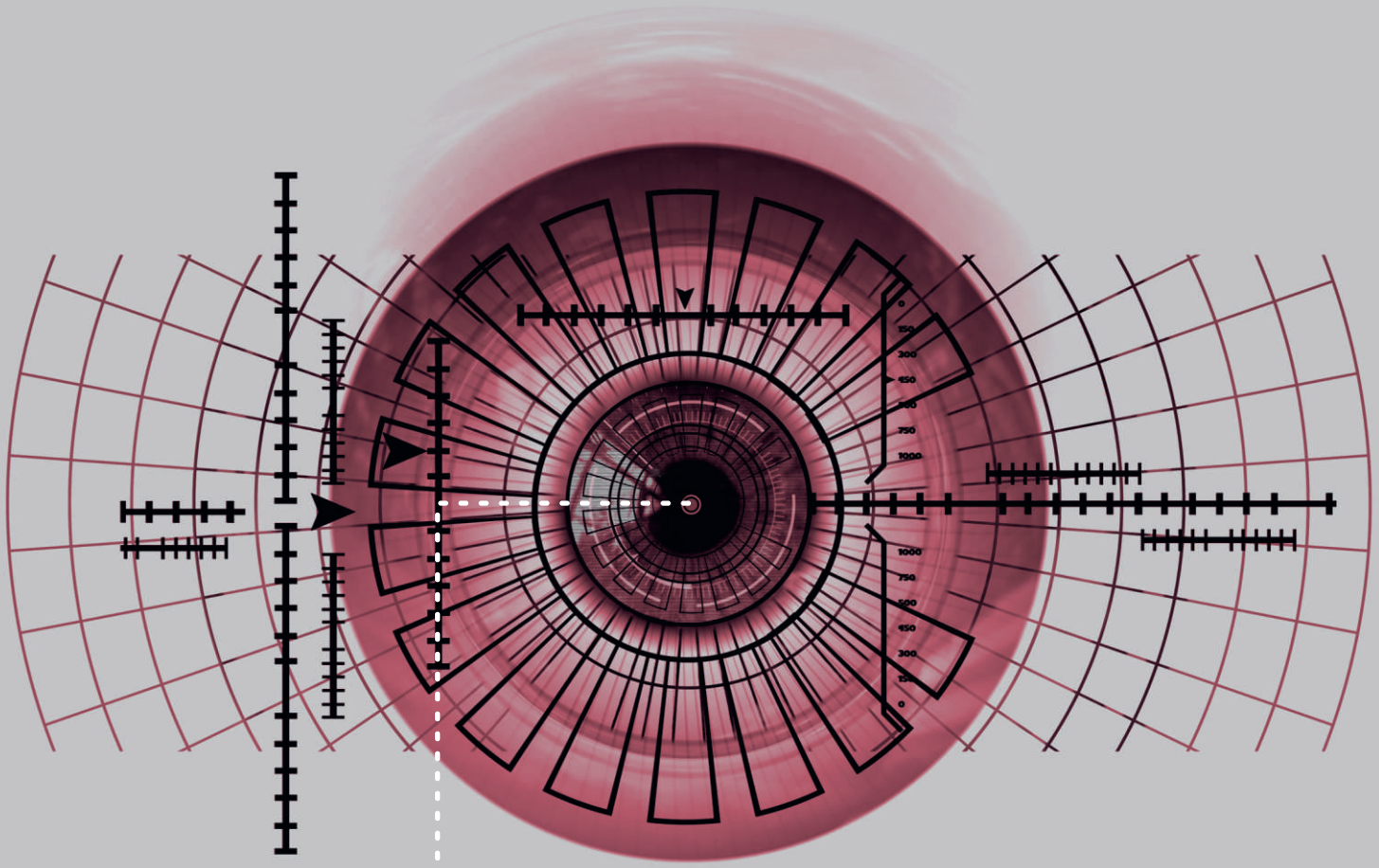


Tätigkeitsbericht 2024

KDSA Ost

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und
des Katholischen Militärbischofs

Herausgeber:

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und des Katholischen Militärbischofs

Badepark 4
39218 Schönebeck
Telefon: 03928 7179018
E-Mail: kontakt@kdsa-ost.de
www.kdsa-ost.de

Wenn ich mir die deutsche Geschichte der letzten hundert Jahre anschaue, weiß ich nicht, ob ich mehr Angst vor Kriminellen haben muss als vor dem Staat..

Ranga Yogeshwar, Moderator, Journalist & Wissenschaftler

9. Tätigkeitsbericht des Diözesandatenschutzbeauftragten

für

das Erzbistum Berlin
das Bistum Dresden-Meißen
das Bistum Erfurt
das Bistum Görlitz
das Bistum Magdeburg
den Katholischen Militärbischof

Berichtszeitraum 01.01.2024 bis 31.12.2024

Inhaltsverzeichnis

Vorwort

Auf dem Digital-Gipfel im Oktober forderte der zuständige Bundesminister für Digitales und Verkehr der Bundesrepublik Deutschland Dr. Volker Wissing auf eine „Digital only Strategie“ umzustellen. Verwaltung und Dienstleister sollen demnach nicht mehr sowohl mit Papier als auch mit Computer arbeiten, sondern nur noch digital. Wirtschaftsminister Robert Habeck sekundiert ein Vorantreiben der Digitalisierung sei notwendig, um die Souveränität Europas zu stärken. Daten würden als Gut auch für die KI-Entwicklung benötigt. Dafür sei es notwendig, dass die deutsche Interpretation des Datenschutzes überdacht werde. Was damit gemeint ist, blieb zunächst offen.

Datenschutz und Digitalisierung dürfen jedoch nicht zu ewigen Antagonisten werden. Vielmehr muss Datenschutz die Digitalisierung begleiten. Nur wenn die Verarbeitung von personenbezogenen Daten für Menschen transparent und nachvollziehbar ist, wird Akzeptanz entstehen.

In unserem ersten Tätigkeitsbericht 2016 hatten wir ausgeführt, dass Datenschutz ursprünglich als ein Abwehrrecht gegen den Staat verstanden worden ist. Wir haben in diesem Zusammenhang die Meinung vertreten, dass im demokratischen System die Ansprüche auf Wahrung des Datenschutzes und der Persönlichkeitsrechte von Bürgern durch die Kontrolle der staatlichen Stellen und nicht zuletzt durch Wahlen beeinflusst werden können. Seinerzeit sind wir davon ausgegangen, dass die größere Gefahr nicht von staatlicher Seite ausgeht, sondern durch die Machtkonzentration, die sich bei wenigen großen Wirtschaftskonzernen angesammelt hat. Als problematisch haben wir damals die freiwillige und umfangreiche Preisgabe von personenbezogenen Daten durch die Nutzer speziell in sozialen Netzwerken betrachtet.

Nun haben sich die gesellschaftlichen Parameter geändert. Demokratische Wahlen sind keine Garantie mehr dafür, dass demokratische Parteien gewählt werden. Radikale Parteien stellen regelmäßig das vermeintliche Volksinteresse vor das Interesse des Einzelnen. Damit ist konsequenter Weise für Persönlichkeitsrechte kein Raum mehr. Für Parteien dieser Denkrichtung wird Datenschutz zum Feind. Gerade deshalb ist es wichtig die Grundsätze des Datenschutzes zu beachten und personenbezogene Daten

nur zu verarbeiten, wenn es für eine legale Zweckerreichung nicht anders möglich ist.

Im Rahmen der Digitalisierung tritt auch der Staat zunehmend als Datensammler auf. Häufig werden personenbezogene Daten erhoben, obwohl sie für die Erfüllung des Zwecks nicht erforderlich sind.

Die Trennung von Staat und Wirtschaft verschwimmt. Dort wo sich der Staat zur Erfüllung seiner Aufgaben privatwirtschaftlicher Anbieter bedient, wird der Abfluss von personenbezogenen Daten an Dritte nicht konsequent unterbunden.

Jedem ist deshalb anzuraten, darauf zu achten, nur personenbezogenen Daten von sich zu offenbaren, wenn dies unbedingt erforderlich und transparent ist, wie und durch wen eine weitere Verarbeitung stattfindet.

Aufgabe des Datenschutzes ist es, Menschen zu schützen, vor staatlichen und wirtschaftlichen Übergriffen auf das Persönlichkeitsrecht. Davor, dass personenbezogene Daten erhoben und verarbeitet werden, die für die Erfüllung des Zwecks nicht erforderlich sind.

Deshalb muss auch in einer Welt des „digital only“ der Datenschutz oberste Priorität behalten.

Das gilt umso mehr in einem Land, in dem eine rechtsextreme Partei Wahlerfolge feiert, obwohl ein Großteil ihrer Landesverbände vom Verfassungsschutz als gesichert rechtsextrem eingestuft wird.

1 Entwicklung des Datenschutzes

1.1 Entwicklung des Datenschutzes in Europa

1.1.1 Neues zum Schadenersatz

Der Europäische Gerichtshof (EuGH) hat in zwei neuen Entscheidungen (beide vom 20.06.2024) klargestellt, dass bei Datenschutzverletzungen ein tatsächlicher Schaden vorliegen muss, um Schadenersatz nach Art. 82 DS-GVO fordern zu können.

1. Fall: Ein Steuerberater verschickte Steuerunterlagen eines Mandanten versehentlich an einen Dritten (AZ: C-590/22)[1]

Die Kanzlei hatte die Steuererklärung der Kläger versehentlich an deren frühere Postadresse gesendet und damit einem anderen Empfänger zugänglich gemacht. Unklar blieb im Verfahren der genaue Inhalt der Sendung und ob der irrtümliche Empfänger tatsächlich Kenntnis von deren Inhalt genommen hatte.

2. Fall: Schadenersatzansprüche gegen den Broker Scalable Capital (AZ: C-182/22)[2]

In einem Verfahren vor dem AG München verklagten zwei Anleger ein Unternehmen einer Trading-App. Die hinterlegten Daten der Anleger (Namen, Geburtsdatum, Postanschrift, E-Mail-Adresse, digitale Kopie des Personalausweises) sowie Daten zum Wertpapier-Depot waren über die App von unbekannten Dritten abgegriffen worden. Die Kläger verlangen einen immateriellen Schadenersatz aufgrund des Diebstahls ihrer persönlichen Daten.

Der EuGH hat Feststellungen vorheriger Entscheidungen bestätigt. Die laut EuGH wesentlichen Aspekte zum Anspruch aus Art. 82 DS-GVO lassen sich wie folgt zusammenfassen:

1 EuGH, Urteil vom 20.06.2024 - C-590/22
2 EuGH, Urteil vom 20.06.2024 - C-182/22

- Der bloße Verstoß gegen die DS-GVO reicht nicht aus, um einen Schadenersatzanspruch zu begründen. Es muss zudem ein Schaden und eine Kausalität zwischen Verstoß und Schaden nachgewiesen werden (AZ: C-590/22).
- Ein immaterieller Schaden hat keine Erheblichkeitsschwelle (AZ: C-590/22; AZ: C-182/22).
- Die Bußgeldvorschriften dürfen bei der Bemessung der Höhe des Schadens nicht angewendet werden (AZ: C-590/22).
- Der datenschutzrechtliche Schadenersatz erfüllt keine Straf- oder Abschreckungsfunktion, sondern lediglich eine Ausgleichsfunktion (AZ: C-590/22; AZ: C-182/22).
- Schwere und möglicher Vorsatz des DS-GVO-Verstoßes dürfen für die Festlegung der Höhe des Schadenersatzes nicht berücksichtigt werden (AZ: C-182/22).

Diese neuen Feststellungen hat der EuGH getroffen:

- Allein die behauptete Befürchtung eines Datenmissbrauchs ohne nachgewiesene negative Folgen führt nicht zu einem Schadenersatz (AZ: C-590/22).
- Verstöße gegen Normen außerhalb der DS-GVO, wie z. B. berufsrechtliche Verstöße des Steuerberaters, dürfen bei der Festlegung der Höhe des Schadenersatzes nicht berücksichtigt werden (AZ: C-590/22).
- Bei fehlender Schwere des Schadens kann ein geringfügiger Schadenersatz zugesprochen werden (AZ: C-182/22).
- Identitätsdiebstahl und Identitätsbetrug sind synonyme Begriffe und sind erfüllt, wenn ein Dritter die Identität einer Person, deren Daten gestohlen wurden, tatsächlich angenommen hat (AZ: C-182/22).
- Allein der Zugang eines unberechtigten Dritten zu personenbezogenen Daten stellt keinen Identitätsdiebstahl oder -betrug dar, kann aber dennoch zu einem Schadenersatz führen (AZ: C-182/22).

Der Diebstahl personenbezogener Daten kann also selbst ohne eine Aneignung der Daten durch einen Dritten zu einem Schadenersatz führen. Die

Befürchtung eines Datenmissbrauchs kann einen immateriellen Schaden darstellen, sofern der Betroffene die negativen Folgen nachweisen kann.

Sofern Datenschutzverstöße auf mangelnde technische und organisatorische Schutzmaßnahmen nach Art. 32 DS-GVO zurückzuführen sind, muss der Verantwortliche, nach Ansicht des EuGHs, die Geeignetheit der technischen und organisatorischen Maßnahmen nachweisen.

Daher sollte hierauf sorgfältig geachtet und alle Maßnahmen genau dokumentiert werden. Auch wenn die Höhe des Schadenersatzes nicht abschreckend und strafend sein darf, sind für Verstöße gegen die DS-GVO hohe Schadenersatzforderungen möglich.

Der EuGH hatte bereits mehrfach entschieden, dass sich Verantwortliche nicht auf Fahrlässigkeit oder Fehlverhalten von Mitarbeitern berufen und somit von der Haftung befreien können. Dies gilt auch für weisungswidriges Handeln der Mitarbeiter. Der Verantwortliche muss sich vergewissern, dass seine Weisungen von seinen Mitarbeitern korrekt ausgeführt werden. Wir empfehlen daher erneut, jährlich eine Datenschutzschulung durchzuführen und das Datenschutzmanagement zu überprüfen.

Weitere Entscheidungen des EuGHs zum Schadensersatz

In seinem Urteil vom 4. Oktober 2024 hat der EuGH[3] noch einmal ganz deutlich entschieden, dass allein der Kontrollverlust über datenschutzwidrig veröffentlichte Daten bereits einen ersatzfähigen Schaden darstellt. Einen Nachweis zusätzlicher konkreter nachteiliger Folgen müssten Betroffene hingegen nicht führen. Bereits mit Urteil vom 11.04.2024 urteilte der EuGH[4], dass bereits der – Verlust der Datenkontrolle – hinsichtlich der personenbezogenen Daten ausreicht, damit ein Schaden nach der DS-GVO vorliegt. Der EuGH führt aus:

- Für einen Anspruch auf Schadenersatz nach der DS-GVO, etwa wegen eines Datenlecks, müssen Betroffene nicht nachweisen, dass ihre Daten tatsächlich illegal weitergegeben wurden bzw. dass ein Datendiebstahl auch tatsächlich zu Identitätsdiebstahl bzw. -betrug geführt hat.

3 EuGH, Urteil vom 04.10.2024 - C-200/23
4 EuGH, Urteil vom 11.04.2024 - C-741/21

- Begründete Befürchtungen, Ängste und Sorgen vor einem solchen Missbrauch reichen aus, um einen Schaden anzunehmen.
- Auch der faktische Kontrollverlust über die eigenen Daten reicht aus, um einen Schaden annehmen zu können.
- Es gibt beim Schadenersatz keine ‚Erheblichkeitsschwelle', der Schaden muss also keine bestimmte Schwere erreichen, um ersatzfähig zu sein.
- Der Begriff des Schadens ist weit zu betrachten, denn die DS-GVO soll die Rechte der Betroffenen ausreichend schützen.

Es bleibt spannend zum DS-GVO-Schadensersatz

Insgesamt hat der EuGH die Voraussetzungen und Rechtsfolgen des datenschutzrechtlichen Schadenersatzanspruchs insbesondere hinsichtlich immaterieller Schäden mit den genannten Urteilen weiter konkretisiert. Es bleibt abzuwarten, wie die nationalen Gerichte mit den Vorgaben des Gerichtshofs umgehen werden.

1.1.2 Fingerabdruckpflicht im Ausweis ist rechtens, Verordnung aber ungültig

Die Verpflichtung zur Aufnahme von zwei Fingerabdrücken im Personalausweis ist mit den Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten vereinbar. Dies hat der EuGH[5] am 21.03.2024 entschieden und folgte damit den Schlussanträgen der Generalanwältin Laila Medina vom 29.06.2023. Zu dem Verfahren hatten wir bereits in unseren Tätigkeitsberichten 2022 Punkt 1.1.2 und 2023 Punkt 1.1.6 berichtet.

Die Fingerabdrücke im Ausweis dienen im weiteren Sinne zur Bekämpfung von Kriminalität und Terrorismus, urteilten die Richter des EUGHs.

Seit mehr als zwei Jahren muss man, wenn man einen neuen Personalausweis beantragt, auf dem Einwohnermeldeamt seine Fingerabdrücke abgeben. Deutschland hat damit eine Verordnung der EU umgesetzt. Die Abdrücke werden nur auf dem Ausweis selbst gespeichert, nicht aber in einer

5 EuGH, Urteil vom 21.03.2024 AZ: C-61/22

zentralen Datenbank. Der EuGH hat jetzt bestätigt, dass diese Speicherung von Fingerabdrücken im Ausweis mit den Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten vereinbar ist.

Geklagt hatte ein Mann aus Wiesbaden. Er hatte einen neuen Personalausweis beantragt, wollte aber nicht, dass seine Fingerabdrücke im Chip des Ausweises gespeichert werden. Eine EU-Verordnung sieht aber genau das vor. Das Verwaltungsgericht Wiesbaden hatte den Fall dem EuGH vorgelegt.

Zwar würden die Grundrechte auf Achtung des Privatlebens und Schutz der personenbezogenen Daten eingeschränkt, dies sei allerdings gerechtfertigt, da damit die Herstellung von gefälschten Ausweisen und Identitätsklau bekämpft werden können, so die Richter. Zudem ermögliche es EU-Bürgern, ihr Recht auf Freizügigkeit in der EU leichter auszuüben.

Der Gerichtshof kam allerdings zu dem Ergebnis, dass die Verpflichtung zur Aufnahme von Fingerabdrücken auf die falsche Rechtsgrundlage gestützt wurde. Nach Ansicht der Richter hätte die Anordnung diese sofort für ungültig zu erklären, schwerwiegende Folgen. Die EU-Gesetzgebung hat daher Zeit bis 2026 für die Änderung.

1.1.3 Aufsichtsbehörden zur Anordnung von Datenlöschung befugt

Der Schutz personenbezogener Daten ist ein grundlegendes Anliegen in der digitalen Ära. Ein Urteil des Europäischen Gerichtshofs[6] hat die Befugnisse einer Aufsichtsbehörde zur Anordnung der Löschung von unrechtmäßig verarbeiteten Daten erweitert. Dieses Recht steht der Aufsichtsbehörde auch dann zu, wenn die betroffene Person selbst keinen Antrag hierfür gestellt hat, wenn dies zur Erfüllung ihrer Aufgabe erforderlich ist, die darin besteht, über die umfassende Einhaltung der DS-GVO zu wachen, so der EuGH.

Die entsprechende Befugnis ergibt sich aus Art. 58 Abs. 2 lit. d) und g) DS-GVO. Anderenfalls könnte der Verantwortliche die Daten unbegrenzt lange

6 EuGH, Urteil vom 14.03.2024 - C-46/23

weiterverarbeiten, obwohl dies rechtswidrig ist und die Aufsichtsbehörde davon Kenntnis hat. Im Übrigen kommt es auch nicht darauf an, ob die Daten unmittelbar bei der betroffenen Person erhoben wurden oder aus einer anderen Quelle stammen.

Der EuGH führt aus:

> *„…Insoweit ist klarzustellen, dass es zwar Sache der Aufsichtsbehörde ist, das geeignete und erforderliche Mittel zu wählen und dabei alle Umstände des Einzelfalls zu berücksichtigen, dass diese Behörde aber gleichwohl verpflichtet ist, mit aller gebotenen Sorgfalt ihre Aufgabe zu erfüllen, die darin besteht, über die umfassende Einhaltung der DSGVO zu wachen (vgl. in diesem Sinne Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn.112).“*

Zur Gewährleistung einer wirksamen Anwendung der DS-GVO ist es daher von besonderer Bedeutung, dass die Aufsichtsbehörde über effektive Befugnisse verfügt, um erfolgreich gegen Verletzungen dieser Verordnung vorzugehen und insbesondere, um solche Verletzungen zu beenden, und zwar auch in den Fällen, in denen die betroffenen Personen nicht über die Verarbeitung ihrer personenbezogenen Daten informiert wurden, ihnen diese nicht bekannt ist oder sie jedenfalls die Löschung dieser Daten nicht beantragt haben, so der EuGH.

Fazit:

Der EuGH stärkt mit diesem Urteil die Befugnisse der Datenschutzbehörden und erhöht damit effektiv auch den Schutz der Bürger. Insbesondere unterstreicht das Urteil auch die Verantwortung der Aufsichtsbehörden, die Einhaltung der DS-GVO zu überwachen und bei Verstößen entsprechend zu handeln.

1.1.4 Exzessive Beschwerden bei Aufsichtsbehörden

Die Datenschutzgrundverordnung (DS-GVO) schützt die Rechte von Betroffenen umfassend, insbesondere durch Auskunftsansprüche und Beschwerderechte. Diese Rechte können aber auch rechtsmissbräuchlich eingesetzt

werden. Der EuGH hatte über die Frage, wann exzessive Beschwerden im Sinne von Art. 57 Abs. 4 DS-GVO vorliegen, zu entscheiden.

Sachverhalt: Ein österreichischer Betroffener rief aufgrund der Nichterfüllung seines Auskunftsrechts nach Art. 15 DS-GVO die Aufsichtsbehörde an. In einem Zeitraum von 20 Monaten reichte er wegen nicht fristgerechter Beantwortung seiner Begehren insgesamt 77 Beschwerden bei der Datenschutzbehörde ein, die sich auf unterschiedliche Verantwortliche bezogen.

Die Behörde verweigerte die Bearbeitung der konkreten Beschwerde, da diese wiederholten Anfragen exzessiv seien. Zu den unzähligen Anfragen kämen auch noch regelmäßige telefonische Beratungsanfragen.

Das österreichische Bundesverwaltungsgericht, an das sich der Betroffene gewandt hatte, gab diesem Recht. Die Behörde habe nicht ausreichend begründet, warum sie die Anfrage als rechtsmissbräuchlich ansah. Neben Häufigkeit müsste für die „exzessive Natur" die Anfragen auch einen „offensichtlich schikanösen bzw. rechtsmissbräuchlichen Charakter" haben, so das Gericht.

Die Datenschutzbehörde legte Revision beim Verwaltungsgerichtshof in Österreich ein. Dieses wandte sich mit einem Vorabentscheidungsersuchen mit verschiedenen Fragen an den EuGH.

