die zumindest die grundsätzliche Gewichtung von Interessen vorsehen.

## Schwerpunktthema Nr. 8 – Profiling

### 1. Problemaufriss

Die Bildung von persönlichen Profilen und deren – kommerzielle und politische – Auswertung sind eine der zentralen datenschutzpolitischen Herausforderungen unserer Zeit. Die Werkzeuge der Datenverarbeitung ermöglichen das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten. Verbunden mit immer weiter verfeinerten Möglichkeiten des Einsatzes selbstlernender Mechanismen eröffnet dies vielfältige Möglichkeiten, Verhalten von Einzelnen (vermeintlich) vorherzusagen und ggf. zu steuern. Obwohl diese Entwicklung diverse datenschutzrechtliche Grundprinzipien herausfordert – z. B. das Gebot der Datenminimierung oder die Zweckbindung – bleibt die DS-GVO gerade in diesem Punkt vage und weitgehend auf dem Stand von 1995. Bei den Verhandlungen zur Schaffung der DS-GVO war es nicht gelungen, die Bildung von Profilen und das Scoring einer detaillierten modernen europäischen Regelung zuzuführen.

Die DS-GVO enthält zwar in Art. 4 Nr. 4 DS-GVO eine Definition des Profiling und der Begriff wird in verschiedenen Erwägungsgründen und Artikeln erwähnt (beispielsweise

ErwG 60 DS-GVO, Art. 21, Art. 22, Art. 13 und 14 DS-GVO). Die Profilbildung als solche wird jedoch von den meisten dieser Normen nicht erfasst. Einschränkende Kernregelung ist vielmehr das Verbot der automatisierten Einzelentscheidung mit Erlaubnisvorbehalt (Art. 22 DS-GVO). Das Profiling an sich ist nach geltendem Recht daher vielfach nach den allgemeinen Tatbeständen des Art. 6 DS-GVO zu beurteilen. Beispielsweise wird Profilerstellung auf Grundlage von Internet- Kommunikationsinhalten und Metadaten u. a. für Werbezwecke von den Unternehmen oftmals nicht als automatisierte Entscheidung angesehen, mit der Folge, dass diese Profilbildung nicht vom grundsätzlichen Verbot des Art. 22 DS-GVO umfasst ist.

### 2. Bewertung

Die DSK ist der Auffassung, dass vor dem Hintergrund der dargestellten Probleme Änderungsbedarf an den Regelungen der DS-GVO zum Profiling besteht. Ziel der Neuregelungen sollte eine Verschärfung des geltenden Rechtsrahmens sein, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen. Die betroffenen Personen sollten von einem größeren Maß an Transparenz bezüglich der erstellten Profile profitieren und zugleich eine größere Kontrolle über die Verarbeitung ihrer Daten zur Profilbildung erhalten. Zu diesem Zweck sollte das Verbot der automatisierten Einzelentscheidung in Art. 22 DS-GVO um die Datenverarbeitung zu Zwecken der Profilbildung erweitert werden. Als Rechtsgrundlagen für das Profiling soll – neben einer spezialgesetzlichen Grundlage – allein eine Einwilligung oder ein Vertrag in Betracht kommen. Damit wird sichergestellt, dass ein Profiling nur stattfindet, wenn die betroffene Person sich dessen bewusst ist und damit einverstanden ist.

Die von der Art. 29-Gruppe beschlossenen und vom EDSA bestätigten „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679“ geben zwar wichtige Hilfestellung für die datenschutzrechtliche Einordnung der Profilbildung in der Praxis. Sie können aber eine gesetzliche Regelung nicht ersetzen.

## Schwerpunktthema Nr. 9 – Akkreditierung

### 1. Problemaufriss

In Deutschland gibt es eine Auseinandersetzung zwischen der deutschen nationalen Akkreditierungsstelle und den Aufsichtsbehörden über die Anwendung von Art. 41 DS-GVO. Die deutsche Akkreditierungsstelle vertritt die Auffassung, dass sie auch an Akkreditierungen nach Art. 41 DS-GVO zu beteiligen sei, während die deutschen Aufsichtsbehörden der Auffassung sind, dass die Akkreditierung im Sinne von Art. 41 DS-GVO

ausschließlich von den Aufsichtsbehörden durchzuführen ist. Im Verlaufe der Auseinandersetzung hat die Deutsche Akkreditierungsstelle die Aufsichtsbehörden gebeten, sich für eine Klarstellung des Wortlauts einzusetzen.

### 2. Bewertung

Die deutsche nationale Akkreditierungsstelle schließt aus der Verordnung (EG) Nr. 765/2008, dass sie allgemein für Akkreditierungen in Deutschland zuständig ist. Daher geht sie bisher davon aus, dass auch für die Akkreditierung nach Art. 41 Abs. 1 DS-GVO ein ähnliches Verfahren wie nach Art. 43 Abs. 1 DS-GVO unter Beteiligung der Aufsichtsbehörden durchgeführt wird. Die deutschen Aufsichtsbehörden weisen demgegenüber darauf hin, dass Art. 41 Abs. 1 DS-GVO ausschließlich die Aufsichtsbehörden als akkreditierende Stelle benennt. Der Wortlaut des Art. 43 Abs. 1 Satz 2 DS-GVO unterscheidet sich wesentlich von dem des Art. 41 Abs. 1 DS-GVO. Auch sind im Hinblick auf die Akkreditierung nach Art. 41 Abs. 1 DS-GVO mit Ausnahme von Art. 57 Abs. 1 lit. p DS-GVO (Abfassen und Veröffentlichen der Kriterien) keine konkreten Aussagen in der – im Übrigen im Vergleich zur VO 765/2008 spezielleren – DS-GVO getroffen worden. Nach Auffassung der deutschen Aufsichtsbehörden ist vielmehr davon auszugehen, dass das Wort „Akkreditierung“ in Art. 41 DS-GVO nicht gleichbedeutend mit Akkreditierung im Sinne von Art. 43 DS-GVO und der Verordnung Nr. 765/2008 zu verstehen ist, sondern eine andere Form der „Anerkennung“ darstellt, für die die Verordnung Nr. 765/2008 nicht anwendbar ist.

### 3. Änderungsvorschläge

In Art. 41 Abs. 1 DS-GVO soll zur Klarstellung vor den Worten „von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde“ das Wort „ausschließlich“ eingefügt werden.

Zusätzlich soll rein klarstellend das Wort „akkreditiert“ gestrichen und stattdessen das Wort „anerkannt“ eingesetzt werden.

**Liste weiterer Änderungsvorschläge**

| **Betroffene Vorschrift der DS-GVO** | **Änderungsvorschlag mit Kurzbegründung** |
|---|---|
| Art. 4 | Eine Definition der Anonymisierung fehlt bisher in der DS-GVO. Sie wäre für die Praxis hilfreich. Sie sollte sich an den Vorgaben der „Opinion 05/2014“ zu Anonymisierungsverfahren orientieren. |
| Art. 13, 14 | Die Kataloge der Absätze 2 in Art. 13 und 14 werden aneinander angepasst, indem die Information nach Art. 14 Abs. 2 lit. b DS-GVO auch in Art. 13 DS-GVO nicht in Ansatz 1, sondern in Abs. 2 aufgelistet wird. |
| Art. 18 Abs. 1 | Recht auf Einschränkung der Verarbeitung:<br>Über die unter Art. 18 Abs. 1 lit. a - d DS-GVO aufgezählten Gründe hinaus sollte das Recht auf Einschränkung der Verarbeitung auch in den Fällen bestehen, in denen die an sich gebotene Löschung unterbleibt, weil die Daten gemäß Art. 17 Abs.3 lit. b DS-GVO lediglich zur Einhaltung von Aufbewahrungsfristen vorgehalten werden müssen. |
| Art. 21 Abs. 2 | Widerspruchsrecht bei Direktmarketing:<br>Durch die Einfügung der Worte „neben dem Widerspruchsrecht nach Abs. 1“ sollte klargestellt werden, dass Abs. 2 kein Unterfall von Abs. 1 ist, sondern dass der Anwendungsbereich, anders als bei Abs. 1, auch dann eröffnet ist, wenn die Daten nicht auf der Grundlage von Art. 6 Abs. 1 lit. e und f DS-GVO verarbeitet werden. |
| Art. 24 Abs. 2 | Der Wortlaut von Art. 24 Abs. 2 DS-GVO erscheint missverständlich. Er sollte der englischen Fassung wie folgt angeglichen werden: „Einführung“ statt „Anwendung“ und Datenschutz„regelwerke“ statt Datenschutz„vorkehrungen“. |
| Art. 27 | In Art. 27 DS-GVO sollte eine Pflicht zur Veröffentlichung des Vertreters wie in Art. 37 Abs. 7 DS-GVO (Datenschutzbeauftragter) eingeführt werden, da in vielen Fällen unklar ist, ob der Verantwortliche/Auftragsverarbeiter seiner Bestellpflicht nachgekommen ist und wo der Vertreter seinen Sitz hat. |
| Art. 40 Abs. 4 , Art. 41 Abs.1 u. 4 | Klarstellung durch Änderungen der genannten Regelungen, ob die Einrichtung einer akkreditierten Überwachungsstelle obligatorisch ist (entsprechend der verabschiedeten Leitlinien des EDSA mit Stand vom 12.02.2019) oder nur fakultativ. |