Am 09.01.2025 entschied das Gericht[7] wie folgt:

1. Die Frage des Gerichts, ob Art. 57 Abs. 4 DS-GVO so auszulegen ist, dass der enthaltene Begriff „Anfrage" Beschwerden nach Art. 77 DS-GVO umfasst, beantwortete der EuGH mit einem klaren Ja.
2. Beantwortet hat der EuGH zudem die Frage, ob für einen exzessiven Charakter allein eine bestimmte Anzahl an Anfragen in Bezug auf verschiedene Fälle ausreicht oder ob darüber hinaus weitere Kriterien vorliegen müssen, die die Anfragen als rechtsmissbräuchlich darstellen. Hier entschied der EuGH, dass Anfragen nicht allein aufgrund ihrer Anzahl während eines bestimmten Zeitraums als „exzessiv" im Sinne dieser Bestimmung eingestuft werden können, da die Ausübung der in dieser Bestimmung vorgesehenen Befugnis voraussetzt, dass die Aufsichtsbehörde das Vorliegen

7 EuGH, Urteil vom 09.01.2025 - C- 416/23

einer Missbrauchsabsicht der anfragenden Person nachweist. Der Gerichtshof hielt zudem fest, dass für die Verfolgung des Ziels, ein gleichmäßiges und hohes Schutzniveau für natürliche Personen in der EU sicherzustellen und das ordnungsgemäße Funktionieren der Aufsichtsbehörden zu gewährleisten ist.

Dadurch soll erreicht werden, dass die Arbeit der Aufsichten durch offenkundig unbegründete oder exzessive Beschwerden im Sinne von Art. 57 Abs. 4 DS-GVO torpediert wird. Diese Bestimmung gibt den Aufsichtsbehörden somit die Möglichkeit, mit diesen Beschwerden besser umzugehen, indem sie die Belastungen verringern, die diese bei ihnen auslösen können.

3. Art. 57 Abs. 4 DS-GVO entnimmt der EuGH auch, dass eine Aufsichtsbehörde bei tatsächlichem Vorliegen von exzessiven Anfragen durch eine mit Gründen versehene Entscheidung wählen kann, ob sie eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangt oder sich weigert, aufgrund der Anfrage tätig zu werden, wobei sie alle relevanten Umstände berücksichtigen und sich vergewissern muss, dass die gewählte Option geeignet, erforderlich und verhältnismäßig ist.

Fazit:

Das Urteil des EuGHs bringt eine wichtige Klarstellung für die Praxis der Aufsichtsbehörden: Sie müssen bei einer hohen Anzahl an Anfragen sorgfältig abwägen, ob diese gerechtfertigt sind oder missbräuchliches Verhalten darstellen. Die Beweislast für einen „exzessiven Charakter“ liegt dabei bei der Behörde.

1.1.5 Mündliche Datenverarbeitung fällt unter die DS-GVO

Am 7. März 2024 endschied der EuGH[8], dass auch die mündliche Weitergabe von Informationen als personenbezogene Datenverarbeitung zu betrachten und die DS-GVO zu beachten ist (Fall Endemol Shine).

Im Kern des Falles stand der Antrag von Endemol Shine bei einem finnischen Gericht, mündlich Informationen über die verhängten oder bereits

8 EuGH, Urteil vom 07.03.2024 – C 740/22

verbüßten Strafen einer Person zu erhalten, die an einem von Endemol Shine veranstalteten Wettbewerb teilgenommen hatte. Das finnische Gericht wies diesen Antrag auf Auskunft zurück, woraufhin Endemol Shine Berufung einlegte. Das Berufungsgericht bat den EuGH um Klärung der Rechtslage bezüglich der mündlichen Datenverarbeitung.

Die Entscheidung des EuGHs

Der EuGH bestätigte, dass die DS-GVO nicht nur schriftliche oder elektronische Verarbeitung personenbezogener Daten umfasst, sondern auch mündliche Weitergaben. Der Gerichtshof betonte, dass die breite Auslegung des Begriffs „Verarbeitung" dem Ziel der DS-GVO entspricht, ein hohes Datenschutzniveau zu gewährleisten.

Dafür ist es jedoch erforderlich, dass mündliche Verarbeitungen von Daten, hier die mündliche Auskunft, in einem (analogen oder digitalen) Dateisystem gespeichert werden sollen, damit sie eine Verarbeitung personenbezogener Daten sind, und in den Anwendungsbereich der DS-GVO fallen. Im spezifischen Fall von Endemol Shine waren die angeforderten Daten Teil eines Gerichtsregisters, bei dem es sich um ein Dateisystem handelt.

Der EUGH urteilte zudem, dass die Weitergabe sensibler Daten, wie die über strafrechtliche Verurteilungen, an Dritte ohne nachgewiesenes besonderes Interesse gegen die DS-GVO verstößt. Die Entscheidung unterstreicht die Notwendigkeit des Schutzes personenbezogener Daten und der Privatsphäre, insbesondere bei sensiblen Informationen.

Diese Entscheidung verdeutlicht, dass nahezu jede Handhabung personenbezogener Daten als „Verarbeitung" angesehen werden kann und somit der DS-GVO unterliegt, sofern die Daten auch in einem Dateisystem gespeichert oder anderweitig verarbeitet werden sollen. Unternehmen und Organisationen müssen sich bewusst sein, dass Datenschutzverpflichtungen nicht nur für elektronische Datenverarbeitungen gelten, sondern für jegliche Form der Datenverarbeitung, einschließlich mündlicher Übermittlungen.

Fazit:

Für die Praxis bedeutet dies, dass Organisationen ihre Datenschutzrichtlinien überprüfen und sicherstellen sollten, dass sie auch mündliche Da-

tenübertragungen adäquat berücksichtigen. Das Urteil des EuGHs ist ein klares Signal, dass der Schutz personenbezogener Daten eine hohe Priorität in der EU hat. Außerdem zeigt sich deutlich, dass die Datenverarbeitung umfassend interpretiert wird. Dies stärkt das Vertrauen in den Datenschutz und soll die Rechte der Bürgerinnen und Bürger innerhalb der EU weiterhin schützen.

1.1.6 Haften Unternehmen/Kirchliche Rechtsträger für ihre Mitarbeiter

Bußgelder wegen Verstöße gegen die DS-GVO richten sich oft an Unternehmen, die für das rechtswidrige Handeln ihrer Mitarbeiter einstehen müssen. Auch Kirchliche Datenschutzaufsichten nehmen Kirchliche Rechtsträger in die Haftung, wenn Mitarbeiter gegen Bestimmungen des KDG verstoßen.

Kommt es dabei für die Haftung des Unternehmens/des Kirchlichen Rechtsträgers darauf an, ob der Mitarbeiter Führungskraft oder Sachbearbeiter ist? Kann das Unternehmen/der Kirchliche Rechtsträger selbst überhaupt haften? Kommt es auf ein Verschulden an und wenn ja, wie wird das zugerechnet? Fragen über Fragen.

Nach der ständigen Rechtsprechung des Interdiözesanen Datenschutzgerichts (IDSG) haftet eine juristische Person als Verantwortliche für schuldhafte Datenschutzverstöße ihrer Beschäftigten, auch wenn diese keine Organstellung -etwa als Geschäftsführer einer GmbH- oder sonstige Führungsposition innehat.[9] Verantwortliche ist gem. § 4 Nr. 9 KDG die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Auch die deutschen Datenschutzaufsichtsbehörden (Konferenz der Deutschen Datenschutzaufsichten -DSK-) gehen davon aus, dass Unternehmen für Datenschutzverstöße eines jeden Mitarbeiters haften, unabhängig davon, welche Funktion dieser im Unternehmen hat.[10] Es komme auch nicht darauf an, ob die Unternehmensleitung Kenntnis von einem Verstoß habe

9 IDSG, Beschluss vom 27. September 2021 - IDSG 08/2021
10 DSK-Entschließung Nr. 97 vom 03.04.2019

oder ob eine Verletzung der Aufsichtspflicht vorliege, so die DSK. Ist ein Datenschutzverstoß unstrittig und objektiv festgestellt, sollen Aufsichtsbehörden nicht einmal ermitteln müssen, welcher konkrete Mitarbeiter gehandelt habe.

Dieses Haftungsverständnis geht vom sog. „funktionalen Unternehmensbegriff" des europäischen Primärrechts (Art. 101, 102 AEUV) und der europäischen Rechtshistorie aus.

Entscheidung des Europäische Gerichtshofs (EuGH)

Der EUGH hat am 05.12.2023[11] ein wegweisendes Grundsatzurteil zu den Voraussetzungen für die Verhängung von (verwaltungsrechtlichen) Geldbußen bei DS-GVO-Verstößen gefällt.

Worum ging es (Kurzfassung)?

Der EuGH hat mit Urteil vom 05.12.2023[12] die Vorlagefragen des Kammergerichts Berlin (KG) in Bezug auf das im Oktober 2019 durch die Berliner Aufsichtsbehörde verhängte Bußgeld i. H. v. 14,5 Millionen Euro gegen die Deutsche Wohnen SE beantwortet.

Zentral ging es dabei um den Rahmen für die datenschutzrechtliche Haftung des Verantwortlichen. Fraglich war bis dato, ob ein Verschulden des Verantwortlichen Voraussetzung für die Haftung nach der DS-GVO ist. Dies wurde nun durch den EuGH bestätigt.

1. Geldbußen sind unmittelbar gegen juristische Personen möglich

Der EuGH entschied, dass Datenschutzaufsichtsbehörden bei DS-GVO-Verstößen Geldbußen direkt gegen juristische Personen verhängen dürfen. Der Verstoß muss nicht zuvor einer identifizierten natürlichen Person zugerechnet werden. Der EuGH stellt sich damit hinter das von deutschen Gerichten bereits praktizierte „Funktionsträgerprinzip".

2. Verstoß durch untergeordnete Mitarbeiter genügt

Nach der von dem EuGH vertretenen Auffassung können gegen Unternehmen Bußgelder auch verhängt werden, wenn die Verstöße von irgendeiner Person begangen werden, die im Rahmen der Geschäftstätigkeit des

11 EuGH, Urteil vom 05.12.2023 - C-807/21
12 EuGH, Urteil vom 05.12.2023 - C-807/21

Unternehmens und für dessen Rechnung handelt. Es muss also lediglich feststehen, dass irgendein Mitarbeiter einen Verstoß gegen die DS-GVO begangen hat. Dieser Mitarbeiter muss auch nicht näher bestimmt werden.

3. Unternehmen muss aber schuldhaft gehandelt haben

Die Verhängung einer Geldbuße setzt aber voraus, dass das Unternehmen den Verstoß gegen die DS-GVO vorsätzlich oder zumindest fahrlässig begangen hat. Das bedeutet, dass Geldbußen gegen Unternehmen nicht verschuldensunabhängig verhängt werden können.

Erforderlich bleibt also der Nachweis, dass der vermeintliche Datenschutzverstoß vorsätzlich oder fahrlässig begangen wurde. Allerdings soll es für ein Verschulden ausreichen, wenn sich der Verantwortliche über die Rechtswidrigkeit seines Verhaltens „nicht im Unklaren sein konnte". Dabei ist es egal, ob ihm dabei bewusst war, dass sein Verhalten gegen die Vorschriften der DS-GVO verstößt. Für eine Geldbuße gegen eine juristische Person soll jetzt „keine Handlung" und nicht einmal die „Kenntnis seitens des Managements" erforderlich sein.

Ergebnis: Die Verhängung von Bußgeldern gegen juristische Personen (z.B. Unternehmen) und auch gegen Kirchliche Rechtsträger setzt nach der Entscheidung des EuGH Folgendes voraus:

1. Das Unternehmen bzw. der Kirchliche Rechtsträger ist eine juristische Person und Verantwortlicher gem. Art. 4 Nr. 7 DS-GVO bzw. § 4 Nr. 9 KDG.
2. Es steht fest, dass irgendein Mitarbeiter des Verantwortlichen einen bußgeldfähigen Verstoß gegen die DS-GVO bzw. gegen das KDG begangen hat.
3. Den Verantwortlichen trifft nachweislich ein Verschulden (Vorsatz oder Fahrlässigkeit).

Liegen diese Voraussetzungen vor, dürfen Bußgelder direkt gegen das Unternehmen/ den Kirchlichen Rechtsträger nach § 3 Abs. 1 lit. c) KDG als juristische Person verhängt werden, die als Verantwortlicher i. S. d. DS-GVO/ des KDG zu qualifizieren sind.

Wann haften Unternehmen dennoch nicht für Verstöße ihrer Mitarbeiter?

Nicht entschieden wurde, wann eine Haftung dennoch ausscheidet. Nach derzeitiger Auffassung soll ein Unternehmen lediglich bei einem sog. „Mitarbeiterexzess" nicht haften. Darunter versteht man ein bewusstes Fehlverhalten des Mitarbeiters, das nicht dem unternehmerischen Aufgaben- und Tätigkeitsbereich zuzurechnen ist.

Das ist z. B. der Fall, wenn sich ein Beschäftigter nicht an die vom Verantwortlichen des Unternehmens festgelegten Verfahren hält und auf eigene Initiative unrechtmäßig die Daten von Kunden oder anderen Beschäftigten verarbeitet. Dies sind also jene Fälle, in denen Mitarbeiter eigenmächtig und außerhalb ihrer vertraglich festgelegten Tätigkeiten Datenschutzverstöße begehen.

Fazit:

Das EuGH-Urteil schafft Klarheit bezüglich der Haftung von Verantwortlichen bei Datenschutzverstößen. Für Unternehmen/Kirchliche Rechtsträger hat das Urteil zur Folge, dass sie sich nicht darauf berufen können, dass Bußgelder nicht gegen sie als juristischen Personen verhängt werden können. Das Urteil verdeutlicht aus unserer Sicht noch einmal mehr, dass Verantwortliche daher weiterhin konsequent darauf achten und sicherstellen sollten, dass Datenschutzvorgaben in der gesamten Organisation operativ umgesetzt und beachtet werden. Mitarbeiter sollten regelmäßig sensibilisiert werden, um einem Datenschutzbußgeld entgehen zu können. Die bisherige Rechtsauffassung des IDSG und auch die Ansicht der DSK wird durch diese Entscheidung des EuGHs bestätigt.

1.1.7 Einheitliche Regeln für Künstliche Intelligenz in der EU

Ein Meilenstein in der Entwicklung des Datenschutzes sollte die KI-Verordnung (AI-Act) werden, die von der EU verabschiedet worden ist, um Grundlagen für eine Regulierung von Künstlicher Intelligenz zu schaffen. Es zielt darauf ab, ein sicheres und vertrauenswürdiges Umfeld für die Entwicklung und den Einsatz von KI-Technologien zu schaffen. Grundprinzipien wie Transpa-

renz, Sicherheit und die Wahrung der Grundrechte wären entscheidend, um das Vertrauen der Bürger in KI-Systeme zu stärken.

Ein positiver Aspekt der Verordnung ist zunächst die Risikokategorisierung von KI-Anwendungen. Durch die Einstufung in verschiedene Risikostufen besteht die Möglichkeit, angemessene Maßnahmen zu ergreifen, um potenzielle Gefahren zu minimieren. Insgesamt ist der AI-Act grundsätzlich ein wichtiger Schritt, um die Chancen und Herausforderungen der Künstlichen Intelligenz verantwortungsvoll zu gestalten. Jedoch gibt es aus datenschutzrechtlicher Sicht auch Kritik:

So benötigen KI-Systeme oft große Mengen an Daten, um effektiv zu funktionieren. Dies kann zu einer übermäßigen Verarbeitung personenbezogener Daten führen, was im Widerspruch zu den Prinzipien der Datenschutz-Grundverordnung (DS-GVO) steht. Dabei besteht die Gefahr, dass die Rechte der Nutzer nicht ausreichend geschützt werden.

Auch im Hinblick auf Transparenz, z. B. wie Daten verwendet werden, dürfte es aufgrund der Komplexität von KI-Systemen schwierig sein, die Datenverarbeitung nachzuvollziehen. Eine Gefährdung der Privatsphäre der Nutzer besteht darin, dass Unternehmen Daten in einem Umfang verarbeiten, der über das hinausgeht, was für die Erbringung ihrer Dienstleistungen notwendig ist. Außerdem besteht in der Möglichkeit, Daten aus verschiedenen Quellen zu kombinieren, das Risiko zu einer noch umfassenderen Überwachung und Erstellung eines Persönlichkeitsprofils von Individuen. Dies wirft ernsthafte Fragen hinsichtlich des Datenschutzes und der informierten Einwilligung auf.

Die KI-Verordnung der EU kann deshalb einige potenzielle Gefahren für die Persönlichkeitsrechte von Individuen nicht verhindern. Datenschutz darf deshalb nicht nur als nachgelagertes Thema behandelt werden, sondern ist von Anfang an in die Entwicklung und Implementierung von KI-Systemen zu integrieren. Ein ausgewogenes Verhältnis zwischen Innovation und dem Schutz der Privatsphäre der Nutzer ist entscheidend, um das Vertrauen in KI-Technologien zu fördern.

1.2 Entwicklung des Datenschutzes in Deutschland

1.2.1 DSK veröffentlicht Orientierungshilfe zur Künstlichen Intelligenz

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 06. Mai 2024 die Orientierungshilfe Künstliche Intelligenz (KI) und Datenschutz[13] veröffentlicht.

Die Orientierungshilfe dient als Leitfaden, um KI-Anwendungen hinsichtlich der datenschutzrechtlichen Erfordernisse auswählen zu können. Bei der Verarbeitung personenbezogener Daten mit KI-Anwendungen bzw. durch KI-Systeme ist genauso wie für Verarbeitungen ohne KI eine Rechtsgrundlage erforderlich. Im Weiteren dürfen Entscheidungen mit rechtlicher Wirkung für eine betroffene Person nicht von der KI-Anwendung, sondern nur von einem Menschen getroffen werden (Art. 22 Abs. 1 DS-GVO / § 24 Abs. 1 KDG). Ergebnisse der KI sollten auf ihre Rechtmäßigkeit überprüft werden. Wird die Rechtmäßigkeit nicht erfüllt (z.B. diskriminierendes Ergebnis), so sollte das von der KI generierte Ergebnis nicht verwendet werden. Weiterhin ist zu prüfen, ob bei der Verwendung von Ergebnissen eine Kennzeichnung als KI-generierte Inhalte notwendig ist, um beispielsweise Urheberrechtsverletzungen zu vermeiden.

Falls sich KI-Systeme in Drittstaaten befinden und dorthin eine Datenübermittlung erfolgt, müssen die entsprechenden Regularien zur Drittstaatenübermittlung beachtet werden (Art. 44 ff DS-GVO / § 39 ff KDG).

Durch den Einsatz zusätzlicher Systeme, mit denen auch personenbezogene Daten verarbeitet werden, sind u.U. Datenschutzhandbücher, Verfahren und Prozesse anzupassen. Davon betroffen wären z.B. Informationspflichten und Hinweise auf die Rechte der betroffenen Person, der Prozess bei Auskunftsersuchen oder das Löschen von Daten.

Die Orientierungshilfe gibt u.a. auch Hinweise, welche datenschutzrechtlichen Konstellationen es bei der Verantwortlichkeit geben kann. Je nach

13 DSK, https://www.datenschutzkonferen online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf, zuletzt aufgerufen am 22.01.2025

Anwendungsfall muss ein Vertrag zur Auftragsdatenverarbeitung oder eine Vereinbarung zur gemeinsamen Verantwortlichkeit getroffen werden.

Vor einem Einsatz sollten Organisationen und Einrichtungen Regelungen treffen, wie verfügbare KI-Systeme/-Anwendungen einzusetzen sind. Dabei kann sich eine Risikoeinschätzung bzw. eine DSFA (Datenschutz-Folgenabschätzung) als hilfreich erweisen. In der Orientierungshilfe wird eine Dienstvereinbarung mit dem Betriebsrat (Mitarbeitervertretung) empfohlen.

1.2.2 Exzessive Auskunftsverlangen

Das Amtsgericht Arnsberg (AG) hat mit Beschluss vom 31.07.2024[14] ein Vorabentscheidungsersuchen beim EuGH eingereicht. Konkret geht es hier um die Frage, wann Anfragen (Auskunftsersuchen) verweigert werden können, wenn diese im Rahmen eines Geschäftsmodells (Schadensersatzforderung) missbraucht werden und wann ein solches vorliegt.

Im vorliegenden Fall abonnierte der Betroffene online einen Newsletter und forderte im Anschluss Auskunft über die von der Betreiberin verarbeiteten Daten gemäß Art. 15 DS-GVO. Mit der Empfangsbestätigung erklärte die Betreiberin die Anfrage innerhalb eines Monats beantworten zu wollen. Schlussendlich gab die Betreiberin allerdings dem Auskunftsbegehren nicht statt, und begründete dies damit, es handele sich um eine rechtsmissbräuchliche Anfrage i.S.v. Art. 12 Abs. 5 S. 2 lit. b) DS-GVO. Zu dem Schluss der Rechtsmissbräuchlichkeit kam die Betreiberin, da sie durch Berichte verschiedener Onlinemedien herausgefunden hatte, dass der Beklagte datenschutzrechtliche Auskunftsanfragen systematisch und rechtsmissbräuchlich ausnutze, um anschließend Schadensersatzforderungen zu stellen. Gegen die Ablehnung des Auskunftsersuchens klagte der Betroffene vor dem AG Arnsberg.

Das AG möchte vom EuGH wissen welche Voraussetzungen vorliegen müssen, unter denen ein Auskunftsverlangen als rechtsmissbräuchlich abgelehnt werden kann. Nach Art. 12 Abs. 5 S. 2 DS-GVO kann sich der Verantwortliche bei „exzessiven Anträgen“ weigern, tätig zu werden. Dem

14 AG Arnsberg, Beschluss vom 31.07.2024 - 4 C 434/23

AG ist dabei unklar, ob dafür auch schon eine erstmalige Anfrage bei dem Verantwortlichen ausreicht und ob eine Auskunft verweigert werden kann, wenn mit der DS-GVO-Anfrage Schadenersatzansprüche provoziert werden sollen. Es sei auch fraglich, ob sich ein Weigerungsrecht auf öffentliche Informationen über das Verhalten des Anfragenden stützen lasse.

Der EuGH soll zudem die Frage klären, ob sich (allein) aus einer Verletzung des Auskunftsrechts auch ein Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO ergeben kann und ob für einen solchen Anspruch eine Verarbeitung von personenbezogenen Daten erforderlich ist.

Des Weiteren soll auch die Frage geklärt werden, ob öffentlich zugängliche Informationen ausreichen, um diese Rechtsmissbräuchlichkeit zu belegen.

Bisherige Rechtsprechung

In der Vergangenheit haben sich bereits verschiedene deutsche Gerichte mit den Voraussetzungen des Rechtsmissbrauchs bei DS-GVO-Anfragen beschäftigt. So haben etwa das Oberlandesgericht (OLG) Hamm,[15] das OLG Brandenburg[16] und das OLG Nürnberg[17] entschieden, dass ein Auskunftsbegehren dann als missbräuchlich zu werten ist, wenn es nicht zur Prüfung der datenschutzkonformen Datenverarbeitung erfolgt.

Unabhängig davon bleibt auch fraglich, ob das Begehren auf immateriellen Schadensersatz Erfolg haben wird. Der EuGH hat nämlich mittlerweile vermehrt entschieden, dass zwar keine „Erheblichkeitsschwelle" für immateriellen Schaden überschritten werden muss, der Betroffene jedoch den Schaden nachweisen muss (vgl. Pkt. 1.1.1 in diesem Bericht).

Fazit:

Insofern bleibt es für die Voraussetzungen der Auskunftsverweigerung bei exzessiven DS-GVO-Anträgen spannend, wie das Urteil des EuGHs ausfallen wird (bis zum Redaktionsschluss war noch keine Entscheidung ergangen). Unabhängig davon sollten Unternehmen ihre internen Prozesse/Abläufe so anpassen, dass sie bei Auskunftserteilungen keine Verstöße gegen Datenschutzvorschriften begehen. Der Betroffene, auch wenn er

15 OLG Hamm, Urteil vom 20.05.2023 - 20 U 146/22
16 OLG Brandenburg, Urteil vom 14.04.2023 - 11/U 233/22
17 OLG Nürnberg, Urteil vom 14.03.2022 - 8 U/2907/21

rechtsmissbräuchliche Ziele verfolgt, kann dann keine Schadensersatzansprüche geltend machen.

1.2.3 Neues zum Auskunftsrecht

BGH definiert „Umfang von Kopien personenbezogener Daten“

Der Umfang des datenschutzrechtlichen Auskunftsanspruch und der Anspruch auf eine Kopie der personenbezogenen Daten gem. Art. 15 DS-GVO war lange Zeit umstritten.

Nachdem der Europäische Gerichtshof[18] Mitte 2023 das datenschutzrechtliche Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO umfassend erläuterte und Fragen zu Inhalt und Umfang des Betroffenenrechts klärte, hat der Bundesgerichtshof (BGH) in einem wegweisenden Urteil vom 05.03.2024[19] klargestellt, wie der **Begriff „Kopie von personenbezogenen Daten“** zu verstehen ist.

Vorab hatte der BGH das Verfahren ausgesetzt[20], um die Entscheidung des EuGHs abzuwarten.

Der Bundesgerichtshof (BGH) hat mit Urteil vom 05.03.2024 klargestellt, dass der Anspruch auf „Kopien“ im Sinne von Art. 15 Abs. 3 DS-GVO nicht die vollständigen Unterlagen mit Bezug auf die betroffene Person meint. Der Anspruch beziehe sich lediglich auf die personenbezogenen Daten selbst, nicht auf die Dokumente, in denen sie enthalten sind. Der Betroffene kann zwar vollständige Kopien solcher – noch vorhandener – Unterlagen verlangen, die von ihm selbst erstellt und an den Auskunftsverpflichteten übermittelt wurden, z. B. eigene E-Mails oder Briefe. Ein Anspruch auf vollständige Herausgabe beispielsweise von Aktenvermerken, Telefonnotizen oder Beratungsprotokollen besteht dagegen in der Regel nicht.

Das Urteil des BGH erging im Rahmen der Klage einer Anlegerin, die auf der Grundlage von Art. 15 Abs. 3 S. 1 DS-GVO von der Vermittlerin einer Kapitalanlage verlangt hatte, ihr Kopien sämtlicher sie betreffender Unterlagen aus der langjährigen Geschäftsbeziehung zu übermitteln. Das Kla-

18 EuGH, Urteil vom 04.05.2023 – C-487/21
19 BGH, Urteil vom 05.03.2024 - VI ZR 330/21
20 BGH, Beschluss vom 21.02.2023 - VI ZR 330/21

gebegehren diente unstreitig dazu, der Klägerin den Zugriff auf mögliche Beweismittel für das von ihr parallel geführte Schadenersatzverfahren zu ermöglichen. Während das Schadenersatzbegehren in allen Instanzen erfolglos blieb, hatte das Auskunftsverlangen in den ersten beiden Instanzen weitgehend Erfolg.

Der BGH legt zunächst noch einmal dar, dass Art. 15 DS-GVO der betroffenen Person ein Auskunftsrecht über die Verarbeitung personenbezogener Daten gibt. Der Begriff „personenbezogene Daten" umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur, unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt. Die letztgenannte Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist.

Unter Berücksichtigung dessen bewertet der BGH die Schreiben der betroffenen Person (verfasste Briefe und E-Mails) an den Verantwortlichen ihrem gesamten Inhalt nach als personenbezogene Daten.

Begründung des BGH: Die personenbezogenen Informationen bestehen bereits darin, dass die betroffene Person sich dem Schreiben gemäß geäußert hat, umgekehrt aber Schreiben des Verantwortlichen an die betroffene Person nur insoweit, als sie Informationen über die betroffene Person nach den oben genannten Kriterien enthalten, so der BGH. Dabei sei es unerheblich, dass diese Schreiben der betroffenen Person bereits bekannt sind.

Demgegenüber seien weder Schreiben und E-Mails, noch Telefonnotizen, Aktenvermerke oder Gesprächsprotokolle des Verantwortlichen oder Zeichnungsunterlagen für Kapitalanlagen zwangsläufig in ihrer Gesamtheit personenbezogene Daten der betroffenen Person, auch wenn diese Dokumente Informationen über die betroffene Person enthalten.

Denkbar ist bei diesen Dokumenten zwar, dass diese ausschließlich Informationen über die betroffene Person enthalten. Das kann und muss aber nicht immer der Fall sein.

Daher entfällt grundsätzlich der Anspruch auf entsprechende Kopien. Etwas anderes gilt nur dann, wenn diese Dokumente erforderlich sind, damit die betroffene Person den Gesamtzusammenhang der Datenverarbeitung

nachvollziehen und ihre Betroffenenrechte effektiv ausüben kann. Diese Gründe muss die betroffene Person jedoch mit überzeugender Begründung vortragen, es sei denn, die Notwendigkeit ist allgemein ersichtlich.

Fazit:

Das Urteil des BGH bringt dringend benötigte Klarheit bezüglich des Umfangs auf Kopie der personenbezogenen Daten. Hiernach gilt nun, dass der Anspruch jedenfalls bei vom Anspruchsinhaber erstellten Dokumenten besteht. Bei internen vom Verantwortlichen erstellten Unterlagen ist dies hingegen nicht zwangsläufig der Fall.

1.2.4 Schadensersatz wegen verspäteter Auskunft

Nach § 17 Abs. 1 KDG hat jede betroffene Person zunächst das Recht, von dem Verantwortlichen eine Auskunft darüber zu bekommen, ob sie betreffende personenbezogene Daten verarbeitet werden. Darüber hinaus besteht ein weiterer Anspruch auf die Informationen, die in dieser Vorschrift benannt sind, wenn tatsächlich personenbezogene Daten verarbeitet werden. Die Parallelvorschrift im staatlichen Recht findet sich in Art. 15 DS-GVO.

Datenschutzrechtliche Auskunftsansprüche zählen zu den wichtigsten Ansprüchen des Datenschutzrechtes für Betroffene. Gleichzeitig sind sie auch häufig Gegenstand gerichtlicher Auseinandersetzungen.

Die Frist innerhalb derer solche Ansprüche zu beauskunften sind, ist kurz. Sie wird in § 14 Abs. 3 Satz 1 KDG benannt. Danach sind die geforderten Informationen „unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags“ zur Verfügung zu stellen. Der Begriff unverzüglich ist definiert, als „ohne schuldhaftes Zögern“. Damit bedeutet „unverzüglich“ weder „sofort“ noch ist damit eine starre Zeitvorgabe verbunden. Nach einer Zeitspanne von mehr als einer Woche ist aber ohne das Vorliegen besonderer Umstände grundsätzlich keine Unverzüglichkeit mehr gegeben.[21] Das bedeutet aber auch, dass bei einfachen Vorgängen, wie der Erteilung einer Negativauskunft, eine Auskunftserteilung nach Ablauf einer Woche nicht mehr fristgemäß im Sinne von § 14 Abs. 1 Satz 1 KDG ist.

21 BAG, Urteil vom 27.02.2020 – 2 AZR 390/19

So sah es auch das Arbeitsgericht Duisburg[22] in einem Fall, in dem ein Bewerber sechs Jahre nach seiner Bewerbung bei dem verantwortlichen Unternehmen einen Auskunftsanspruch gestellt hatte. Dem Verantwortlichen lagen keine personenbezogenen Daten des Bewerbers mehr vor, da er diese bereits gelöscht hatte. Obwohl der Verantwortliche die Auskunft nach 19 Tagen -also weit vor Ablauf eines Monats- erteilt hatte, erkannte das Gericht eine Datenschutzverletzung, weil der Auskunftsanspruch nicht „unverzüglich" erteilt worden ist. Der Kläger erhielt dafür einen Ersatz für seinen immateriellen Schaden in Höhe von 750,00 € zugesprochen. Dieser bestünde in Form des Kontrollverlusts des Klägers über seine Daten. Der Kläger habe sich im Ungewissen darüber befunden, ob und wie die Beklagte seine personenbezogenen Daten verarbeitet habe. Eine Prüfung dessen sei ihm verwehrt gewesen.

Fazit:

Eine pauschale und verlässliche Aussage darüber, innerhalb welcher Frist aus Sicht nationaler und europäischer Gerichte auf ein Auskunftsersuchen regiert werden muss, ist gegenwärtig nicht möglich. Nationale Gerichte handhaben die unter Umständen verlängerbare Monatsfrist des Art. 12 Abs. 3 DS-GVO (entspricht § 14 Abs. 3 KDG) mitunter restriktiv.

Die Auslegung des Tatbestandsmerkmals „unverzüglich" sollte im Anwendungsbereich der DS-GVO/KDG unter Berücksichtigung aller Umstände einzelfallbezogen sein. Hilfreich wäre eine Auslegung des Begriffs „unverzüglich" durch den EuGH.

Aufsichtsbehörden können empfindliche Bußgelder aufgrund von Verstößen gegen die DS-GVO/das KDG verhängen. Es ist somit im Interesse jedes Verantwortlichen, rechtzeitig auf Anträge betroffener Personen zu reagieren.

1.2.5 Immaterieller Schadensersatz bei Datenschutzverletzungen

Der Bundesgerichtshof (BGH) hat eine Leitentscheidung zum „Facebook-Datenleck" gefällt[23] und entschieden, dass Facebook-Nutzer nach einem

22 ArbG Duisburg, Urteil vom 03.11.2023 – 5 Ca 877/23
23 BGH, Urteil vom 18.11.2024 - VI ZR 10/24

Datenleck allein aufgrund des Kontrollverlustes über ihre Daten einen Anspruch auf immateriellen Schadensersatz geltend machen können. Im Rahmen der Schadensersatzansprüche nach einem umfangreichen Datendiebstahl bei Facebook hat der BGH die Rechte der betroffenen Nutzer gestärkt. Die Karlsruher Richter entschieden, dass der bloße Verlust der Kontrolle über die eigenen Daten für einen Anspruch auf immateriellen Schadensersatz ausreichend sein kann.

Mit diesem Urteil hat der BGH im ersten Leitentscheidungsverfahren eine maßgebliche Entscheidung für tausende ähnlich gelagerte Fälle getroffen.

Aufgrund der Einstellungen der Konzernmutter Meta innerhalb der Sucheinstellung des Netzwerks konnten potenziell alle Nutzer gefunden erden, was wohl dem Grundsatz der Datenminimierung widersprechen dürfte.
Der BGH entschied zudem, dass auch der bloße Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden i. S. d. Art. 82 Abs. 1 DS-GVO darstellt. Es sei nicht erforderlich, dass die Daten missbräuchlich verwendet wurden oder dass es zusätzliche spürbare negative Folgen, wie etwa Angst oder Sorge vor Kontrollverlust für die Betroffenen gebe. Es genügt der Nachweis, Opfer des Vorfalls gewesen zu sein, um Schadensersatz zu verlangen. Der Senat vertritt die Ansicht, dass der Schadensersatz beim bloßen Kontrollverlust nicht allzu hoch ausfallen könne, ein Betrag von 100 Euro sei angemessen.

Insgesamt bewegt sich der BGH mit seinem Urteil auf der Linie des EuGH [24], der zuletzt insbesondere feststellte, dass die Geltendmachung eines Anspruchs aus Art. 82 DS-GVO nicht die Überschreitung einer Erheblichkeitsschwelle voraussetzt, gleichzeitig jedoch der Anspruch ausschließlich zur Kompensation des erlittenen Schadens und nicht zur Genugtuung oder zu Strafzwecken dient.

Wichtig: Angemessene TOMs

Die Umsetzung von geeigneten technischen und organisatorischen Maßnahmen ist unerlässlich, um Risiken wie Verlust, unbefugtem Zugriff oder Missbrauch der Daten zu minimieren. Es sind nach Art. 32 Abs. 1 lit. d) DS-GVO/§ 26 Abs. 1 lit. d) KDG Verfahren zur regelmäßigen Überprüfung,

24 EuGH, Urteil vom 20.06.2024 - C-182/22 und C-189/22

Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen zu implementieren und der aktuelle Stand der Technik sollte regelmäßig überprüft werden. Sicherheitsmaßnahmen sollten nachvollziehbar dokumentiert werden.

Auch wenn ein Schadensersatzanspruch bei einem reinen Kontrollverlust im Einzelfall also nur gering ausfallen dürfte, können sich auch solche Beträge bei einer Vielzahl Betroffener summieren. Datenschutz-Compliance lohnt sich!

1.2.6 Das neue Digitale-Dienste-Gesetzes (DDG)

Am 14. Mai 2024 ist das Digitale-Dienste-Gesetz (DDG) in Kraft getreten. Das Gesetz soll den EU-Digital-Services-Act (DSA) ergänzen und den Rechtsrahmen in Deutschland an die Vorgaben des DSA anpassen. Diese Verordnung ist bereits am 16. November 2022 in Kraft getreten, gilt aber vollständig erst seit dem 17. Februar 2024.

Beim DSA geht es im Kern darum, ein sicheres Online-Umfeld zu schaffen und die Verbreitung illegaler Inhalte zu reduzieren. Wie die entsprechenden Pflichten umgesetzt werden, regelt das Digitale Dienste Gesetz für Deutschland.

Telemediendienste sind jetzt Digitale Dienste

- Die bisher als „Telemediendienste“ bekannten Dienste werden nun als „Digitale Dienste“ bezeichnet. Das Telemediengesetz (TMG) ist im DDG aufgegangen. Das Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG), das noch gar nicht so lange existierte, wurde zum Telekommunikation-Digitale-Dienste-Datenschutzgesetz (TDDDG) umbenannt.
- Der Adressatenkreis der Gesetze und auch der Inhalt bleiben unverändert. Dennoch ergibt sich u. U. ein Handlungsbedarf.

Impressumspflicht ist jetzt im DDG geregelt

- Die Pflicht zur Anbieterkennzeichnung, vorher im § 5 TMG geregelt, findet sich jetzt in § 5 DDG. Inhaltliche Änderungen sind damit nicht verbunden. Es wurden lediglich redaktionelle Anpassungen

vorgenommen. Wer bisher ein Impressum vorhalten musste, ist dazu auch nach dem DDG verpflichtet.

- Erfolgt auf der Website ein Verweis auf „Pflichtangaben nach § 5 TMG“, ist eine Anpassung vorzunehmen. Eine Verpflichtung die Norm explizit zu nennen besteht nicht. „Impressum“ oder „Anbieterkennzeichnung“ genügt.

Cookie-Opt-in-Regelung jetzt im TDDDG

- Die Regelung aus § 25 TTDSG, wonach für das Setzen und Auslesen technisch nicht erforderlicher Cookies eine explizite Zustimmung der Nutzer erforderlich ist, ist jetzt in § 25 TDDDG enthalten. Inhaltliche Änderungen erfolgten auch hier nicht.

- Sofern in der Datenschutzinformation oder im Rahmen eines Cookie-Management-Systems noch auf § 25 TTDSG als Rechtsgrundlage verwiesen wird, sollte das geändert werden, denn das Gesetz existiert seit dem 14. Mai 2024 nicht mehr. Wobei zu berücksichtigen ist, dass es eines Verweises auf § 25 TDDDG wohl nicht bedurft hätte. Rechtsgrundlage für die mit dem Setzen oder Auslesen von Cookies verbundene Datenverarbeitung ist die Einwilligung, nicht das Gesetz. Allenfalls bei notwendigen Cookies ist denkbar, dass es eines Hinweises auf § 25 Abs. 2 TDDDG bedarf. Das sollte in der jeweiligen Datenschutzerklärung oder Cookie-Policy geändert werden.

Haftung für Inhalte

Das DDG übernimmt zwar einige der Regeln aus dem TMG, doch auch im DSA der EU sind bereits ehemalige Vorschriften aus dem TMG enthalten, wie z. B. Regelungen zur Haftung für Inhalte:

Die Haftung bei Durchleitung, Caching und Hosting sind nunmehr in Art. 4 ff. DSA geregelt. Die Sondervorschriften zur Störerhaftung und der Haftung von WLAN-Betreibern wurden dagegen in die §§ 7, 8 DDG übernommen.

Wenn noch nicht erfolgt, sollte Folgendes getan werden:

- Impressum und den Link, der dorthin führt, prüfen. Sofern noch auf § 5 TMG verwiesen wird, sollte das geändert werden. Das TMG ist aufgehoben.

- Prüfung der Datenschutzinformation und einer etwaige Cookie-Policy, ob darin noch das „TTDSG“ genannt ist. „TTDSG durch „TDDDG“ ersetzen. Dabei sollte auch gleich geprüft werden, ob es einer Angabe überhaupt bedarf und ob die Datenschutzerklärung insgesamt auf dem aktuellen Stand ist.

1.2.7 Beschäftigtendatenschutzgesetz – eine weitere vertane Chance

Die Notwendigkeit zur Schaffung eines speziellen Beschäftigtendatenschutzgesetzes ist in Literatur und Rechtsprechung weitgehend unbestritten. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert ein solches Gesetz.

Diese Erkenntnis ist auch beim Bundesgesetzgeber vorhanden. Bereits zu Beginn der 17. Legislaturperiode des Deutschen Bundestages ist dazu ein Gesetzesentwurf der SPD-Fraktion eingebracht worden. Nachdem dieser vier Jahre lang beraten worden ist, fiel er am Ende der Legislaturperiode dem Diskontinuitätsgrundsatz zum Opfer. Danach verschwand dieses Vorhaben von der Tagesordnung. Ende der 19. Legislaturperiode wurde ein Expertenbeirat eingesetzt, der sich mit diesem Thema erneut beschäftigen sollte. Das Gremium legte im Januar 2022 (inzwischen 20. Legislaturperiode) seinen Abschlussbericht vor. Ein weiteres Jahr später legten die Bundesministerien für Arbeit und Soziales sowie des Innern und für Heimat „Vorschläge für einen modernen Beschäftigtendatenschutz“ vor. Die darin referierten Eckpunkte entsprechen im Wesentlichen einer Zusammenfassung der Ergebnisse des Abschlussberichtes.

Am 8. Oktober 2024 haben die Bundesministerien für Arbeit und Soziales und des Innern und für Heimat einen gemeinsamen Referentenentwurf für ein Beschäftigtendatenschutzgesetz veröffentlicht. Die Festlegung im Koalitionsvertrag: „Wir schaffen Regelungen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen“ sollten damit umgesetzt werden. Aufgrund der Beendigung der Ampelkoalition am 6. November 2024 war bereits zu diesem Zeitpunkt davon auszugehen, dass eine Mehrheit im Bundestag für ein solches Gesetz nicht mehr vorhanden ist.

Auch wenn bei Gewerkschaften Arbeitgeberverbänden und in weiten Teilen der Politik die Notwendigkeit eines solchen Gesetzes nicht in Frage gestellt wird, ist fraglich, ob der nächste Bundestag bereit ist, über ein Beschäftigtendatenschutzgesetz zu beraten. Beschäftigtendatenschutz wird dann weiterhin von

Richterrecht geprägt sein. Für Beschäftigte bedeutet dies, auch in Zukunft ihre Rechte stets im Einzelfall entscheiden lassen zu müssen.

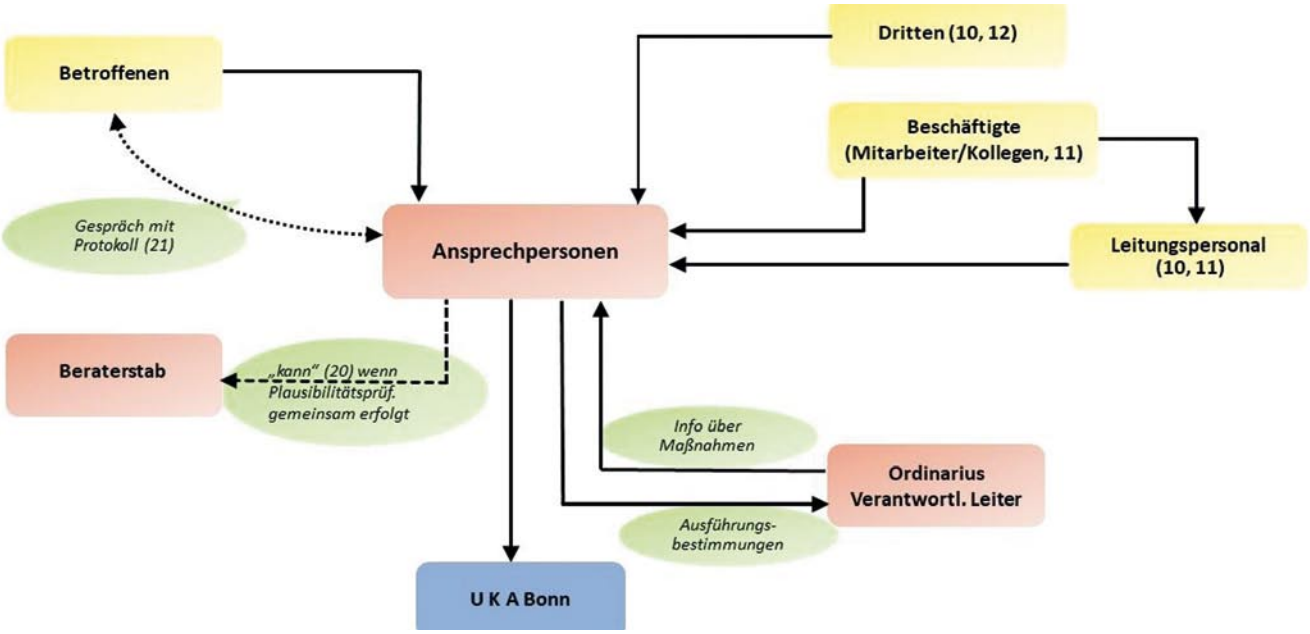
1.3 Entwicklung des Datenschutzes in der Kirche

1.3.1 Aufarbeitung und Datenschutz

Die katholische Kirche hat anerkannt, dass Kleriker und sonstige Beschäftigte der katholischen Kirche in Deutschland in der Vergangenheit Kinder und Jugendliche sexuell missbraucht haben.[25] Die Deutsche Bischofskonferenz hat sich in dieser Erklärung zur Fortsetzung der umfassenden Aufarbeitung des sexuellen Missbrauchs verpflichtet.

Im Folgenden wurden aufgrund der „Ordnung für den Umgang mit sexuellem Missbrauch Minderjähriger und schutz- oder hilfebedürftiger Erwachsener durch Kleriker und sonstige Beschäftigte im kirchlichen Dienst (Interventionsordnung)“ Gremien und Personen ernannt, die sich mit der Aufarbeitung befassen. Dazu zählen Ansprechperson, Beraterstab, Interventionsbeauftragter, Aufarbeitungskommission und Betroffenenbeirat.