# Anlage zum Beitrag 5.9 – Fragebogen zur Prüfung der Einhaltung datenschutzrechtlicher Vorgaben bei Banken, Versicherungen und Versorgungsunternehmen

| 1 Allgemeine Informationen |
|---|
| Name, Rechtsform, Anschrift Ihres Unternehmens: |
| Ansprechpartner (Name, Funktion, Telefon, E-Mail) |
| Datenschutzbeauftragter (Name, Telefon, E-Mail) |

| 2 Datenschutzorganisation | |
|---|---|
| 2.1 | Welche Unternehmensbereiche sind mit dem Thema Datenschutz betraut? |
| 2.2 | Beschreiben Sie bitte das Zusammenwirken der einzelnen Stellen in datenschutzrechtlichen Angelegenheiten unter Beifügung eines aussagekräftigen Organigramms |
| 2.3 | Sofern es einen Datenschutzbeauftragten gibt, wie und in welcher Häufigkeit berichtet er an die Geschäftsführung? |
| **3 Umsetzung der DS-GVO** | |
| 3.3 | Welche Unternehmensbereiche waren oder sind maßgeblich in die Umsetzung der DS-GVO involviert? |
| 3.4 | Kreuzen Sie bitte die **wesentlichen** Maßnahmen an, die Sie im Rahmen der Umsetzung getroffen haben.<br><br>☐ Sensibilisierungsmaßnahmen<br>☐ interne Datenschutz-Richtlinie<br>☐ Erstellung von Datenschutzhinweisen zur Erfüllung der Informationspflicht<br>☐ Löschkonzept<br>☐ Neuverhandlung Auftragsverarbeitungsverträge<br>☐ Prozess Datenschutz-Folgenabschätzung |

| | |
|---|---|
| | ☐ Anpassung und Erweiterung interner Vorgaben zur Dokumentation<br>☐ Dokumentation der Umsetzung der DS-GVO<br>☐ Überarbeitung/Erstellung von Betriebsvereinbarungen<br>☐ Benennung eines internen bzw. Beauftragung eines externen Datenschutzbeauftragten<br>☐ Prozesse für Betroffenenrechte<br>☐ Prozesse für Beschwerdebearbeitung<br>☐ Prüfung vertraglicher Grundlagen für internationalen Datentransfer<br>☐ Überprüfung/Neuverhandlung der Verträge mit externen Dienstleistern<br>☐ Dokumentation der internen Datenschutzorganisation<br>☐ Prozess für die Meldung von Datenpannen<br>☐ Sonstige: |
| 3.5 | Erläutern Sie bitte kurz den Umsetzungsstatus, falls noch nicht bzw. nicht vollständig umgesetzt. Benennen Sie bitte auch die Gründe. |
| 3.6 | Hat Ihre Internen Revision oder eine vergleichbare Einheit die Einführung und Umsetzung der DS-GVO in Ihrem Unternehmen geprüft? |
| **4 Zulässigkeit der Datenverarbeitung** | |
| 4.1 | Bitte listen Sie die **wesentlichen unternehmensspezifischen** Datenverarbeitungen auf und ordnen Sie diesen die Rechtsgrundlagen zu, auf die Sie die Verarbeitung personenbezogener Daten stützen (Artikel 6, 9 DS-GVO inklusive Spezialnormen). |
| 4.2 | Sofern Sie auf Basis von Einwilligungen personenbezogene Daten verarbeiten, fügen Sie bitte exemplarisch Ihr(e) Muster bei. |
| **5 Beschwerde-Bearbeitung** | |
| 5.1 | Listen Sie bitte die mit der Bearbeitung datenschutzrechtlicher Beschwerden befassten Stellen Ihres Unternehmens auf. |