Die Zusammenarbeit dieser Institutionen ist in der Ordnung dargestellt. Der Datenfluss laut Interventionsordnung gestaltet sich wie folgt:[26]



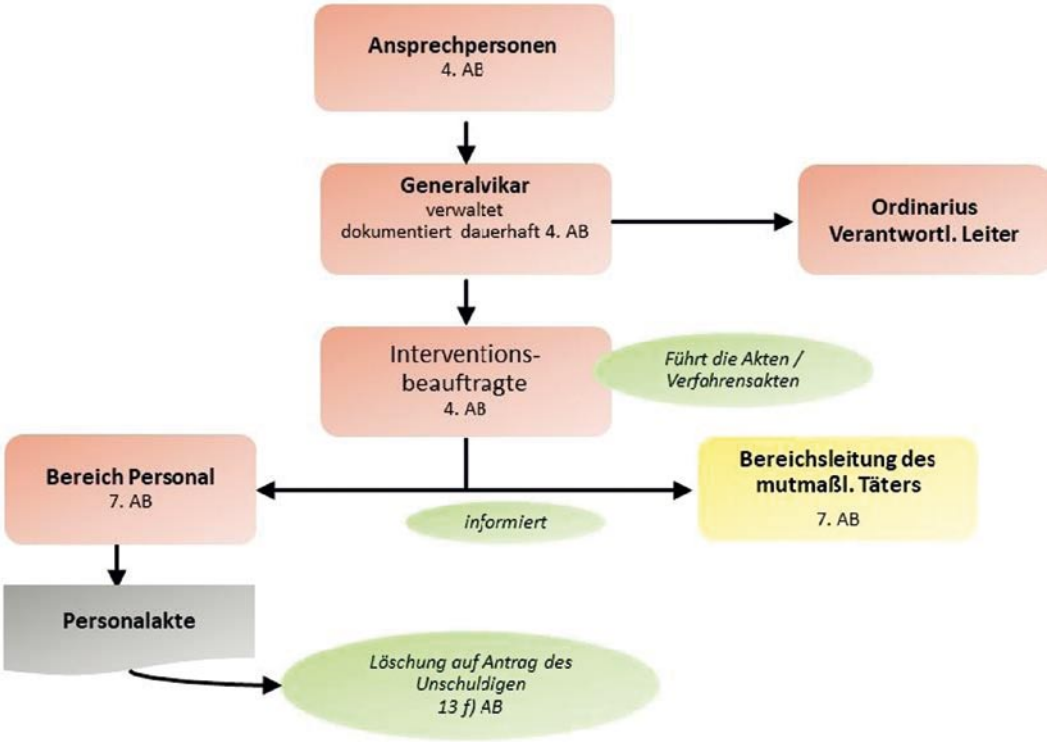
25 Gemeinsame Erklärung über verbindliche Kriterien und Standards für eine unabhängige Aufarbeitung von sexuellem Missbrauch in der katholischen Kirche in Deutschland, https://www.dbk.de/fileadmin/redaktion/diverse_downloads/presse_2020/2020-074a-Gemeinsame-Erklaerung-UBSKM-Dt.-Bischofskonferenz.pd

26 Die angefügten Ziffern bezeichnen die Nummerierung in der Ordnung

Aus dieser Darstellung wird deutlich, dass personenbezogene Daten, in der Regel auch solche besonderer Kategorie, an verschiedenen Stellen verarbeitet werden. In der Ordnung ist dazu bislang nicht festgelegt, auf welchem Weg die Daten die einzelnen Institutionen erreichen und ob oder wie sie dort ggf. gespeichert werden.

Dies gilt auch für den weiteren Verlauf der Aufarbeitung, wie sie in den „Ausführungsbestimmungen zur Ordnung für den Umgang mit sexuellem Missbrauch Minderjähriger und schutz- oder hilfebedürftiger Erwachsener durch Kleriker und sonstige Beschäftigte im kirchlichen Dienst" erlassen worden sind.[27]

Der Datenfluss der Sanktionen ist folgendermaßen:



In diesem Fall sind die allgemeinen Regelungen des Datenschutzes anzuwenden, nach denen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die jeweiligen Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

Eine Duplizierung der personenbezogenen Daten an jede sich damit zu befassender Stelle scheidet danach aus. Vielmehr ist dafür Sorge zu tragen,

27 Die genannten Nummern beziehen sich auf die Nummerierung der Ausführungsbestimmungen (AB)

dass personenbezogene Daten nach der Weiterleitung an die zuständige Stelle bei der meldenden Stelle gelöscht werden. Nur auf diese Weise ist sicher zu stellen, dass einem Auskunftsanspruch von Betroffenen umfangreich entsprochen werden kann. Außerdem ist bei einem solchen Verfahren gewährleistet, dass personenbezogene Daten nicht von einzelnen Empfängern kopiert werden.

In einem von der KDSA-Ost zu diesem Thema veranstalteten Workshop, an dem Vertreter aller beteiligten Institutionen teilnahmen, konnten Regelungen für ein zukünftiges Verarbeiten von personenbezogenen Daten in diesem Zusammenhang erarbeitet werden.

Die Teilnehmenden einigten sich für die Zukunft auf folgendes Vorgehen:

- Alle personenbezogenen Daten werden digitalisiert.
- Alle digitalisierten Daten werden ausschließlich auf einem zentralen Server gespeichert.
- Die Zugriffsrechte auf den Server werden aufgabenbezogen und zeitlich beschränkt vergeben.

Damit hat jeder Akteur nur auf die Daten Zugriff, die er zur Erfüllung seiner Aufgaben benötigt und auch nur innerhalb des Zeitraumes, der zur Aufgabenerfüllung erforderlich ist.

Ursprünglich analog vorgelegte Daten werden nach der Digitalisierung für Dritte unzugänglich bei der Leitung (Generalvikar) gesichert.

Wie ein zentraler Datenspeicher (private Cloud) funktionieren kann ist in Punkt 7.3 in diesem Tätigkeitsbericht dargestellt.

2 Datenschutz allgemein

2.1 Weitergabe von (Masernschutz)-Attesten an Gesundheitsämter

Seit dem 31. Juli 2022 gilt die Masernimpfpflicht in Gemeinschaftseinrichtungen wie Schulen und Kindertageseinrichtungen. Diese gilt für alle, die in

einer dieser Einrichtungen betreut werden oder tätig sind. Im Weiteren gilt die Masernimpfpflicht auch für viele Beschäftigte in Gesundheitseinrichtungen wie Krankenhäuser, Rehabilitationseinrichtungen oder Arztpraxen.

Wie die Impf- oder Immunitätsnachweise datenschutzkonform erhoben werden können, kann in unserem Tätigkeitsbericht 2022[28] nachgelesen werden.

Wie handeln aber die Verantwortlichen richtig, wenn der Betroffene den Nachweis nicht erbringt oder ein Attest vorlegt, dass eine Kontraindikation zur Masernschutzimpfung besteht?

Gemäß § 20 Abs. (9) Satz 2 IfSG „…hat die Leitung der jeweiligen Einrichtung unverzüglich das Gesundheitsamt, in dessen Bezirk sich die Einrichtung befindet, darüber zu benachrichtigen und dem Gesundheitsamt personenbezogene Angaben zu übermitteln."

Ausgeschlossen ist damit jegliche Weitergabe von Attesten oder Bescheinigungen an das Gesundheitsamt. Die Einrichtungen dürfen nur die personenbezogenen Angaben übermitteln, die notwendig sind, damit das Gesundheitsamt Kontakt mit dem Betroffenen aufnehmen kann. Dazu zählen Name, Vorname und Anschrift, die auf einem gesicherten Weg übermittelt werden müssen. Weder im o.g. Abschnitt des IfSG noch im KDG finden sich Rechtmäßigkeiten, die eine Weitergabe des gesamten Attestes erlauben. Nach § 7 Abs. 1 lit. c KDG muss die Datenverarbeitung und somit auch die Weitergabe auf das notwendige Maß beschränkt sein.

Auch vor der Weitergabe anderer Atteste (z.B. Sportbefreiungen, gehäufte Krankschreibungen) an das zuständige Gesundheitsamt muss ganz genau geprüft werden, ob eine Rechtsgrundlage die komplette Weitergabe des Attestes erlaubt oder ob eine Übermittlung der Kontaktdaten des Betroffenen ausreichend und zweckdienlich ist.

28 TB 2022, Pkt. 5.1 Bundesverfassungsgericht bestätigt Masernimpfpflicht

2.2 Werbe-ID: Das Nummernschild für Smartphones

Jedes Smartphone besitzt eine individuelle Kennung, die Werbe-ID (auch Advertising ID), unabhängig davon, ob dieses mit einem Android oder iOS Betriebssystem betrieben wird.

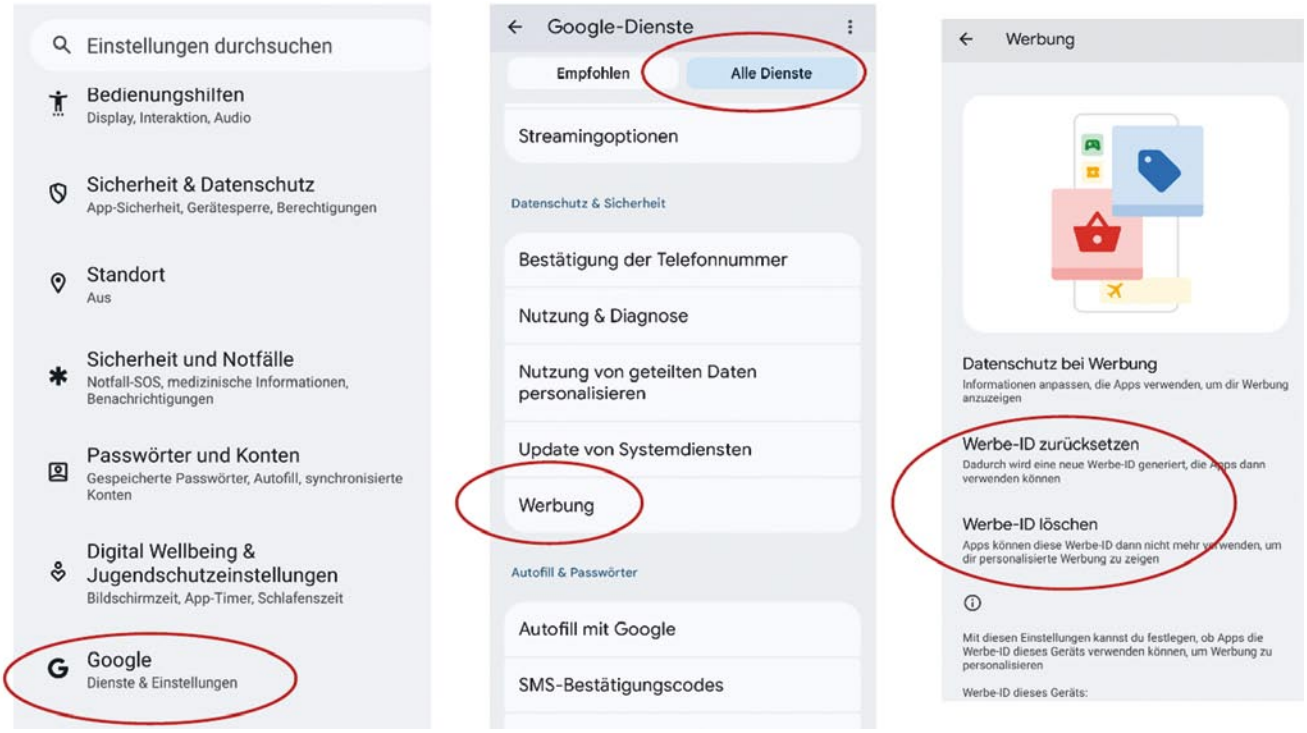
Die Werbe-ID dient dazu dem Handy-Nutzer personalisierte Werbung zukommen zulassen. App-Anbieter und werbende Unternehmen gleichen dabei diesen „Baustein" ab und senden dann dem Nutzer personalisierte Werbung, ohne dabei zu erfahren, wer der Nutzer eigentlich ist. Nun könnte man denken, dass die Werbe-ID für einen gewissen Datenschutz sorgt und deshalb nicht zu beanstanden ist. Dem ist jedoch nicht so. Da jedoch viele Apps und datensammelnde Unternehmen genau diese Werbe-ID mit anderen Informationen bzw. Daten (z.B. Standortdaten oder Suchanfragen) verknüpfen, lassen sich ganz einfach Nutzer- und Bewegungsprofile anlegen. So hat eine Recherche von netzpolitik.org[29] zusammen mit dem BR (Bayerischer Rundfunk) ergeben, dass Datenhändler die Werbe-IDs mit GPS-Daten der Handynutzer verknüpfen und dann anschließend verkaufen. Aus GPS-Daten, die einer Werbe-ID zugeordnet sind, lässt sich ohne Probleme ein Bewegungsprofil erzeugen, welches auch zur Identifizierung der Person führen kann.
Die Recherche hat auch gezeigt, wie einfach es ist, an diese Datensätze zu gelangen.

Doch was kann man tun, um sich davor zu schützen?

Einen 100 prozentigen Schutz wird es nicht geben, wenn man ein Smartphone nutzen möchte. Man kann aber seinen eigenen Datensatz möglichst „klein" halten, indem man die GPS-Funktion nur aktiviert, wenn diese auch benötigt wird (z.B. zum Navigieren). Zudem ist es empfehlenswert, die Werbe-ID regelmäßig zu löschen oder zu erneuern, um den Prozess der Zuordnung zu unterbrechen.

29 Netzpolitik.org, https://netzpolitik.org/2024/databroker-files-firma-verschleudert-36-milliarden-standorte-von-menschen-in-deutschland/, zuletzt aufgerufen am 17.02.2025

Bei den meisten Geräten kann man die Werbe-ID unter den Einstellungen, Google (Dienste & Einstellungen) finden und zurücksetzen. Das funktioniert so:



2.3 Alte Handys entsorgen und recyceln: Darauf sollte man achten

Das neue Smartphone ist eingerichtet und läuft – aber was macht man jetzt mit dem alten Gerät? In der Schublade sollte es besser nicht landen.

Das Smartphone ist zwar nicht mehr taufrisch, tut aber noch seinen Dienst?

Alte Modelle kann man bei verschiedenen Stellen abgeben. Experten prüfen die Geräte und entscheiden, ob sie noch funktionstüchtig sind:

- Wenn sie nicht mehr funktionieren, werden alte Mobiltelefone recycelt.
- Sind sie noch funktionstüchtig, werden die Mobiltelefone aufbereitet, weiterverkauft und die Erlöse häufig gespendet.

Ob beim Recycling, Spenden, Verkaufen oder Verschenken: Sichern Sie unbedingt Ihre Daten mit einem Back-up und entfernen Sie danach alles von dem ausgedienten Handy, bevor es entsorgt wird.

So geht man vor, wenn das Smartphone von Daten bereinigt werden soll:

1. **SIM-Karte herausnehmen**, denn darauf können Kontakte gespeichert sein.
2. **Entfernung (falls vorhanden) der SD-Karte** aus dem Gerät: Auf ihr befinden sich viele persönliche Daten.
3. **Sicherung via Backup** aller Fotos, Videos, Kontakte, Chat-Nachrichten und SMS, die auf dem Handy gespeichert sind. Danach erfolgt eine manuelle Löschung dieser Daten vom Gerät.
4. **Abmeldung von allen Konten.** Auf einem iPhone ist das die iCloud und bei einem Android-Smartphone das Google-Konto. Beides erledigt man in den Einstellungen.
5. **Zurücksetzen des Gerätes** auf Werkseinstellung. Damit entfernt das Betriebssystem alle persönlichen Daten und Einstellungen vom Gerät. Bei Android findet man die Option in den Einstellungen meist unter „System“ und bei iOS in den allgemeinen Einstellungen „Zurücksetzen“.

Mit dieser Checkliste kann man sich selbst prüfen, ob alle Schritte ausgeführt worden sind.

2.4 Richtlinien-Änderung bei Facebook: Gut zu wissen

Für Instagram und Facebook gilt seit dem 26. Juni 2024 eine neue Regelung für den Datenschutz. Der Mutterkonzern Meta gibt sich selbst das Recht, seine künstliche Intelligenz (KI) mit den Daten der Nutzer zu trainieren.

Das umfasst laut der neuen Richtlinie alle „Aktivitäten“ der Nutzer, d. h. alle Beiträge, also auch Bilder und Videos, Kommentare und Audio-Dateien, aber auch Nachrichten, die man versendet einschließlich der mitgeschickten Inhalte wie Bilder, Videos und Metadaten.

Kurz: Meta verwendet für dieses Projekt fast sämtliche Nutzerdaten.

Privatnachrichten, die mit Familienmitgliedern oder Freunden ausgetauscht werden, sollen davon ausgenommen sein. Was das genau heißt, ist aber nicht klar.

Was passiert mit den Daten?

Meta möchte mit den Daten seine KI-Modelle trainieren. Bekanntlich brauchen diese riesige Mengen an Lernmaterial. Welche KI-Arten damit trainiert werden sollen, sagt Meta aber nicht. Naheliegend dürfte aber sein, dass mit Nachrichten, Fotos und Audio vor allem KI-Textmodelle für Chatbots, künstliche Stimmen und Bildgeneratoren gefüttert werden sollen.

Meta will diese KI-Modelle und die für das Trainieren gebrauchten Nutzerdaten auch Dritten, wie z.B. Entwicklern und Forschern, bereitstellen.

Scharf kritisiert werden diese Änderungen u. a. von Noyb, der Datenschutzorganisation des österreichischen Juristen und Aktivisten Max Schrems. Diese stört sich insbesondere daran, dass es sich um eine „Opt out“ Änderung handelt.
Das bedeutet, Nutzer müssen selbst aktiv werden und sich von der Datenverwertung für KI abmelden statt der Änderung zuzustimmen, wenn sie damit einverstanden sind.

Die Abmeldung sei unnötig kompliziert, so Nyob. Die Organisation hat in elf Ländern Beschwerden eingereicht, einen sofortigen Stopp „des Missbrauchs persönlicher Daten“ gefordert und ein Dringlichkeitsverfahren eingeleitet.

Was sind die Risiken?

Weil es sich um persönliche Daten handelt, sind die Risiken besonders hoch. Kriminelle könnten den KI-Chatbots sehr persönliche Informationen entlocken, die aus Trainingsdaten stammen– etwa Kreditkartennummern.

Üblicherweise ist die Verarbeitung persönlicher Daten in der EU standardmäßig verboten. Meta muss sich daher auf eine Rechtsgrundlage gemäß Art. 6 Abs. 1 DS-GVO für die Verarbeitung berufen. Die logische Wahl wäre, eine Einwilligung der Nutzer einzuholen. Stattdessen argumentiert Meta

erneut, dass es ein „berechtigtes Interesse“ gäbe, das über den Grundrechten der Nutzer steht.

Wie kann man sich dagegen wehren?

Wer seine Daten nicht für das Training der KI hergeben möchten, muss ein Formular ausfüllen, d.h. der Nutzung widersprechen. Wichtig: Dies gilt jeweils separat pro Plattform!!!

So gehts:

Rufen Sie Instagram oder Facebook auf und melden sich an.

Wenn Sie angemeldet sind, müssen Sie das Widerspruchsformular der jeweiligen Plattform aus der Datenschutzrichtlinie heraus öffnen. Sie finden den Link zum Formular «Widerspruchsrecht» zuoberst in der Infobox zur neuen Datenschutzrichtlinie.

2.5 Digitalzwang: Wie gut funktioniert eigentlich noch ein Leben jenseits von digitalen Einflüssen?

Ohne Internet, Smartphone, Tablet und Co. geht oftmals gar nichts mehr. Ob bei Behörden, beim Einkaufen oder in der Bahn – immer mehr Menschen werden mit Druck zu Smartphone, App und Internet genötigt.

Wie viele Neuerungen hat auch die Digitalisierung ihre Schattenseiten. Dazu zählen unter anderem die Cyberkriminalität und der Digitalzwang. Wie groß die Einschränkungen dabei inzwischen ausfallen, geht aus den Bereichen hervor, in denen der Druck zur Verwendung eines Smartphones oder Computers überhandnimmt.

Bankgeschäfte per Handy, Terminvereinbarung auf der Internetseite der Arztpraxis, E-Rezepte via digitaler Gesundheitskarte einlösen, Schnäppchen nur im Internet, Lebensmittel einkaufen im hybriden Supermarkt, kassenlose Bezahlmöglichkeit, Fahrkarten für den öffentlichen Nahverkehr per App kaufen, ein Auto über eine Carsharing-App mieten oder auch „nur“ das Ablesen des Energieverbrauchs oder das Beantragen von Leistungen, z. B. Bürgergeld, geht digital. Ein weiterer Vorreiter bei der Zwangsdigitali-

sierung ist das Logistik-Unternehmen DHL. Wenn Sendungen in Paketstationen landen, weil der Postbote den Empfänger verpasst hat, dann hat der Kunde nun oft ein Problem, sofern er ohne Smartphone ist. Denn in vielen Paketstationen erhalten Abholer ausschließlich mit der „Post & DHL App“ Zugang.

Und auch in etlichen Restaurants sind Menschen ohne Smartphone inzwischen unwillkommen. Anstatt der Speisekarte prangt ein QR-Code auf dem Tisch, den man einscannen soll, um dann seine Auswahl zu treffen.

Und dann sind da noch die Kommunen, deren Parkplätze nur für Smartphonebesitzer nutzbar sind. Gerade öffentliche Einrichtungen sollten ihre Angebote barrierefrei zur Verfügung stellen.

Massiven Digitalisierungszwängen sind zudem Studenten an deutschen Universitäten ausgesetzt. Ohne Smartphone bleibt ihnen oftmals der Zugang zu Bibliotheken oder die Nutzung des Semestertickets verwehrt.

Die Nötigung der Bürger zum Gebrauch von Smartphones oder Computern wird meist mit Kosten- und Umweltargumenten entschuldigt. Stromverbrauch und Elektroschrott bleiben dabei außer Acht.

Digitalisierung bietet zudem die Möglichkeit der Bevölkerungskontrolle. Zur Erinnerung: Während der Corona-Zeit war der auf dem Smartphone gespeicherte Impfnachweis oftmals Voraussetzung für den Zugang zu Örtlichkeiten und Dienstleistungen.
Die Bahn kann ihre Kunden mit der App „DB Navigator“ überwachen. Die App registriert z. B. wer, wann, mit wem, wohin fahren möchte. Dem zu widersprechen, was auch für die Weitergabe der Daten an Dritte gilt, ist nicht möglich. Darüber hinaus besteht der Zwang, in regelmäßigen Abständen ein neues Gerät auszuwählen und zu kaufen, um die aus Sicherheitsgründen notwendigen Software-Aktualisierungen vornehmen zu können. Das führt nicht selten zumindest zur finanzieller oder auch mentaler Überforderung.

Digital ist spitze! Aber nur wenn wir die Wahl haben und nicht dazu gezwungen werden. Bereits im Tätigkeitsbericht 2021 haben wir uns im Bei-

trag „Ohne Smartphone Mensch zweiter Klasse aber sicher“ mit der zunehmenden Digitalisierung im Alltag beschäftigt.[30]

Digitalisierung ist nützlich zur Verbesserung von Wirtschaftlichkeit und Bürgerservice. „Digital only“, also das Fehlen einer analogen Alternative, kann aber zu Diskriminierungseffekten und Grundrechtsbeeinträchtigungen führen, wenn Menschen ausgeschlossen werden, weil ihnen die Nutzung praktisch nicht möglich oder nicht zumutbar ist, etwa wegen der Kosten, des Alters, einer Behinderung oder wegen der Furcht vor einem Datenmissbrauch.

Wird die digitale Schranke zur sozialen Barriere?

Immerhin zählen rund drei Millionen Menschen in Deutschland zu den sogenannten Offlinern. Was einer von DeStatis veröffentlichten Studie[31] nach bedeutet, dass fünf Prozent unserer Bevölkerung im Alter zwischen 16 und 74 Jahren noch nie das Internet genutzt haben. Damit werden durch den Digitalzwang Millionen von Bundesbürgern von einem wesentlichen Teil des öffentlichen Lebens ausgeschlossen, wobei die Älteren und Ärmeren überdurchschnittlich betroffen sind.

Die Gründe dafür sind vielschichtig. Neben einem geringen Einkommen, um sich Internetverträge, -anschlüsse und internetfähige Geräte leisten zu können, führen auch Unwissen und Unsicherheit sowie eine teilweise noch immer fehlende digitale Infrastruktur, insbesondere im ländlichen Raum, dazu, dass digitale Angebote nicht genutzt werden.
Hinzu kommt der stetige technische Fortschritt oder die Angst nicht mehr Herr über die vielen Digitalangebote und Anwendungen zu sein. Sorgen und Ängste um Datenschutz und Sicherheitsrisiken kommen dazu.

Und es gibt immer noch Menschen, die sich bewusst gegen Handynutzung und Internet entscheiden – ganz freiwillig.

Wahlfreiheit – Grundrecht auf analoges Leben

Ein Leben ohne Internet, ohne Smartphone, ohne Apps – das muss möglich sein und bleiben. Dieser Meinung ist auch Leena Simo, eine Netzphilo-

30 TB 2021, Pkt. 1.2.7
31 https://www.destatis.de/DE/Presse/Pressemitteilungen/Zahl-der-Woche/2024/PD24_15_p002.html

sophin der Initiative Digitalcourage, die ein „Recht auf Leben ohne Digitalzwang“ im Grundgesetz verankern will.[32] Die Forderung an den Bundestag beinhaltet, dass es zu digitalen Angeboten stets auch eine analoge oder datenschutzfreundliche Alternative geben muss.

Wenn man faktisch gar keine andere Wahl mehr hat, man z. B. bei Behörden Termine nur noch online bekommt oder weil man nur mit der Bahn reisen kann, wenn man ein Smartphone hat, ist Zwang gegeben. Das ist die Kehrseite des digitalen Standards, der bereits jetzt schon dazu führt, dass Menschen ohne Internet und Smartphone an einigen Stellen nicht mehr am öffentlichen Leben teilhaben können.

So stellen z. B. Krankenkassen, Banken und Co., ihre Apps ausschließlich in Verbindung mit einem Google-Account für den Download zur Verfügung. Das bedeutet: Ohne Google-Konto oder Apple-ID keine Apps! Um sich mit seiner Krankenkasse auszutauschen, muss dann zunächst ein Geschäftsverhältnis mit Google eingegangen werden. Ein Unding! Google ist ein US-Konzern, der überhaupt nichts mit den Gesundheitsdaten der Krankenkassenmitglieder zu tun hat.

Dem Internetzwang Einhalt bieten

Wenn es wirklich um die Teilhabe am öffentlichen Leben – also die Grundversorgung – geht, dann muss es eine alternative Option geben. Wenn z. B. die Technik ausfällt, braucht es ja auch eine Fallback-Option. Auch im Hinblick auf Sicherheitsaspekte ist es wirklich kein guter Rat, sich allein auf die Technik zu verlassen. Es sollte auch immer noch eine analoge Alternative dazu geben, die dann auch diejenigen nutzen können, die aus welchen Gründen auch immer, auf diesen Weg setzen.

Mit der Digitalisierung kann das Leben für viele Menschen leichter gemacht werden. Das funktioniert aber nur, wenn digitale Teilhabe wirklich für alle möglich ist und durchgängig funktioniert. Also jeden mitnehmen, keinen zurücklassen.

Fazit: Zwang findet auf vier Ebenen statt.

32 https://digitalcourage.de/digitalzwang, zuletzt abgerufen am 17.02.2025

- Es fehlen zunehmend analoge Alternativen, um auch ohne Smartphone oder Computer am gesellschaftlichen Leben teilhaben zu können.
- Es wird enormer Druck ausgeübt, bestimmte Geräte, Programme oder Apps einzelner Hersteller nutzen zu müssen.
- Immer häufiger besteht die Pflicht, ein digitales Konto anzulegen und dabei umfangreiche Angaben über die eigene Person zu machen.
- Der Digitalisierungszwang führt auch sonst zur unfreiwilligen Aufgabe von Privatsphäre. Die aufgenötigten Dienste sind nur verfügbar, wenn die Nutzer bereit sind diverse Überwachungstechnologien zu akzeptieren.

Dazu kommen die allgemeinen Nachteile der Nutzung von Smartphones. Sie schüren die Erwartung, dass jeder immer und überall erreichbar sein möge.

2.6 Barrierefreiheit als Herausforderung für den Datenschutz?

Die Barrierefreiheit von Dienstleistungen, Produkten und Informationen ist ein zentraler Baustein für eine inklusive Gesellschaft. Dabei geht es um den Abbau von Hindernissen für Menschen mit Beeinträchtigungen, die diese an der „vollen, wirksamen und gleichberechtigten Teilhabe an der Gesellschaft hindern können“ (vgl. Art. 3 Nr. 1 Richtlinie (EU) 2019/882).

Insbesondere im digitalen Raum erfordert die Umsetzung barrierefreier Angebote oft komplexe technische und organisatorische Anpassungen. Auch im Hinblick auf den Datenschutz werden in diesem Kontext einige Fragen aufgeworfen, die näher betrachtet werden sollen.

Rechtslage und Anwendungsbereich bei der Barrierefreiheit

Aufbauend auf dem Behindertengleichstellungsgesetz (BGG), der Barrierefreie-Informationstechnik-Verordnung (BITV 2.0) und einem Sammelsurium weiterer Rechtsnormen sind öffentliche Stellen bereits jetzt verpflichtet, Webseiten und sonstige Angebote barrierefrei zu gestalten (u.a. durch „einfache Sprache“, Gebärdensprache). Die Privatwirtschaft unterlag bisher

keinen derartigen Regularien. Auf Grund der EU-Richtlinie 2019/882 nimmt das Barrierefreiheitsstärkungsgesetz (BFSG) nun auch Privatunternehmen – in Relation zu Größe und Umsatz – in die Pflicht.

Wer ist betroffen?

Das neue Gesetz richtet sich wie der neue Cyber Resilience Act an Hersteller, Händler und Importeure von bestimmten Produkten sowie an Erbringer bestimmter Dienstleistungen. Abhängig von der Größe und dem Umsatz des Unternehmens müssen Privatunternehmen die verschiedenen Vorgaben umsetzen. Kleinstunternehmen, also Unternehmen, die weniger als zehn Personen beschäftigen und entweder einen Jahresumsatz von höchstens 2 Millionen Euro erzielen oder dessen Jahresbilanzsumme sich auf höchstens 2 Millionen Euro beläuft, sind zu Teilen von den Vorgaben befreit.
Nach § 1 BFSG fallen unter den Anwendungsbereich beispielsweise Hardwaresysteme von Universalrechnern, inklusive Betriebssysteme, Geldautomaten, Smartphones, E-Book-Reader oder Webseiten von Personenbeförderungsdiensten, wie etwa Fluggesellschaften.

Datenschutzrechtliche Relevanz

Muss in einem der oben genannten Bereiche eine Anpassung aufgrund des BFSG vorgenommen werden, muss hierbei auch die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere der DS-GVO (KDG), beachtet werden.

Transparenzpflichten

Art. 13 und 14 der DS-GVO regeln Vorgaben zu Informations- und Transparenzpflichten. Art. 12 Abs. 1 DS-GVO schreibt vor, dass diese Mitteilungen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln sind. Hierneben müssen betroffene Unternehmen bei der Datenschutzerklärung nun auch die Barrierefreiheit beachten.

Betroffenenanfragen

Art. 15 ff. DS-GVO/§ 17 KDG bestimmt eine Reihe von Rechten, die von Datenverarbeitungen Betroffene gegen Verantwortliche geltend machen

können. Unternehmen müssen in Anbetracht des BFSG nun auch sicherstellen, dass diese Betroffenenrechte zukünftig auch barrierefrei geltend gemacht werden können. Gerade wegen fehlender Formvorgaben sollte sichergestellt werden, dass sowohl eine telefonische als auch eine schriftliche Geltendmachung möglich ist. Zudem sollten auch nicht eindeutige Anfragen wenigstens mit einer Nachfrage beantwortet werden, statt sie nicht zu beantworten, um eine Benachteiligung potenziell geistig beeinträchtigter Personen zu vermeiden. Die Beantwortung von Anfragen sollte in leicht verständlicher Sprache und unter Verweis auf audiovisuelle Mitteilungen erfolgen.

Sicherheitsmaßnahmen

Angesichts der eigentlich erforderlichen Sicherheitsvorkehrungen (vgl. Art. 32 Abs. 1 DS-GVO/§ 27 Abs. 1 KDG) kann es gegebenenfalls zu einer Reduzierung des Sicherheitsniveaus aufgrund der jeweiligen Umstände und Zwecke der Datenverarbeitung kommen.

Bereits 2023 entschied das Sozialgericht Hamburg[33] , dass blinde und sehbehinderte Menschen gegenüber dem Jobcenter Anspruch auf elektronische Übersendung der maßgeblichen Dokumente, d.h. Anträge, Hinweisblätter, Verwaltungsakte und Widerspruchsbescheide, nach entsprechender Einwilligung des Betroffenen auch durch unverschlüsselte E-Mail, haben, um eine elektronische Vorlesefunktion nutzen zu können.

Fazit:

Das BFSG markiert einen Schritt hin zu einer inklusiveren Gesellschaft. Für Unternehmen kann dies jedoch eine Fülle an technischen und organisatorischen Anpassungen bedeuten. Dies erfordert eine frühzeitige Planung und auch ein Umdenken, um den Spagat zwischen Zugänglichkeit und Datenschutz erfolgreich zu meistern. Binden Sie frühzeitig Ihren Datenschutzbeauftragten bei der Implementierung entsprechender Umstrukturierungen in Ihrem Unternehmen /Ihrer Einrichtung ein.

33 Sozialgericht Hamburg, Urteil vom 30.06.2023 - S 39 AS 517/23

3 Datenschutzaufsicht

3.1 Prüfaktion der Datenschutzaufsicht

3.1.1 Prüfung eines Seniorenzentrums

Wie auch im letzten Berichtszeitraum haben wir im Jahr 2024 eine anlassbezogene Prüfung eines Seniorenzentrums vorgenommen. Die Prüfung war angemeldet. Neben der Einrichtungsleitung und dem IT-Administrator waren auch der Datenschutzbeauftragte und der QM-Beauftragte anwesend. Geprüft haben wir auch in dieser Einrichtung die datenschutzrechtlich relevanten Abläufe im Zusammenhang mit dem Betrieb des Heims, insbesondere die Verwaltung und Aufbewahrung der Bewohnerakten, der Pflegedokumentation und der Personalakten.

1. Datenschutzkonzept, Verzeichnis von Verarbeitungsvorgängen (VVT) und Verpflichtungserklärungen gem. § 5 KDG

Ein Datenschutzkonzept und ein VVT waren vorhanden. Das VVT wird vom Datenschutzbeauftragten gepflegt.

2. Auskünfte über Bewohner an Angehörige

Wie mit Auskunftsersuchen von Angehörigen und anderen Dritten hinsichtlich des Aufenthaltes und des Gesundheitszustandes von Bewohnern umzugehen ist, war den Anwesenden, insbesondere der Einrichtungsleiterin, bekannt. Bewusst war der Leiterin zudem, dass bei unbekannten Angehörigen eine Identitätsprüfung zu erfolgen hat.

3. Bewerbungsverfahren Bewohner

Ein Muster eines Aufnahmeantrages kann online über die Webseite der Einrichtung abgerufen werden. Danach werden unnötige Daten nicht erhoben. Die Abfrage der Daten Geburtsort/Geburtsland/Staatsangehörigkeit konnte nachvollziehbar dargelegt werden. Die Abfrage des Berufes wurde mit der Biographiearbeit erklärt.

4. Pflegedokumentation

Die Pflegedokumentation erfolgt nur digital. In jedem Wohnbereich befinden sich kleine Monitore, die nur mit einem Transponder bzw. mit einem Authentifizierungsstift (Benutzer-ID) entsperrt werden können.

Nach Aussage der Leiterin gab es bisher kein Verlangen auf Einsichtnahme in die Pflegedokumentation. Bekannt war zudem, wem Einsicht unter welchen Voraussetzungen zu gewähren ist (Bewohner/MDK/ Heimaufsicht/ Angehörige/Pflegversicherung/Hausarzt/Betreuer). Bekannt war, dass der Pflegekasse nur Einsicht in die Abrechnungsunterlagen zu gewähren ist.

Es besteht ein Berechtigungskonzept.

5. Wunddokumentation (Fotos)

Die Wunddokumentation erfolgt durch eine sog. Wundschwester (externer Anbieter). Diese verfügt über eine eigene Fotoausrüstung. Da die Wundschwester vom jeweiligen Hausarzt beauftragt wird, besteht keine vertragliche Beziehung zwischen der Einrichtung und dem Wundversorger. Ein Auftragsverarbeitungsvertrag ist daher nicht erforderlich.

6. Fotos

Eine Einverständniserklärung für Foto- und Filmaufnahmen wird mit dem Heimvertrag eingeholt. Bilder von Veranstaltungen bleiben in den Wohnbereichen.

7. Umgang mit Datenpannen

Datenschutzverletzungen entstehen durch die Verletzung des Schutzes personenbezogener Daten, wenn die Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen bedeutet. Dies ist z. B. der Fall bei der ungewollten Veröffentlichung von personenbezogenen Daten, Versendung einer Mail mit offenem Adressverteiler, Versand personenbezogener Daten an den falschen Empfänger oder die Nutzung von Daten für andere als die ursprünglichen Zwecke. Die Einrichtungsleiterin vermittelte den Eindruck dafür sensibel zu sein. Der Leiterin war auch bekannt, dass Datenpannen der Aufsicht zu melden (§ 33 KDG) sind.

Der Datenschutzbeauftragte hat zugesagt auf der nächsten Datenschutzunterweisung die Mitarbeiter nochmal entsprechend zu schulen. Als pro-

blematisch wurden verschiedene Trojaner und Bewerbungen angesehen, die Zip-Dateien enthalten. Angegeben wurde, dass die Einrichtung viele Bewerbungen aus dem Ausland erhält, die den Eindruck vermitteln nicht ernst gemeint zu sein. Diese werden in einem Spam-Ordner verschoben und später gelöscht.

8. Betroffenenrechte

Mit der Informationspflicht des Verantwortlichen geht das Recht des Betroffenen auf Auskunft über die Verarbeitung der sie betreffenden personenbezogenen Daten einher. Angegeben worden ist, dass es bisher keine Anfragen Betroffener oder deren Angehöriger zur Verarbeitung ihrer personenbezogenen Daten gegeben hat. Wie mit derartigen Anfragen umzugehen ist, schien bekannt zu sein. Es wurde darauf hingewiesen, dass auch im Rahmen eines Auskunftsersuchens nach § 17 KDG die Akten in Kopie auszuhändigen sind. Auch die Pflegeakte.

Datenschutz-Informationen nach § 15 KDG sind Bestandteil des Heimvertrages.

9. Weitere Punkte

- Die Dienstpläne können von den Mitarbeitern im Büro der Wohneinheit eingesehen werden. Die Dienstpläne enthalten die Gründe der Abwesenheit (Urlaub, Krankheit, Weiterbildung usw.). Es wurde daraufhin gewiesen, dass die Angabe der Gründe nicht erforderlich ist.
- Die Frage, ob es in der Einrichtung gestattet ist, dass Mitarbeitende während ihrer Dienste private Smartphones bei sich führen dürfen, wurde verneint.
- Namensschilder: Die Namensschilder tragen den Vor- und Zunamen sowie die Funktionsbezeichnung. Es wurde darauf hingewiesen, dass wir die Auffassung vertreten, dass nur der Vorname oder nur der Nachname ausreichend ist. Es wurde angeregt, die Verwendung beider Namen zu überdenken.
- Videoüberwachung: Der Eingangsbereich wird videoüberwacht. Ein Hinweisschild ist angebracht, dies ist jedoch nicht ausreichend. Ein Muster für ein vorgelagertes Hinweisschild wurde der Einrichtung übersandt.

Das Protokoll der Prüfung wurde der Einrichtungsleiterin und der Leitung der Trägergesellschaft übersandt.

Ergebnis:

Die Prüfung des Seniorenzentrums ergab keine Beanstandungen.

Die KDSA kam zu dem Ergebnis, dass die Bereitschaft zur Umsetzung der gesetzlichen Vorgaben zum Datenschutz im hohen Maß vorhanden ist.

3.1.2 Prüfung einer sozialen Einrichtung

In diesem Berichtszeitraum haben wir anlasslos eine Organisation geprüft, deren Aufgabe es ist, auf verschiedenen Wegen schnell und unbürokratisch direkte Hilfen für in Not und Bedrängnis geratene Schwangere, Kinder, Männer und Frauen, Ehen und Familien zu leisten. Es erfolgt eine enge Zusammenarbeit mit verschiedenen Fachberatungsstellen.

Die Prüfung war angemeldet.

Geprüft wurden die datenschutzrechtlich relevanten Abläufe im Rahmen der Arbeit der Organisation.

Im Büro der Geschäftsführerin werden die Unterlagen (Anträge der Hilfesuchenden) in verschlossenen Schränken aufbewahrt. In der Regel suchen die Hilfesuchenden die Beratungsstellen auf. Die Berater weisen diese im Bedarfsfall auf die Möglichkeit hin Hilfen zu beantragen und sind beim Ausfüllen der Anträge behilflich. Die ausgefüllten Anträge werden von den Beratungsstellen an die Geschäftsstelle übersandt. Diese entscheiden über die Gewährung von Hilfen.

1. Datenschutzkonzept und Verzeichnis von Verarbeitungsvorgängen (VVT)

Angegeben wurde, dass ein Datenschutzkonzept nicht vorliegt. Die Erkenntnis, dass dies erforderlich sein dürfte, war vorhanden. Es wurde daraufhin gewiesen, dass eine zeitnahe Erstellung zu realisieren ist. Die Geschäftsführerin sagte die Erledigung zu.

2. Verpflichtungserklärungen gem. § 5 KDG

Ob entsprechende Erklärungen von den Mitarbeiterinnen unterschieben worden sind, konnte nicht geklärt werden. Es wurde zugesagt, dies zu prüfen und ggf. kurzfristig nachzuholen.

3. Internetseite / Datenschutzerklärung

Da auf der Internetseite Mitarbeitende namentlich benannt wurden, haben wir darauf hingewiesen, dass für die Verarbeitungen personenbezogener Daten eine Einwilligung bei den Mitarbeitenden eingeholt werden sollte. Die Leiterin erklärte, Möglichkeiten zu finden, wie hier Abhilfe geschaffen werden kann.

4. Datenspeicherung und Löschung von Daten

Die Akten (Anträge nebst Nachweisen der Bedürftigkeit) werden ausschließlich in der Geschäftsstelle (Büro der Leiterin) aufbewahrt. Papierakten werden nach 10 Jahren datenschutzkonform vernichtet. Die Anträge der Hilfesuchenden werden nicht nur analog in Papierform erfasst und aufbewahrt, sondern auch digital über eine Tabelle (Excel), um mehrfache Antragstellungen zu erfassen und damit zu verhindern, dass Hilfen doppelt/mehrfach bewilligt werden.

Nicht geklärt ist derzeit die Löschung dieser elektronisch vorhandenen Daten (Löschkonzept).

5. Fotos

Eine Einverständniserklärung für Foto- und Filmaufnahmen wird eingeholt.

Ergebnis:

Bis auf die genannten Punkte ergab die Prüfung keine wesentlichen Beanstandungen.

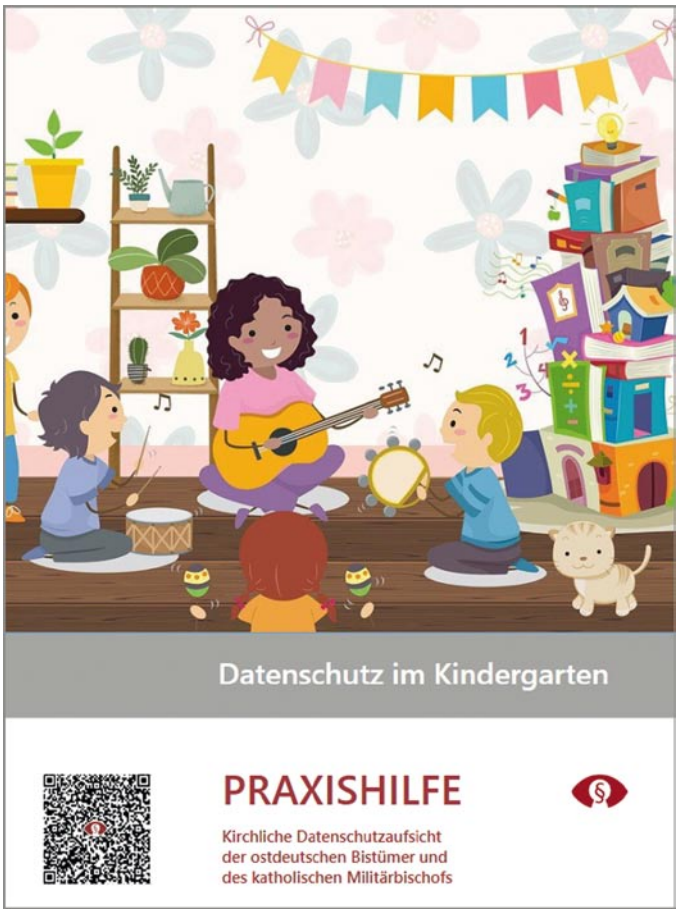
Die KDSA kam zu dem Ergebnis, dass die Bereitschaft zur Umsetzung der gesetzlichen Vorgaben zum Datenschutz vorhanden ist und auch erfolgt. Da in § 16 KDG-DVO geregelt ist, dass der Verantwortliche ein Datenschutzkonzept zu erstellen hat, ist diese Vorgabe umzusetzen. Gleiches gilt für die gem. § 31 KDG bestehende Verpflichtung zur Führung eines

Verzeichnisses von Verarbeitungstätigkeiten. Angeregt worden ist durch unsere Behörde, dass geklärt werden sollte wie und in welchen Abständen digital erhobene Daten gelöscht werden müssen.

Wir haben aufgegeben die Vorgaben bis zum 30.06.2025 zu erledigen

3.2 Praxishilfe für Kindergärten

Datenschutz im Kindergarten – davon sollen vor allem die Kinder -, aber auch die Sorgeberechtigten sowie auch die Beschäftigten profitieren. Für Kitaleitungen ist der Datenschutz oft ein notwendiges Übel, was mit den Interessen und Aufgaben der Kita, wie z.B. Dokumentieren und Beobachten des Kitaalltages oder Erbringen von Nachweisen für die Masernimpfung, nur schwer unter einen Hut zu bekommen ist.