| | |
|---|---|
| 5.2 | Anhand welcher Kriterien stuft Ihr Unternehmen die Rückmeldung eines Kunden als datenschutzrechtliche Beschwerde ein (Beschwerdedefinition)? |
| 5.3 | Wie unterscheidet sich die Bearbeitung einer datenschutzrechtlichen Beschwerde von der Bearbeitung einer sonstigen Beschwerde? |
| **6 Betroffenenrechte** | |
| 6.1 | Wie stellen Sie sicher, dass den Betroffenenrechten auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Nachberichtspflicht und Datenübertragbarkeit angemessen nachgekommen wird? Bitte kreuzen Sie zutreffendes an.<br><br>☐ Regelungen der Verantwortlichkeiten, Zuständigkeiten und des Kommunikationsverlaufs im Unternehmen<br>☐ Prozesse zur Beantwortung von Anfragen der Betroffenen (einschließlich Erkennen als Anfrage zu einem Betroffenenrecht z. B. durch Schlüsselwörter, Identifikation der Betroffenen, Bearbeitungsdauer, Rückmeldung an Betroffene u.a.)<br>☐ Verwenden von Mustern für Antwortschreiben<br>☐ Prozesse zur Sicherstellung der Einhaltung von Fristen<br>☐ Prozesse zur Nachverfolgung des Fortschritts der Bearbeitung<br>☐ Verfahren zur Reaktion, wenn ein(e) Betroffene(r) mit der Beantwortung nicht zufrieden ist<br>☐ Sensibilisierung der Mitarbeiter |
| 6.2 | Skizzieren Sie bitte überblicksartig Ihre **wesentlichen** Prozesse zu den o.g. Betroffenenrechten. Legen Sie bitte möglichst Nachweise (z.B. Verfahrensbeschreibungen, Mustertexte etc.) bei, die eine Überprüfung Ihrer Angaben ermöglichen. |
| 6.3 | Wie kommen Sie Ihren Informationspflichten gegenüber Kunden gem. Art. 13 bzw. 14 DS-GVO nach (z.B. Homepage, Postversand, E-Mail-Link, Aushang)? Bitte fügen Sie exemplarisch Ihre Muster-Texte bei. |

| | |
|---|---|
| 6.4 | Zu welchem Zeitpunkt informieren Sie Ihre Kunden i.S.v. 6.3? |
| 6.5 | Wie werden Missstände und Schwachstellen im Umgang mit Betroffenenrechten kontinuierlich verbessert und die Verbesserungsmaßnahmen auf ihre Wirksamkeit hin überprüft? |
| **7 Sensibilisierungsmaßnahmen** | |
| 7.1 | Stellen Sie sicher, dass Ihre Mitarbeiterinnen und Mitarbeiter für den Umgang mit personenbezogenen Daten hinreichend sensibilisiert sind?<br>☐Ja<br>☐Nein |
| 7.2 | Benennen Sie, wenn zutreffend, die **wesentlichen** Sensibilisierungsmaßnahmen und machen Sie Angaben zum Ausführungsturnus. |
| **8 Rechenschaftspflicht** | |
| 8.1 | Wie können Sie die Einhaltung der Grundsätze der Datenverarbeitung nachweisen? Benennen Sie die Art der Dokumentation, die Sie für diesen Zweck vorhalten. |
| 8.2 | Welche Aspekte bereiten ggf. Schwierigkeiten? |
| **9 Bereichsspezifische Fragen** | |
| 9.1 | |
| 9.2 | |
| **10 Sonstiges** | |
| Haben Sie Anregungen an die Aufsicht? | |