Um Einrichtungen die Umsetzung der Erfordernisse aus dem Datenschutz zu erleichtern oder auch Sorgeberechtigten einen verständlichen Einblick in den Datenschutz zu geben, haben wir im Berichtsjahr 2024 eine Praxishilfe "Datenschutz im Kindergarten"[34] veröffentlicht.

Dieser Leitfaden soll Mitarbeitenden in Kindertageseinrichtungen vermitteln, warum Datenschutz wichtig ist und wie typische Abläufe in den Einrichtungen datenschutzkonform und praxistauglich umgesetzt werden können.

Musterformulare und Informationen zum Beschäftigtendatenschutz runden die Praxishilfe ab.

34 KDSA, https://www.kdsa-ost.de/images/CONTENT/INFOTHEK/Mpraxishilfen/dok/PH-KITA_Datenschutz_im_Kindergarten_1.0.pdf

3.3 Datenschutzvorfälle

Beim Erstellen und Versenden von E-Mails kann viel schieflaufen. So haben wir in den vergangenen Jahren mehrmals über dieses Thema berichtet. Die folgenden Vorfälle stehen exemplarisch für die Vielfältigkeit der Datenpannen allein beim Versand von E-Mails.

3.3.1 Vertauschter Bescheid an Kursteilnehmer

Ein Verwaltungsmitarbeiter einer Bildungseinrichtung hat eine E-Mail an eine zukünftige Kursteilnehmerin gesandt. Im Anhang der E-Mail sollte ein Bescheid dieser Teilnehmerin sein, den sie beim Kostenträger einreichen sollte. Beim Hinzufügen des Anhangs ist es jedoch zu einer Verwechselung gekommen, so dass nicht der Bescheid der Kursteilnehmerin enthalten war, sondern ein Bescheid einer anderen Kursteilnehmerin.

Die E-Mailempfängerin hat den Anhang direkt an den Kostenträger weitergeleitet, da sie davon ausging, dass es der richtige Anhang war. Dort ist der falsche Anhang sofort aufgefallen und die Kursteilnehmerin wurde entsprechend informiert. Die verantwortliche Stelle hat erst durch den Rücklauf des gesamten E-Mail-Verkehrs von der Verwechselung erfahren und den Vorfall anschließend bei uns gemeldet.

Wir haben daraufhin die verantwortliche Bildungseinrichtung gebeten, uns das Verfahren hinsichtlich dieser Datenverarbeitung zu beschreiben, um nachvollziehen zu können, an welcher Stelle die Datenschutzverletzung verursacht worden ist. Festgestellt wurde dabei, dass gem. § 7 Abs. 1 lit. f) KDG keine angemessene Sicherheit beim Versand personenbezogener Anhänge gewährleistet war. Im vorliegenden Fall gab es für jede Kursteilnehmerin einen Ordner auf dem PC des Mitarbeiters. Beide Ordner waren zum Zeitpunkt des Versendens der E-Mail geöffnet. Der Bescheid wurde in die geöffnete E-Mail eingefügt und nicht noch einmal auf Richtigkeit kontrolliert.

Um derartige Verwechselungen zu verhindern und die Sicherheit für den Versand von personenbezogenen Anhängen zu erhöhen, sollten die Verantwortlichen sicherstellen,

- dass der Anhang nach dem Einfügen und vor dem Versenden noch einmal verifiziert wird, ob Adressat des Anhangs und Adressat der E-Mail-Adresse übereinstimmen oder
- dass bei der Verarbeitung personenbezogener Daten jeweils nur ein Fall bzw. Ordner einer betroffenen Person bearbeitet werden darf, um zu verhindern, dass angefügte Dokumente vertauscht werden.

Zu vergessen sind in diesem Zusammenhang auch nicht die weiteren Sicherheitsmaßnahmen, die beim Versenden von personenbezogenen Daten per E-Mail einzuhalten sind (u.a. gesicherte Verbindung).

3.3.2 Liste mit sensiblen Daten

Eine Mitarbeiterin einer Beratungsstelle hat eine E-Mail an eine Empfängergruppe von 18 Personen versendet. Anlass der E-Mail war eine Einladung zu einem Elternstammtisch. Statt der Einladung war jedoch eine Liste mit teilweise sensiblen Daten anderer Familien enthalten. Das Versehen wurde kurz nach dem Versenden bemerkt, da eine Empfängerin der E-Mail den Verantwortlichen telefonisch von dem Versehen in Kenntnis gesetzt hat. Die Mitarbeiterin bat umgehend alle Empfänger die E-Mail mit der Adressliste zu löschen und bereits zur Kenntnis genommene Daten vertraulich zu behandeln. Der Vorfall wurde noch am selben Tag an uns gemeldet.

Wir haben daraufhin mit der Beratungsstelle Kontakt aufgenommen und diese gebeten uns bestehende Dienst- oder Handlungsanweisungen für das Versenden von E-Mails zur Verfügung zu stellen sowie die dabei angewendeten Sicherungsmechanismen zu beschreiben. Im Weiteren haben wir auch das Vorhandensein von Verpflichtungserklärungen der dort beschäftigten Mitarbeiter sowie Schulungsmaßnahmen zum Datenschutz überprüft.

Wir konnten feststellen, dass die Beratungsstelle sehr umfassende Regelungen zum Versand von E-Mails hat sowie alle Beschäftigten auf das Datengeheimnis verpflichtet und regelmäßig geschult worden sind.

Fazit:

Der Vorfall hätte jedoch verhindert werden können, wenn die Mitarbeiterin, wie im vorherigen Abschnitt bereits erwähnt, den Anhang vor dem Versand noch einmal auf dessen Richtigkeit überprüft hätte.

3.3.3 Offenlegung gegenüber Dritten

Ein Pfarrer hat eine E-Mail an mehrere Vertreter seiner Kommune einschließlich dem Bürgermeister, weitere Vertreter anderer Initiativen und einem betroffenen Gemeindemitglied gesendet. Alle E-Mailempfänger waren im An-Feld (offen) eingetragen. Das Gemeindemitglied hatte bereits vorher mehrfach mit dem Pfarrer in Gemeindeangelegenheiten per E-Mail, wohl über einen offenen Verteiler, kommuniziert. Doch Vorsicht, wenn zwei das Gleiche tun, ist es immer noch nicht dasselbe!

Vom verantwortlichen Pfarrer konnte keine gültige Einwilligungserklärung für die Nutzung der E-Mail-Adresse des Betroffenen für den beschriebenen Zweck und auch nicht für andere Zwecke vorgelegt werden.

Auch wenn der Betroffene selbst einen offenen Verteiler verwendet, so rechtfertigt dies nicht die Offenlegung der E-Mail-Adresse gegenüber einem anderen Verteilerkreis durch den Verantwortlichen. Mit der Bekanntgabe der eigenen E-Mailadresse, auch in einem offenen Verteiler, darf nicht darauf geschlossen werden, dass der Verantwortliche berechtigt ist, diese gegenüber Dritten offenzulegen.

Zudem war es in diesem Fall überhaupt nicht zweckdienlich, dass die Empfänger offengelegt wurden. Die Verarbeitung personenbezogener Daten, zu denen unstreitig auch E-Mailadressen gehören, muss nach § 7 Abs. 1 lit. c) KDG dem Zweck angemessen sowie auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein. Beides war hier nicht der Fall.

3.3.4 Offener E-Mail Verteiler – Dauerbrenner und bußgeldbewährt

Wie bereits in den letzten Jahren mehrfach berichtet, ist der offene E-Mail Verteiler ein Dauerbrenner. **Unangefochten ist dies die Datenpanne Nr.1.**

Egal ob Schulen die Nichterledigung von Aufgaben gegenüber mehreren Erziehungsberechtigten anmerken, Kindertagesstätten Informationsschreiben an die gesamte Elternschaft weiterleiten oder Pfarrgemeinde Informationen an Mitglieder versenden, dass Offenlegen der Mailadressen der Empfänger ist in den meisten Fällen nicht erforderlich. Regelmäßig ist bei derartigen Vorfällen ein Datenschutzverstoß festzustellen.

Für einige an uns gemeldete Verstöße, die einen offenen E-Mailverteiler betreffen, wäre eine Geldbuße geeignet und angemessen. Aufgrund der Regelung des § 51 Abs. 6 KDG ist jedoch die Verhängung von Geldbußen gegen kirchliche Stellen im Sinne des § 3 Abs. 1 KDG, soweit sie im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind, jedoch nicht möglich. Dies gilt jedoch nicht, soweit die Einrichtungen als Unternehmen am Wettbewerb teilnehmen.

Zudem können die Betroffenen auch einen Schadensersatzanspruch gegenüber der verantwortlichen Stelle nach festgestellter Datenschutzverletzung geltend machen.

4 Datenschutz im Gesundheitswesen

4.1 Elektronische Patientenakte für alle

Es ist wohl das größte IT-Projekt in Deutschland: die elektronische Patientenakte (ePA). Die elektronische Patientenakte (ePA) gibt es schon seit 2021. Allerdings wurde das Angebot bislang nur wenig genutzt. Das ändert sich nun durch einen Beschluss des Bundestags vom Dezember 2023: Ab dem 15. Januar 2025 soll für jeden gesetzlich Versicherten automatisch eine ePA angelegt werden, sofern Versicherte dem nicht aktiv widersprochen haben. Getestet wird die ePA aber vorerst an 250 Standorten in Hamburg, Franken und Teilen Nordrhein-Westfalens. Nach der Testphase soll sie stufenweise in ganz Deutschland eingeführt werden:

Arztbriefe, Befunde, E-Rezepte, Medikationspläne und Röntgenbilder sollen künftig zentral in der ePA gespeichert werden. Für Patienten heißt das: Jeder Arzt, der künftig aufgesucht wird, hat Einsicht in alle Diagnosen. Egal ob Haus- oder Facharzt. Damit sollen unnötige Mehrfachuntersuchungen

vermieden, schwere Krankheiten schneller erkannt und die Forschung vorangetrieben werden. Ärzte, Krankenhäuser und Apotheken sollen so vernetzt und relevante Informationen gesammelt zur Verfügung gestellt werden. Diese digitale Revolution im Gesundheitswesen verspricht zahlreiche Vorteile, wirft aber auch ernsthafte datenschutzrechtliche Bedenken auf.

Von den Patientinnen und Patienten selbst wird die ePA über eine App aufgerufen, die die jeweilige Krankenkasse zur Verfügung stellt. Ärztinnen und Ärzte stellen bestimmte Dokumente ein. Doch sie haben, genauso wie Apotheken, nicht automatisch Zugriff. Die Versicherten müssen die Daten freigeben.

Auch die Dauer des Zugriffs der einzelnen Zugriffsberechtigten kann über die ePA-App modifiziert werden. Weiterhin können Versicherte über ihre App bestimmte Dokumente, z. B. ausgewählte Befundberichte oder Arztbriefe, so einstellen, dass diese nur von ihnen selbst eingesehen werden können. Diese Einstellungen können aber nur vorgenommen werden, wenn Versicherte die ePA einrichten. Dies erfolgt über eine individuelle PIN, die bei der Krankenkasse beantragt werden muss. Die Beantragung kann in einer Filiale der Krankenkasse oder über den Weg des Post-Ident-Verfahrens erfolgen. Versicherte müssen ihre Identität mit einem Personalausweis oder Reisepass nachweisen.

Während sie erhebliche Vorteile für die Patientenversorgung verspricht, bleiben datenschutzrechtliche Bedenken bestehen. Gesundheitsdaten sind bedeutende personenbezogene Daten, welche besonders schützenswert sind.

1. Grundsätzliche datenschutzrechtliche Bedenken

Trotz der potenziellen Vorteile gibt es auch erhebliche grundsätzliche datenschutzrechtliche Bedenken, wie z. B.

- **Zentralisierte Datenspeicherung:** Die zentrale Speicherung sensibler Gesundheitsdaten erhöht das Risiko für Datenmissbrauch und Hackerangriffe.
- **Datenzugriff:** Obwohl Patienten theoretisch die Kontrolle über ihre Daten haben, bleibt die Frage, wie sicher diese vor unbefugtem Zugriff sind.

- **Opt-out statt Opt-in:** Die Umstellung auf ein Opt-out-Modell ab 2025 bedeutet, dass Patienten aktiv widersprechen müssen, wenn sie keine ePA wünschen. Dies könnte u. U. zu unbeabsichtigter Teilnahme führen.
- **Datennutzung für Forschungszwecke:** Ab 2025 sollen Versicherte die Möglichkeit haben, ihre Daten für Forschungszwecke zur Verfügung zu stellen. Hier stellen sich Fragen zur Anonymisierung und möglichem Missbrauch.
- **Technische Sicherheit:** Von entscheidender Bedeutung ist auch die Sicherheit der Telematikinfrastruktur. Betreiber müssen Störungen und Sicherheitsmängel unverzüglich melden, bei Versäumnissen drohen hohe Bußgelder.

Datenschutzbedenken äußerte u. a. der Berufsverband der Kinder- und Jugendärzt*innen (BKVJ). Der Chaos Computer Club (CCC) informierte auf dem Kongress in Hamburg im letzten Jahr über erneut aufgedeckte Sicherheitslücken.

2. Viele ungeklärte Fragen bei elektronischer Patientenakte von Kindern und Jugendlichen

Der BVKJ warnte bereits in seiner Pressemitteilung vom 11.12.2024 vor Problemen im Umgang mit der (ePA).[35] Er ist der Ansicht, dass etliche Fragen für den Praxisalltag im Zusammenhang mit der ePA-Nutzung durch Minderjährige von der Politik noch nicht gelöst worden sind.

Ab Anfang 2025 wird standardmäßig eine ePA für alle Bürger eingerichtet, die nicht ausdrücklich widersprochen haben bzw. widersprechen. Auch Kinder und Jugendliche bekommen eine ePA. Wenn Eltern keinen Einspruch erhoben haben, erhalten Kinder die ePA mit der Geburt. Ab einem Alter von 15 Jahren haben Jugendliche die volle Entscheidungsgewalt über ihre Akte.

Nach Ansicht des BVKJ ist bislang nicht geklärt, wie sich die Arztpraxen bei der „Befüllung der ePA“ verhalten sollen, wenn die Sorgeberechtigten unterschiedliche Wünsche äußern, was in der ePA ihrer Kinder gespeichert werden soll. Wer soll ein Widerspruchsrecht bzw. Löschungsrecht haben? Müssen diese von beiden Sorgeberechtigten zugestanden

35 https://www.bvkj.de/politik-und-presse/pressemitteilung/bvkj-ev-sieht-eine-reihe-ungeklaerter-fragen-bei-der-benutzung-der-epa-durch-kinder-und-jugendliche/

werden oder reicht es aus, wenn ein Sorgeberechtigter widerspricht? Kann dieser Widerspruch bzw. die Löschung von Daten in der ePA ggf. von Sorgeberechtigten gerichtlich eingefordert werden? Derartige Problematiken zeigen sich häufig bei sogenannten „hochstrittigen Eltern".

Ungeklärt ist die Frage der Zugriffsrechte, wenn Hauptversicherte nicht auch der Sorgeberechtigte sind. Ebenso ungeklärt: die Frage, wie die Einsichtsfähigkeit bei Jugendlichen festgestellt werden soll und wie die Rechte Dritter bei Einsicht in Dokumentationen geschützt werden sollen.

Vom BVKJ wird ferner kritisiert, dass die Befüllung der ePA von Kindern mit hochsensiblen Daten, die zu Stigmatisierung oder Diskriminierung führen könnten, für Ärzte verpflichtend ist, auch wenn diese überzeugt sind, dass dies nicht im Interesse des Kindes ist.

Problematisch sei darüber hinaus, dass Jugendliche unter 15 Jahren datenschutzrechtlich ihren Sorgeberechtigten gegenüber „bisher ungeschützt sind, auch wenn sie ein berechtigtes Interesse auf Nichtinformation der Sorgeberechtigten äußern". Der BVKJ verweist hierzu beispielhaft auf die Inanspruchnahme von Verhütungsberatung und die Verordnung von Verhütungsmitteln.

Weiter könnte es für Kinder und Jugendliche problematisch sein, wenn sie kritische Diagnosen in ihrer ePA mit in das Erwachsenenleben übernehmen, etwa bei Depressionen. „Die sensiblen Daten werden ohne Überprüfung ins Erwachsenenleben mitgenommen und können die Berufslaufbahn oder die Versicherung in der PKV, Haftpflicht etc. negativ beeinflussen.", so der BVKJ.

Michael Hubmann, Präsident des BVKJ, führt aus „Wir begrüßen eine moderne und funktionale digitale Patientenakte. Aber solange die von uns benannten Probleme nicht gelöst sind, werde ich Sorgeberechtigten und Patienten dazu raten, die Entscheidung über ihre Teilnahme an der ePA sorgsam abzuwägen".

3. Kritik des Chaos Computer Clubs (CCC)

Der CCC hatte sich bereits in der Vergangenheit kritisch hinsichtlich der Sicherheit der ePA geäußert. IT-Experten haben im Rahmen des 38. Chaos Communication Congress in Hamburg, einer Veranstaltung des CCC, eine

Analyse vorgestellt, die erneut Sicherheitslücken bei der ePA (Version 3.0) aufgedeckt hat.

Der Chaos Computer Club entdeckte im Dezember 2024 Lücken, durch die Angreifer mit gefälschtem Praxisausweis oder gefälschten Gesundheitskarten auf Gesundheitsdaten hätten zugreifen können. Diese Sicherheitslücken waren zum Beispiel möglich durch

- die unverschlüsselte Kartennummer auf der elektronischen Gesundheitskarte,
- Mängel im Kartenausgabeprozess für sogenannte Instituts- und Heilberufsausweise und
- den Erwerb gebrauchter Konnektoren. Das sind Geräte, die Zugang zur Infrastruktur des Gesundheitswesens gewähren.

Demonstriert wurde, wie es aufgrund von Mängeln in der Spezifikation möglich ist, Zugriffstoken für die ePA beliebiger Versicherter zu erstellen – und zwar ohne, dass die Gesundheitskarten präsentiert oder eingelesen werden müssen.

4. Auch die Ärzteschaft sorgt sich

Aufgrund der aufgedeckten Sicherheitslücken des CCC auf dem Jahreskongress sorgen sich auch Ärzte um den Schutz von Gesundheitsdaten in der ePA. Dies ergibt sich aus einem Bericht vom 07.01.2025 der Bundesärztekammer im Ärzteblatt (BÄK).[36]

Ende gut, alles gut?

Die Einführung der ePA stellt einen bedeutenden Schritt in der Digitalisierung des deutschen Gesundheitswesens dar. Während sie erhebliche Vorteile für die Patientenversorgung verspricht, bleiben datenschutzrechtliche Bedenken bestehen. Dabei ist auch immer wieder im Blick zu behalten, dass es sich bei den Gesundheitsdaten um bedeutende personenbezogene Daten handelt, welche besonders schützenswert sind.

Vor diesen Hintergründen ist den Versicherten zu empfehlen, für sich festzustellen, ob sich durch die ePA für sie ein persönlicher Vorteil ergibt, der die Inkaufnahme der datenschutzrechtlichen Unwägbarkeiten rechtfertigt.

36 https://www.aerzteblatt.de/nachrichten/156770/Aerzte-sorgen-sich-um-Datenschutz-bei-elektronischer-Patientenakte

4.2 Patientenrechte bei der elektronischen Patientenakte

Vertrags-, Zahn- und Krankenhausärzte ebenso wie Vertragspsychotherapeuten und Apotheken sind künftig zum Befüllen der ePA verpflichtet.

Das Grundprinzip ist dabei immer das gleiche: Unternimmt man nichts, wird eine ePA eingerichtet und genutzt. Ärzte, bei denen man in Behandlung ist, haben dann standartmäßig Zugriff auf alle Daten. Deshalb ist es wichtig, dass Patienten selbstbestimmt über ihre Gesundheitsdaten verfügen können. In der ePA ist dies vorwiegend über eine Reihe von Widerspruchsrechten geregelt. Man muss also aktiv tätig werden.

Wenn man einzelne sensible Informationen oder Diagnosen gegenüber Ärzten verbergen möchte, muss man abwägen von welchen Widerspruchsrechten man Gebrauch machen möchte, denn Rückschlüsse auf gesundheitliche Probleme oder Krankheiten sind oft nicht nur über Diagnosen oder Laborbefunde möglich, sondern auch über andere Daten.

Besonders sensible Daten in der ePA

Auch Daten, deren Bekanntwerden Anlass zu Diskriminierung oder Stigmatisierung des Versicherten geben kann, wie z. B. sexuell übertragbare Infektionen, psychische Erkrankungen und Schwangerschaftsabbrüche sollen grundsätzlich in der ePA gespeichert werden. Ärzte müssen Patienten in diesen Fällen aber explizit auf ihre Widerspruchsrechte hinweisen. Nach dem Widerspruch erfolgt keine Speicherung der Informationen in der ePA.

Wie diese Anforderung umzusetzen sind und wie dies im Alltag erfolgen wird (genügt ein einmaliger Widerspruch oder muss dieser jedes Mal erneuert werden) ist noch unklar. Zu klären bleibt zudem, wie die Kommunikation zwischen Ärzten und Patienten ablaufen soll.

Auch bei einem Widerspruch: Sensible Informationen können in der ePA landen, zum Beispiel über die Medikationsdaten oder die Abrechnungsdaten der Krankenkassen. Hier sind darüber hinaus gehende Widersprüche erforderlich.

Wo kann man widersprechen?

Es gibt es unterschiedliche Möglichkeiten zum Widerspruch:

- selbstständig in der ePA-App,
- bei der Krankenkasse,
- bei der Ombudsstelle der Krankenkasse.

Ombudsstellen sollen bei allen Fragen zur und Problemen mit der ePA helfen und sollen Patienten auch bei der Wahrnehmung ihrer Widerspruchsrechte unterstützen.

ePA-Widerspruch bei der Krankenkasse

Krankenkassen informieren derzeit ihre Versicherten über die „ePA für alle" und wie Versicherte widersprechen können.

Manche Krankenkassen haben ein Formular eingerichtet, mit dem Versicherte den Widerspruch online erledigen können (z.B. TK, DAK, BARMER, AOK). Zur Nutzung benötigt man z.B. bei der Barmer-Ersatzkasse die 5 letzten Ziffern der eGK sowie die PIN, die mit dem Informationsschreiben übermittelt wird.

Darüber hinaus ist auch ein Widerspruch per Post möglich oder Versicherte können eine Filiale ihrer Versicherung aufsuchen. Viele Krankenkassen stellen auf ihrer Interseite ein spezielles PDF-Formular zur Verfügung, welches heruntergeladen, ausgefüllt und an die Krankenkasse zurückgesandt werden kann.

Wie lange gilt der Widerspruch?

Ein Widerspruch gegen die Einrichtung der ePA kann jederzeit von den Versicherten zurückgenommen werden. Trotz zunächst erhobenem Widerspruch gegen die Einrichtung der ePA, ist eine spätere Einrichtung möglich.

Welche Widerspruchsrechte gibt es?

Eine gute Übersicht zu den Widerspruchsmöglichkeiten findet man auf der Webseite der Deutschen Aidshilfe.[37] Darauf hat die Datenschutzbeauftragte des Landes Sachsen-Anhalt hingewiesen.[38] Kurz zusammengefasst:

37 Deutsche Aidshilfe, https://www.aidshilfe.de/medien/md/epa/widerspruch-epa/
38 LfD Sachsen-Anhalt, https://datenschutz.sachsen-anhalt.de/landesbeauftragte/pressemitteilungen/pm-lfd-14012025

Gegenüber der Krankenkasse:

- dem Anlegen der ePA vor dem Start
- Auswertung und Information zu Gesundheitsrisiken durch Krankenkassen
- Einstellen von Abrechnungsdaten der Krankenkassen und in der ePA-APP

Gegenüber der Ombudsstelle und in der ePA-APP:

- Einstellen von Dokumenten durch Ärzte und Institutionen. Bei sexuell übertragbaren Infektionen, psychischen Erkrankungen, Schwangerschaftsabbrüchen müssen Ärzte aktiv auf das Widerspruchsrecht hinweisen.
- Zugriff einzelner Ärzte/ Institutionen auf die ePA
- Löschen oder Verbergen bestehender Dokumente
- Teilnahme am digitalen Medikationsprozess sowie Einstellen von Daten der E-Rezepte
- Sekundärdatennutzung zu Forschungszwecken

Möchte man seine ePA löschen lassen, beantragt man das bei seiner Krankenkasse oder in der ePA-APP.

4.3 Datenschutzvorfälle

4.3.1 Falsch versandte Patientenunterlagen

Wie auch in den vergangenen Berichtszeiträumen wurden uns in mehreren Fällen gemeldet, dass Entlassungsberichte, Arztbriefe, Rechnungen falsch versandt worden sind. Die Offenlegung erfolgte auch in diesen Fällen durch Übersendung an falsche Empfänger oder durch das Verbinden von nicht zusammengehörigen Unterlagen, wodurch Daten an unberechtigte Empfänger übermittelt worden sind.

Wieder haben wir festgestellt, dass in den meisten Fällen in den Einrichtungen entsprechende Datenschutzunterlagen vorhanden und die Verantwortlichen ihren Verpflichtungen gem. § 26 KDG nachgekommen waren.

Die Verstöße waren in der Regel auf Versäumnisse der Mitarbeiter zurückzuführen. Die Einrichtungen haben die Verstöße zum Anlass genommen die Mitarbeiter auf die Einhaltung der vorhandenen Regelungen zur Herausgabe und Übersendung von Unterlagen, die Gesundheitsdaten enthalten, zu schulen und entsprechend zu sensibilisieren.

In einigen Fällen wurden förmliche Beanstandungen ausgesprochen. Die Bescheide sind rechtskräftig.

4.3.2 Beschwerden wegen fehlender oder verspäteter Erfüllung von Auskunftsersuchen

Wir mussten auch im Jahr 2024 mussten wir feststellen, dass Auskunftsersuchen nicht mit der erforderlichen Sorgfalt bearbeitet werden.

Es kam vermehrt zu Beschwerden von Petenten, die angegeben hatten, ihr Auskunftsersuchen sei nicht oder erst verspätet erfüllt worden. Auch in diesem Berichtszeitraum waren nicht alle Beschwerden berechtigt. Es wurden jedoch auch Beanstandungen ausgesprochen.

Jeder hat das Recht zu erfahren, ob und welche personenbezogenen Daten über ihn verarbeitet werden. Gem. Art. 15 Abs. 1 DS-GVO (§ 17 Abs. 1 KDG) kann Auskunft über die verarbeiteten personenbezogenen Daten und nach Art. 15 Abs. 3 DS-GVO (§ 17 Abs. 3 KDG) zudem noch eine Kopie hiervon verlangt werden.

Kurz: Das Auskunftsrecht ist ein zentraler Bestandteil im Datenschutz. Es bedarf auch keiner Begründung zur Ausübung dieses Rechts.[39] Der Anspruch ist zudem unverzüglich (bedeutet ohne schuldhaftes Zögern), spätestens aber binnen Monatsfrist zu erfüllen. Nur aufgrund besonderer und dem Anspruchssteller binnen Monatsfrist mitgeteilter Umstände kann eine Beantwortung binnen drei Monaten erfolgen (Art. 12 Abs. 3 DS-GVO/§ 14 Abs. 3 KDG).

Die Nichterfüllung des Auskunftsrechts stellt eine datenschutzrechtliche Verletzung dar. Solche Verletzungen können neben Geldbußen auch individualrechtliche Entschädigungsansprüche auslösen, die neben materiellen Schäden auch immaterielle Einbußen umfassen (Art. 82 DS-GVO).

39 EuGH, Urteil vom 26.10.2023 - C-307/22

4.3.3 Herausgabe von medizinischen Unterlagen an unberechtigte Angehörige

Eine Mitarbeiterin eines Altenpflegezentrums hatte einen Medikamentenplan einer Bewohnerin an deren Angehörige herausgegeben, obwohl diese keine Vollmacht oder Betreuungsverfügung besaßen.

Medikamentenpläne enthalten personenbezogene Daten i. S. v. § 4 Nr. 1 KDG sowie personenbezogene Daten besonderer Kategorie i. S. v. § 4 Nr. 2 KDG. Die Bekanntgabe gegenüber Dritten stellt eine Verarbeitung (Offenlegung) i. S. v. § 4 Nr. 3 KDG dar.

Eine rechtmäßige Verarbeitung personenbezogener Daten ist gem. § 6 Abs. 1 KDG nur zulässig, wenn eine der dort genannten Bedingungen erfüllt ist. Gem. § 11 Abs. 1 KDG ist die Verarbeitung personenbezogener Daten der besonderen Kategorie nur erlaubt, wenn eine der in Abs. 2 dieser Vorschrift genannten Bedingungen zutrifft. Diese Voraussetzungen lagen nicht vor.

Neben der rechtmäßigen Verarbeitung müssen von der Verantwortlichen auch die Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Gem. § 7 Abs. 1 lit. f) KDG müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Es sind geeignete technische und organisatorische Maßnahmen zu treffen und einzuhalten, um die personenbezogenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung zu schützen. Insbesondere für die Verarbeitung besonderer Kategorie personenbezogener Daten, zu denen auch Angaben zu medizinischen Verordnungen gehören, sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 11 Abs. 4 KDG).

Die Anweisung der Einrichtung „Einsichtnahme Pflegedokumentation“ regelt, dass Angehörige nur Einsicht in die Pflegedokumentation nehmen dürfen, wenn eine entsprechende Vollmacht vorgelegt wird. An diese Anweisung hat sich die Mitarbeiterin nicht gehalten.

Gem. § 47 Abs. 1 KDG kann die kirchliche Datenschutzaufsicht förmlich feststellen, dass ein Datenschutzverstoß vorliegt. Davon haben wir Gebrauch gemacht. Die Feststellung ist geeignet und notwendig, um die Ver-

antwortliche nachhaltig zur Einhaltung des KDG anzuhalten.
Die Entscheidung, es bei der Feststellung des Verstoßes zu belassen und keine Sanktionen gem. § 47 Abs. 5, 6 KDG auszusprechen, beruhte auf dem Umstand, dass die Anweisung „Einsichtnahme Pflegedokumentation" regelt, dass Angehörige nur Einsicht in die Pflegedokumentation nehmen dürfen, wenn eine entsprechende Vollmacht vorgelegt wird. Regelungen zur Einsichtnahme sind mithin vorhanden.

Die Einrichtungsleitung hat die Mitarbeiter erneut auf die Einhaltung des Datenschutzes sensibilisiert.

4.4 Cyberattacken auf Krankenhäuser und Gesundheitseinrichtungen: Eine wachsende Bedrohung

Im Berichtsjahr haben wir eine zunehmende Anzahl von Cyberattacken auf Krankenhäuser und Gesundheitseinrichtungen beobachten können. Diese Attacken zielen darauf ab, die Datenbestände der Einrichtungen sowie die dazugehörigen Datensicherungen (Backup) zu sperren oder zu verschlüsseln und damit Kapital zu erpressen.

Die Auswirkungen solcher Attacken können katastrophal sein. Sie reichen von der Störung des Terminmanagements bis hin zur Beeinträchtigung der Patientenbehandlung. Ein geregelter Klinikablauf ist dann nicht mehr möglich. Die Patientenversorgung sowie sensible Patientendaten, die u.a. im Bedarfsfall verfügbar sein müssen, sind dann in akuter Gefahr.

Um derartige Vorfälle zu vermeiden oder zumindest im Schadensfall arbeitsfähig zu bleiben, können die Einrichtungen vorbeugende Maßnahmen ergreifen:

- Die IT-Infrastruktur und die IT-Technik regelmäßig überprüfen und ggfs. an die aktuellen Standards anpassen, Sicherheitsupdates zeitnah einspielen und unsichere Geräte austauschen.
- Mitarbeiter sensibilisieren, um sie auf die Bedrohungen durch Cyberattacken aufmerksam zu machen und sie zu befähigen, entsprechende Maßnahmen zu ergreifen.

- Gesetzliche Vorgaben, wie die neue EU-Richtlinie NIS2 und die Vorgaben aus dem SGB V, umsetzen, um die Sicherheit der IT-Systeme zu schärfen.
- Praxisnahe IT-Notfall Szenarien erarbeiten und üben, ähnlich wie bei einer Brandschutz-Übung.
- Empfehlungen der Sicherheitsbehörden folgen und auf Anwendbarkeit in der Einrichtung prüfen und ggfs. Maßnahmen nachschärfen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt regelmäßig Empfehlungen zur Absicherung, um die Einrichtungen bei der Umsetzung von Sicherheitsmaßnahmen zu unterstützen.

Fazit:

Es ist wichtig zu betonen, dass eine 100-prozentige Absicherung gegen Cyberattacken nicht möglich ist. Jedoch kann die Eintrittswahrscheinlichkeit reduziert und die Auswirkungen können minimiert werden, indem die oben genannten Maßnahmen umgesetzt werden. Durch eine Kombination von technischen, organisatorischen und personellen Maßnahmen können die Einrichtungen ihre IT-Systeme und Daten schützen und die Patientenversorgung sicherstellen.

Ein digitaler Einbruch erfolgt in der Regel in mehreren Stufen. Dabei spielt die Qualität der zur Verfügung stehenden Daten eine wichtige Rolle. Je qualifizierter das Datenmaterial ist, desto gezielter und schneller kann ein digitaler Einbruch zum Erfolg führen.

5 Datenschutz in Kita und Schule

5.1 Auskunftsersuchen in der Kita

5.1.1 Ein Fallbeispiel bei Kitawechsel

Der Anspruch auf Auskunft nach § 17 KDG als ein wichtiges Recht für Betroffene hat unsere Dienststelle im Berichtszeitraum nicht nur in den angebotenen Veranstaltungen und bisherigen Veröffentlichungen beschäftigt.

Die Beweggründe für Auskunftsersuchen können höchst unterschiedlicher Natur sein. Die Betroffenen müssen auch gegenüber den Verantwortlichen keine Gründe nennen, warum Sie Auskunft begehren. Zu beobachten ist, dass Betroffene ihre Rechte vermehrt wahrnehmen, die verantwortlichen Einrichtungen aber lieber Gründe suchen, warum sie dieser Pflicht nicht nachkommen müssen.

So begehrte eine Mutter von einer Kindertageseinrichtung alle Informationen, die ihr dort betreutes Kind betreffen. Vorrangig ging es der Mutter um alle Aufzeichnungen, Unterlagen und Dokumentationen zum Verhalten und zur Entwicklung ihres Kindes. Hintergrund war, dass das Kind demnächst in einer anderen Kindertageseinrichtung betreut werden sollte und man dieser Einrichtungen die angefertigten Dokumentationen und Beobachtungen zur Verfügung stellen wollte. Wie auch immer, Auskunftsersuchen müssen nicht begründet werden.

Der Mutter wurde daraufhin mitgeteilt, dass ihr nicht alle Unterlagen bzw. deren Inhalte ausgehändigt werden können. Begründet wurde dies damit, dass nicht alle Kopien der Unterlagen herausgegeben werden müssen. Daraufhin beschwerte sich die Mutter bei unserer Dienststelle, weil sie der Ansicht war, dass ihr die personenbezogenen Daten, die über ihr Kind von der Einrichtung verarbeitet werden, zustehen.

Wir haben daraufhin mit der Einrichtung Kontakt aufgenommen und unsere Rechtsauffassung dargelegt. Das Begehren der Mutter alle personenbezogenen Daten (Informationen) von ihrem Kind zu erhalten, die in der Einrichtung verarbeitet werden, muss erfüllt werden. Ob dabei auch Kopien der Dokumente oder Unterlagen zur Verfügung gestellt werden, muss die Einrichtung abwägen. Kopien können sinnvoll sein, um das Gesamtverständnis der verarbeiteten Daten zu erfassen. So ist es beispielsweise sinnvoll Entwicklungsdokumentationen oder Förderpläne zu kopieren, wenn diese nur das Kind betreffen. Wichtig ist, dass die Rechte Dritter dadurch nicht beeinträchtigt werden. Ggf. müssen dann Daten Dritter geschwärzt werden oder die Daten, die auskunftspflichtig sind, müssen dem Dokument entnommen und in einer anderen Form mitgeteilt werden.

Das Begehren der Mutter wurde nach unserer Kontaktaufnahme erfüllt.

Personenbezogene Daten eines Kindes finden sich in der Regel in folgenden Unterlagen der Kindertageseinrichtung:

- Vertragsunterlagen (Aufnahmeunterlagen, Kinderakte)
- Portfolios (auch in denen anderer Kinder)
- Entwicklungs- und/oder Lernstandsdokumentationen
- Förderpläne, auch Anträge oder Bescheide von Ämtern
- Anwesenheitslisten
- Unfallbücher / Protokolle
- Notfallkontakte
- Fotos

Es kann sich somit u.U. um ein sehr komplexes Verfahren handeln, bei dem gründlich gearbeitet werden muss. Daher ist es eventuell ratsam, bei den Sorgeberechtigten nachzufragen, welche Auskünfte sie begehren.

Der rechtliche Auskunftsanspruch stellt sowohl Einrichtungen, Organisationen, Unternehmen als auch Einzelpersonen immer wieder vor zahlreiche Herausforderungen und Fragen.

- Was muss ich alles herausgeben?
- In welcher Form muss ich die personenbezogenen Daten herausgeben?
- Gibt es eine einzuhaltende Frist?

Tipp: Ein Blick ins Gesetz, ein Gespräch mit Ihrem Datenschutzbeauftragten oder Informationen von der Datenschutzbehörde (Aufsicht) können Sie vor einem Bußgeld oder Schadenersatzansprüchen bewahren.

5.1.2 Besonderheit für Auskünfte an Eltern

Ein Auskunftsersuchen kann entweder von der betroffenen Person selbst oder durch eine von der betroffenen Person bevollmächtigten Person gestellt werden. Sorgeberechtigte Eltern oder Elternteile nehmen diese Rechte in der Regel für ihre minderjährigen Kinder war.

Es gibt aber bei Eltern, beispielsweise im Trennungsfall oder bei unverheirateten Elternpaaren, Besonderheiten, die beachtet werden müssen. So kann beispielsweise ein Kind zwar 2 Elternteile haben, wobei jedoch eines von ihnen nicht sorgeberechtigt ist. Diesem Elternteil darf dann keine Auskunft erteilt werden. Folglich darf nur dem Elternteil Auskunft erteilt werden, bei dem das Sorgerecht liegt.

Beispiel 1

Ein Vater verlangt von der Kindertageseinrichtung Auskunft über die personenbezogenen Daten seines Kindes. Mutter und Vater wohnen zusammen in einer Wohnung, sind aber nicht verheiratet. Bei der Geburt des Kindes wurde es versäumt eine gemeinsame Sorgerechtserklärung abzugeben.

Ergebnis: Dem Vater darf keine Auskunft erteilt werden! Es sei denn die Mutter hat zugestimmt. Dies sollte zu Beweiszwecken am besten schriftlich erfolgen.

Beispiel 2

Vater und Mutter eines Kindes haben sich getrennt. Vorher haben beide das gemeinsame Sorgerecht ausgeübt. Von keinem Elternteil wurde eine anderslautende Entscheidung vorgelegt.

Ergebnis: Beiden Elternteilen, Vater und Mutter, muss Auskunft erteilt werden!

Aufpassen: Nicht-Sorgeberechtigten ist keine Auskunft zu erteilen. Dies gilt auch für nahe Verwandte wie Großeltern, Tanten und Onkel.

5.2 Datenschutz in der Schule

5.2.1 Die Kommunikation des Schulelternrats

Die meisten Landesschulgesetze sowie auch die Schulordnungen der Freien und Kirchlichen Schulen verpflichten diese einen Schulelternrat einzurichten. Aufgabe dieses Gremiums soll die Mitwirkungsmöglichkeit der Erziehungsberechtigten an der Gestaltung des Schullebens sein. In der

Regel bestimmen die Erziehungsberechtigten einer Klasse einen Klassenelternvertreter. Die Klassenelternvertreter aller Klassen einer Schule bilden dann den Schulelternrat.

Der Schulelternrat (oder Elternbeirat) ist somit keine private Organisation oder ein Verein, sondern datenschutzrechtlich gesehen ein Teil der verantwortlichen Schule. Somit muss auch die Verarbeitung personenbezogener Daten der Betroffenen (Schüler, Eltern, Lehrkräfte) innerhalb des Schulelternrats, mit den Erziehungsberechtigen und mit der Schulleitung nach den Maßgaben der Datenschutzgesetze (KDG, DS-GVO) erfolgen.

Dies bedeutet für den Schulelternrat:

- Alle personenbezogenen Daten, die dem Schulelternrat im Rahmen seiner Tätigkeit zugänglich gemacht werden, dürfen nur für diese Arbeit verwendet werden.
- Die zugänglichen personenbezogenen Daten müssen vor unbefugtem Zugang oder Zugriff geschützt werden.
- Sobald die Daten nicht mehr gebraucht werden, sind diese zu löschen.

Die Arbeit im Schulelternrat erfordert aber auch einen regelmäßigen Austausch untereinander, mit den Eltern und mit den Lehrkräften. So teilt z.B. der Schulelternrat über die Klassenvertreter den Eltern die Entscheidungen mit, die dieser getroffen hat.

Doch wie kann diese Kommunikation datenschutzgerecht stattfinden?

Die Nutzung von Messengern bietet sich als schnelle und einfache Lösung an, doch müssen dabei auch die Anforderungen, die sich aus dem Datenschutz ergeben, erfüllt werden. Dazu gehören u. a.:

- Ende-zu-Ende-Verschlüsselung der Nachrichten und verschlüsselte Speicherung auf dem Endgerät und Server des Anbieters.
- Eine Nutzung sollte ohne Mobilfunknummer möglich sein.
- Die gespeicherten Kontakte (Adressbuch) auf dem Endgerät dürfen nicht ausgelesen werden.

- Nachrichten, Dateien und Kontakte müssen gelöscht werden können.
- Die Nutzerdaten dürfen nicht für Werbezwecke genutzt und auch nicht an andere Unternehmen weitergegeben werden.

Eine gute und datenschutzfreundliche Alternative kann auch die Nutzung einer datenschutzkonformen Schul-App sein. Schul-Apps haben gegenüber allgemeinen Messenger-Diensten den Vorteil, dass sich diese vom Verantwortlichen administrieren und verwalten lassen. So können einzelne Chat-Gruppen (Elternvertreter, Klassengruppen, Lehrer-Eltern) zur Kommunikation mit- oder untereinander voreingestellt werden. Eine Nutzung ist oft auch ohne Mobilfunknummer und geräteübergreifend möglich. Das Handling mit Dokumenten, die oft personenbezogene Daten enthalten, ist benutzerfreundlicher. Zudem kann eine Schul-App auch die E-Mailkommunikation ersetzen.

Schlussendlich ist aber auch von allen Beteiligten zu beachten, dass Eltern Messenger und Apps freiwillig nutzen können. Eine gesetzliche Verpflichtung besteht derzeitig nicht. Eltern, die dies nicht möchten, muss ein alternativer Kommunikationsweg ohne Nachteile eingeräumt werden.

5.2.2 Was lange währt wird endlich gut – Update aus 2020 inkl. Klärung weiterer Rechtsfragen

Rückblick

Bereits im Tätigkeitsbericht 2020 haben wir unter Punkt 5.3.3 über die Weiterleitung eines unzureichenden Attestes durch eine Schule an das zuständige Gesundheitsamt berichtet. Eine Schülerin hatte in diesem Corona-Jahr (2020) ein Attest in ihrer Schule vorgelegt, welches sie vom Tragen eines Mund-Nasen-Schutzes (Maske) befreien sollte. Das Attest enthielt keine weiteren Ausführungen zu den Gründen der Befreiung.

Da die Schule jedoch Zweifel an diesem Attest hatte, wurde dieses kopiert und ohne Kenntnis der Schülerin bzw. ihren Sorgeberechtigten an das Gesundheitsamt weitergeleitet.

Unsere Dienststelle sah in diesem Vorgehen einen Datenschutzverstoß und stellte fest, dass die Übermittlung der personenbezogenen Daten der

Schülerin ohne Rechtsgrundlage nach § 6 Abs. 1 KDG, § 11 Abs. 2 KDG erfolgt ist. Der verantwortlichen Schule bzw. dem Träger wurde im Februar 2021 eine Beanstandung mittels Bescheides durch unsere Behörde ausgesprochen. Im Weiteren wurde dem Verantwortlichen die Auflage erteilt, zukünftige Atteste zur Maskenbefreiung dem Gesundheitsamt nur noch anonymisiert vorzulegen.

Antrag auf Rechtsbehelf beim IDSG

Der Träger beantragte daraufhin beim Interdiözesanen Datenschutzgericht (IDSG) den Bescheid der Datenschutzaufsicht aufzuheben. Den Antrag begründete der Schulträger wie folgt:

Der Bescheid sei bereits formell rechtswidrig, da die Datenschutzaufsicht sachlich nicht zuständig sei. Die Übermittlung des Attestes sei weder eine automatisierte Verarbeitung noch eine nicht automatisierte Verarbeitung personenbezogener Daten gem. § 2 Abs. 1 KDG.

Der Bescheid sei zudem auch materiell rechtswidrig, da die Übermittlung des Attestes an das Gesundheitsamt durch die im KDG genannten Erlaubnistatbestände i. V. m. der damals maßgebenden Infektionsschutzverordnung gerechtfertigt sei.

Daraufhin erfolgte das übliche Prozedere. Beide Parteien, die Datenschutzaufsicht und der Schulträger, stellten ihre Rechtsauffassung dar und begründeten diese.

Bereits im Bescheid führten wir aus, dass es sich bei ärztlichen Attesten um personenbezogene Daten besonderer Kategorie (§ 4 Nr. 2, § 17 KDG) handelt, die besonders schützenswert sind. Eine Verarbeitung ist nur unter bestimmten Ausnahmen zulässig. Gründe, die eine Rechtmäßigkeit für das Kopieren und die Weiterleitung des Attestes an das Gesundheitsamt rechtfertigen könnten, lagen nach unserer Ansicht nicht vor. Auch in der damaligen maßgeblichen Corona-Verordnung konnte keine Legimitation für dieses Vorgehen gesehen werden.

Unsere Zuständigkeit sahen wir als begründet an, da es sich bei einem Attest um eine längerfristige Urkunde handelt, welche in die Schülerakte aufgenommen wird, was somit eine nicht automatisierte Verarbeitung per-

sonenbezogener Daten im Sinne des KDG darstellt. Das Kopieren stellt eine automatisierte Verarbeitung i. S. des KDG dar.

Im Oktober 2021 lagen die Antragsbegründungen beider Parteien dem Gericht vor. Eine zeitnahe Entscheidung, die zum damaligen Zeitpunkt im Hinblick auf mögliche ähnlich gelagerte Fälle hätte hilfreich sein können, erging leider nicht. Vielmehr hieß es ganz, ganz lange Warten.

Erst im Frühjahr 2024 wurden wir aufgefordert nochmals Stellung zu nehmen. Eine bis dahin nicht thematisierte Schulordnung, die jedoch maßgebend hätte sein können, wurde unserer Dienststelle vorlegt. Aber auch in der Schulordnung haben wir keine Regelung gefunden, die eine Weiterleitung des Attests an das Gesundheitsamt gerechtfertigt hätte. Nur nebenbei bemerkt: Die Schülerin hatte die Schule längst verlassen und Mund-Nasen-Bedeckungen spielten im Schulalltag schon lange keine Rolle mehr.

Die Entscheidung

Am 17.07.2024 erging nun endlich der Beschluss[40] in diesem Rechtsstreit mit folgendem Ergebnis:

Dem Antrag des Schulträgers den Bescheid der kirchlichen Datenschutzaufsicht aufzuheben wurde nur teilweise stattgegeben.

Durch das IDSG ist festgestellt worden, dass der Bescheid vom Februar 2021 formell rechtmäßig ist. Das Gericht sieht in dem Kopieren des Attestes und in der Weiterleitung an das Gesundheitsamt durch den Schulleiter Verarbeitungen personenbezogener Daten, die den sachlichen Anwendungsbereich des Kirchlichen Datenschutzes eröffnen.

Auch materiell ist der Bescheid nach Auffassung des Gerichts rechtmäßig. Das Gericht schloss sich unserem Standpunkt an, dass die Übermittlung des Attestes an das Gesundheitsamt ohne Rechtsgrundlage erfolgte und deshalb rechtswidrig war. Weder das KDG, noch die damals maßgebenden Infektionsschutzverordnung und auch nicht die Schulordnung des Trägers,

40 IDSG Bonn, Beschluss vom 17.07.2024 – IDSG 04/2021, https://www.dbk.de/fileadmin/user_upload/Beschluss_IDSG_04_2021_v._17.7.2024___Anonym._Fassung.pdf

enthielten Bestimmungen, mit der sich die Weiterleitung des Attestes an das Gesundheitsamt rechtfertigen ließe, so das Gericht.

Für die im Bescheid erteilte Auflage, zukünftige Atteste zur Maskenbefreiung dem Gesundheitsamt nur noch anonymisiert vorzulegen, sah das Gericht jedoch keine Deckelung durch das KDG. Nach § 47 Abs. 5 KDG kann der Bescheid der Datenschutzaufsicht Anordnungen enthalten, um einen rechtmäßigen Zustand wiederherzustellen oder Gefahren für personenbezogene Daten abzuwehren. Das Gericht vertritt die Ansicht, dass diese Auflage zu diesem Zweck nicht geeignet war. Es führte aus, dass ein Gesundheitsamt nur dann eingeschaltet werden dürfte, wenn sich die aufgeworfenen Zweifel durch das Hinzuziehen von diesem beantworten lassen. Dazu hatte der Schulträger jedoch keine Ausführungen gemacht.

Fazit:

Einrichtungen wie Schulen oder Kindergärten bzw. dessen Träger dürfen nur unter ganz engen Voraussetzungen personenbezogene Daten an das Gesundheitsamt übermitteln. Ein reiner Verdacht, dass ein Attest unzureichend ist, genügt auf jeden Fall nicht. Die Angaben auf Attesten oder gleichwertigen Bescheinigungen sind personenbezogene Daten besonderer Kategorie, für die eine Verarbeitung untersagt und nur in wenigen Ausnahmen erlaubt ist (§ 11 KDG). Das Gericht hat in keiner dieser Ausnahmereglungen eine legitime Weitergabe an das Gesundheitsamt gesehen.

Außerdem müssen die Einrichtungen auch genau prüfen, ob weitere Verordnungen (spezielle Schulordnungen des Trägers, Schutzverordnungen etc.) heranzuziehen sind. Die Voraussetzungen für amtsärztliche Schuluntersuchungen bzw. deren Anordnung werden in den entsprechenden Schulgesetzen oder -ordnungen geregelt und müssen demnach mitbeachtet und eingehalten werden.

Dieser Fall hat wie in vielen anderen Fällen gezeigt, dass gerade in der Corona-Pandemie die Verarbeitung personenbezogener Daten nicht immer zweck- und rechtmäßig sowie verhältnismäßig war. Gedankenlos wurden oft personenbezogene Daten besonderer Kategorie (Gesundheitsdaten) preisgegeben oder an unbefugte Dritte übermittelt.

5.3 Datenschutzvorfälle

5.3.1 Fotos auf Abwegen – nicht nur im Kindergarten

In einer Einrichtung - diesmal ein Hort und keine Kita – haben 2 Gruppen einen Ausflug gemacht. Um Eindrücke von diesem Ausflug festzuhalten wurde selbstverständlich die digitale Fotokamera mitgenommen. Jedoch ist der Einrichtungsleitung am nächsten Tag aufgefallen, dass die Fotokamera auf dem Ausflug verloren gegangen sein muss, da sie in der Einrichtung nicht auffindbar war.

Zum Zeitpunkt der Mitnahme befanden sich bereits 800 Bilder auf dem Speicher der Kamera. Dieser wurde letztmalig 2022 gelöscht. Die Einrichtungsleitung zögerte nicht lange und meldete umgehend den Vorfall. Auch unsere Behörde zögerte nicht lange und nahm diesen Vorfall zum Anlass einer anlassbezogenen Datenschutzüberprüfung.

Ziel dieser Überprüfung war die Verarbeitung von Fotos, die bereits mit der reinen Erstellung anfängt, genauer unter die Lupe zu nehmen. Zudem wollten wir auch sensibilisieren, da auf dem Speicher doch erheblich viele Bilder waren und die letztmalige Löschung mehr als 2 Jahre zurück lag.

Trotz des unschönen Vorfalls war die Einrichtung bezüglich der datenschutzrechtlichen Erfordernisse, die das Erstellen und Veröffentlichen von Fotos mit sich bringen, gut aufgestellt. Auch hat die Einrichtungsleitung den Vorfall genutzt, anlassbezogen zu sensibilisieren und neue Verfahrensweisen zu etablieren. So gibt es u.a. eine sehr umfangreiche Fotoeinwilligungserklärung mit auswählbaren Zwecken für die Veröffentlichung. Zudem wurden gruppenbezogene Listen erstellt, in denen für die Mitarbeitenden mit einem Kreuz erkennbar war, welches Kind für welche Zwecke fotografiert werden darf und welches nicht.

Nach dem Vorfall wurde den Mitarbeitenden ein Merkblatt übergeben, worauf sie beim Erstellen von Fotos, Mitführen und Auslesen von Kameras achten müssen. Auch gibt es einen Verantwortlichen, der die Bilder von den Kameras regelmäßig in eine sichere Datenablage überträgt und die Speicherkarten löscht.

Fazit:

Solange Fotos auf Speichermedien wie Speicherkarten oder USB-Sticks unverschlüsselt gespeichert werden, stellt dies ein Sicherheitsrisiko dar. Das Risiko muss durch technische oder organisatorische Maßnahmen minimiert werden, die Verarbeitung auf ein notwendiges Maß beschränkt sein. So ist es sinnvoll die Fotos von Speicherkarten in kurzen Abständen auf ein gesichertes Gerät zu übertragen und die Karten danach zu löschen.

Ein Restrisiko wird jedoch immer bleiben.

6 Datenschutz im Beschäftigungsverhältnis

6.1 Datenschutz bei Kirchenaustritten

6.1.1 Rückblick

Bereits in unserem Tätigkeitsbericht 2022[41] hatten wir darüber berichtet, dass das Bundesarbeitsgericht (BAG) dem Europäischen Gerichtshof (EuGH) in einem Vorabentscheidungsverfahren die Frage vorgelegt hat, ob ein der katholischen Kirche zugeordneter Arbeitgeber, Beschäftigte allein deshalb als ungeeignet ablehnen darf, weil sie aus der katholischen Kirche ausgetreten sind.[42]

Der Frage lag der Fall einer Hebamme zugrunde, die zunächst bei dem Arbeitgeber beschäftigt war und sich dann selbstständig machte. Im Zeitraum der Selbstständigkeit ist sie aus der katholischen Kirche ausgetreten. Dann bewarb sie sich erneut bei dem Arbeitgeber und wurde von diesem wiedereingestellt. In dem Personalbogen, den sie zusammen mit dem unterschriebenen Arbeitsvertrag abgab, hatte sie ihren Kirchenaustritt angegeben, der Arbeitgeber bemerkte dies jedoch zunächst nicht. Erst im Laufe der Probezeit wurde der Kirchenaustritt wahrgenommen, was im Ergebnis zur Kündigung der Arbeitnehmerin führte.

Nachdem das BAG den EuGH angerufen hatte, fand eine mündliche Verhandlung vor der Großen Kammer des EuGHs statt. Dort erkannte der Ar-

41 7. Tätigkeitsbericht 2022, Pkt.1.3.1, KDSA
42 BAG, Beschluss vom 21.07.2022 – 2 AZR 130/21

beitgeber an, dass das Arbeitsverhältnis mit der Klägerin durch die Kündigung nicht beendet worden sei.

Damit war der Rechtsstreit beendet und der EuGH musste (und durfte) über die Vorlagenfragen des BAG nicht mehr entscheiden.

Welche Bedeutung diese Fragen aber im Zusammenhang mit Arbeitsverhältnissen in der Kirche haben, wird nicht zuletzt daran deutlich, dass es nunmehr einen weiteren, gleichgelagerten Fall gibt, in dem das BAG ebenfalls wieder dem EuGH Fragen zur Vorabentscheidung vorgelegt hat.

6.1.2 „Nun sag', wie hast du's mit der Religion" II

Das BAG[43] fragt, ob es mit Unionsrecht vereinbar sei, wenn eine nationale Regelung vorsieht, dass eine private Organisation, deren Ethos auf religiösen Grundsätzen beruht, von ihren Beschäftigten verlangen kann, während des Arbeitsverhältnisses nicht aus einer bestimmten Kirche auszutreten, wenn sie von anderen Beschäftigten nicht verlangt, dieser Kirche anzugehören und die für sie arbeitende Person sich nicht öffentlich wahrnehmbar kirchenfeindlich betätigt.

Weiterhin fragt das BAG, ob ein Arbeitgeber den Fortbestand des Arbeitsverhältnisses davon abhängig machen darf, dass ausgetretene Beschäftigte der Kirche wieder beitreten.

Dem Vorlagenbeschluss lag diesmal der Fall einer Arbeitnehmerin zugrunde, die in einem Frauen- und Fachverband der katholischen Kirche arbeitet, zu dessen Aufgaben u. a. die Beratung von schwangeren Frauen gehört. Die Arbeitnehmerin erklärte, während ihrer Elternzeit im Oktober 2013 vor einer kommunalen Behörde ihren Austritt aus der katholischen Kirche. Der Arbeitgeber kündigte das Arbeitsverhältnis nach Beendigung der Elternzeit am 1. Juni 2019 außerordentlich ohne Einhaltung einer Frist, hilfsweise ordentlich zum 31. Dezember 2019. Zuvor hatte er erfolglos versucht, die Arbeitnehmerin zum Wiedereintritt in die katholische Kirche zu bewegen. Zum Zeitpunkt der Kündigung beschäftigte der Arbeitgeber neben vier katholischen auch zwei evangelische Arbeitnehmerinnen.

43 BAG, Beschluss vom 01.02.2024 - 2 AZR 196/22

Der Fall wird vor den staatlichen Gerichten verhandelt, weil er im kirchlichen Arbeitsverhältnis direkt arbeitsrechtliche Folgen entfaltet. Auch innerkirchlich gibt es dazu unterschiedliche Meinungen, wie im Tätigkeitsbericht 2022 dargestellt.

Wenn Beschäftigte dem Arbeitgeber ihren Kirchenaustritt freiwillig selbst mitteilen, beschränkt sich das Problem der Wirksamkeit einer demzufolge ausgesprochenen Kündigung auch auf arbeitsrechtliche Fragen.

Teilen Beschäftigte ihren Kirchenaustritt nicht selbst mit, ist eine Betrachtung aus datenschutzrechtlicher Sicht interessant.

6.1.3 Die (Nicht)-Kirchenmitgliedschaft im Blickwinkel des Datenschutzes

Auch wenn § 4 Nr. 2 KDG die Kirchenmitgliedschaft ausdrücklich von der Qualifikation als personenbezogenes Datum besonderer Kategorie ausnimmt, handelt es sich aber immer noch um ein personenbezogenes Datum gem. § 4 Nr. 1 KDG. Dieses darf nur dann verarbeitet werden, wenn es dafür eine rechtliche Grundlage gibt.

Nach § 53 Abs. 1 KDG dürfen

> *„personenbezogene Daten eines Beschäftigten einschließlich der Daten über die Religionszugehörigkeit, … für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist."*

Damit besteht grundsätzlich eine Rechtsgrundlage für die Verarbeitung dieses personenbezogenen Datums. Aus datenschutzrechtlicher Sicht stellt sich aber die Frage, wie Arbeitgeber vom Kirchenaustritt Beschäftigter erfahren (dürfen).

Gibt es eine Pflicht zur Mitteilung des Kirchenaustritts durch Beschäftigte selbst?

Arbeitnehmer sind verpflichtet, dem Arbeitgeber solche Umstände von sich selbst mitzuteilen, die sie daran hindern, ihre dienstvertraglichen Ver-

pflichtungen zu erfüllen. Ein Kraftfahrer, der seine Fahrerlaubnis verliert, muss dies dem Arbeitgeber mitteilen, weil er dadurch seine arbeitsvertraglichen Pflichten nicht mehr erfüllen kann. Andererseits sind als schwerbehindert anerkannte Beschäftigte nicht verpflichtet, diesen Umstand dem Arbeitgeber mitzuteilen, solange sie die arbeitsvertraglich geschuldete Leistung erfüllen können. Gleiches gilt für schwangere Beschäftigte.[44]

Gleiches muss auch für die Kirchenmitgliedschaft gelten. Wenn sich aus dem Arbeitsvertrag eine Verpflichtung ergibt, Mitglied der katholischen Kirche zu sein, wird eine Mitteilungsverpflichtung dann bestehen, wenn die Bedingung auf der Grundlage kirchenrechtlicher Regelungen rechtmäßig in den Vertrag aufgenommen worden ist. Das wäre der Fall, wenn es für die Erfüllung arbeitsvertraglicher Verpflichtungen erforderlich ist, katholisch zu sein. Dies ist unbestritten bei pastoralen und katechetischen Tätigkeiten der Fall[45] und bei Personen, die das katholische Profil der Einrichtung inhaltlich prägen, mitverantworten und nach außen repräsentieren.[46] Um die arbeitsvertraglich geschuldete Tätigkeit erfüllen zu können, ist in solchen Fällen die Mitgliedschaft in der katholischen Kirche unabdingbar. D. h. aber auch, dass solche Tätigkeiten konfessionslosen Personen oder solchen mit anderem Bekenntnis nicht übertragen werden können. Betraut der Arbeitgeber aber bekenntnislose oder Personen mit anderen Bekenntnissen mit einer Tätigkeit, macht er deutlich, dass die Mitgliedschaft in der katholischen Kirche nicht arbeitsvertraglich geschuldet wird. Beschäftigte können ihre arbeitsvertraglich geschuldete Leistung also erbringen, ohne Mitglied der Kirche zu sein. Damit besteht auch eine Offenbarungspflicht nicht.

6.1.4 Mitteilung des Kirchenaustritts durch die Gehaltsstelle

Bei der Einstellung von Beschäftigten werden die personenbezogenen Daten, die für die Gehaltsabrechnung erforderlich sind, manuell in das Stammblatt der Beschäftigten bzw. in das Abrechnungssystem übertragen. Sofern Bewerbende ihre Konfession angegeben haben, wird diese in

44 Ullrich, in: Beschäftigtendatenschutz der katholischen Kirche, Rn. 187 ff, 311 ff
45 Art. 4 Abs. 3 Grundordnung des kirchlichen Dienstes (GrO)
46 Art. 4 Abs. 4GrO

das Stammblatt übernommen. Die Kenntnis der Religionszugehörigkeit ist erforderlich für die Einbehaltung der Kirchensteuer durch den Arbeitgeber. Jedoch ist es seit Einführung des ELStAM-Verfahrens durch die Finanzämter nicht mehr erforderlich, dass Arbeitgeber die Religionszugehörigkeit abfragen. Liegen keine Angaben zur Religionszugehörigkeit von Beschäftigten vor, kann für das Abrechnungssystem „konfessionslos" angegeben und an das Finanzamt weitergemeldet werden. Sollte beim Finanzamt ein Religionsmerkmal hinterlegt sein, wird dieses über das ELStAM -Verfahren automatisch in die Gehaltsabrechnung eingepflegt. Die vorherige Angabe wird damit überschrieben. Zwar bekommt die Gehaltsabrechnungsstelle in diesem Fall eine namentliche Änderungsmitteilung vom Finanzamt, aus dieser geht aber nicht hervor, was sich konkret bei der benannten Person geändert hat. So verhält es sich auch, wenn Beschäftigte während des bestehenden Arbeitsverhältnisses aus der Kirche austreten. Auch in diesem Fall wird das Steuermerkmal vom Finanzamt geändert und automatisch über das ELStAM -Verfahren in das Gehaltsabrechnungssystem eingespielt. Auch hier geht aus der an die Gehaltsabrechnungsstelle übermittelten Änderungsmeldung nicht hervor, welche konkrete Änderung vorgenommen worden ist. Um dies zu erfahren müsste von den Beschäftigten der Gehaltsabrechnungsstelle direkt in die Abrechnung einzelner Mitarbeitenden Einsicht genommen werden.

Der Zweck der Übermittlung der Lohnsteuerabzugsmerkmale vom Finanzamt an den Arbeitgeber ist auf die Einbehaltung der Lohn- und Kirchensteuer beschränkt. Die Verwendung für andere Zwecke stellt eine Zweckänderung dar. Eine solche Zweckänderung müsste durch einen in § 6 Abs. 2 KDG genannten Grund gerechtfertigt sein.

In Betracht kommen könnte hier einzig eine Zweckänderung nach § 6 Abs. 2 lit. j) KDG. Danach ist die Verarbeitung für einen anderen Zweck rechtmäßig, wenn „der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert". Dieser Auffangtatbestand ist restriktiv anzuwenden.

Der Auftrag der Kirche wird nicht dadurch beeinträchtigt, dass im kirchlichen Dienstverhältnis jemand beschäftigt wird, der nicht der katholischen Kirche angehört, zumindest sofern auf vergleichbaren Positionen nicht oder anders konfessionelle Beschäftigte tätig sind oder sein können.

Es ist auch nicht ersichtlich, warum die Zweckänderung für die Glaubwürdigkeit des kirchlichen Dienstes erforderlich sein sollte. Wenn Beschäftigte ihren Kirchenaustritt „in aller Stille“ vollziehen, kann dies keinen Einfluss auf die Glaubwürdigkeit der Kirche oder ihres Dienstes haben, weil niemand davon weiß.

Wenn die Bischöflichen Erläuterungen in der Grundordnung des kirchlichen Dienstes (GrO) unter Art. 7 Rn. 5 feststellen,

> *„Mitarbeitende, die katholisch sind und während ihrer Tätigkeit bei einer katholischen Einrichtung aus der katholischen Kirche austreten, müssen sich fragen, ob sie weiterhin bei der Kirche arbeiten wollen.“*

stellt dies vielleicht die Glaubwürdigkeit und Konsequenz der Mitarbeitenden in Frage, aber nicht die der Kirche.

Falls der Arbeitgeber auf einem anderen rechtmäßigen Weg vom Austritt erfährt, mag es arbeitsrechtlich möglich sein, betreffende Beschäftigte zu kündigen. Insoweit wird die Regelung des Art. 7 GrO sowie die dazu ergangenen Bischöfliche Erläuterungen zum kirchlichen Dienst an dieser Stelle nicht infrage gestellt und die arbeitsrechtliche Wertung übernimmt der EuGH. Aus datenschutzrechtlicher Sicht ist aber eben nicht jedes Mittel geeignet, um den Sachverhalt eines möglichen Kirchenaustritts festzustellen. Dies gilt insbesondere dann, wenn für die Feststellung regelmäßig die Steuermerkmale aller Beschäftigten geprüft werden müssten, um Ausgetretene zu ermitteln.

Für die Nutzung dieser Daten für arbeitsrechtliche Maßnahmen fehlt deshalb eine Rechtfertigung nach dieser Vorschrift. Eine Zweckänderung ist deshalb nicht rechtmäßig.

Fazit:

Beschäftigte der Gehaltsstelle sind also nicht berechtigt, Daten, die vom Finanzamt für die korrekten Steuerberechnungen übermittelt worden sind, für arbeitsrechtliche Zwecke auszuwerten.

6.1.5 Mitteilung des Kirchenaustritts durch die Meldestelle

Ein Kirchenaustritt ist abhängig vom Bundesland vor dem Standesamt oder dem Amtsgericht zu erklären. Die jeweilige Behörde erteilt der staatlichen Meldebehörde sowie der Kirche, aus der ausgetreten worden ist, eine beglaubigte Abschrift der Austrittserklärung. Von der staatlichen Meldebehörde wird zusätzlich der Austritt automatisch in die Meldedatei des zuständigen Bistums übertragen. Der Zweck der Mitteilung besteht darin, dass die Kirche die Ausgetretenen aus ihrer Mitgliederdatei löschen kann. Die Mitteilung durch das Standesamt oder das Amtsgericht an die Kirche ist für diesen Zweck erforderlich. Insoweit ist auch hier eine Zweckbestimmung getroffen. Diese wird durch § 42 Abs. 1 Nr. 10 Bundesmeldegesetz (BMeldG) konkretisiert.

> *„(1) Die Meldebehörde darf einer öffentlich-rechtlichen Religionsgesellschaft … zur Erfüllung ihrer Aufgaben, nicht jedoch zu arbeitsrechtlichen Zwecken folgende Daten ihrer Mitglieder auch regelmäßig übermitteln:*
>
> *…*
>
> *10. rechtliche Zugehörigkeit zu der öffentlich-rechtlichen Religionsgesellschaft,“*

Beschäftigte der Meldestelle oder andere Beschäftigte, die von einem Kirchenaustritt durch Mitteilung eines Standesamtes oder eines Amtsgerichtes erfahren, dürfen diese Daten nicht an andere weitergeben, die damit eine dem ursprünglichen Zweck entgegenstehende Absicht, insbesondere arbeitsrechtliche Konsequenzen, verfolgen.

6.1.6 Anzeigepflicht durch den Beschäftigten – nur bei Bedarf

Beschäftigte sind nur dann verpflichtet, ihren eigenen Kirchenaustritt dem Arbeitgeber anzuzeigen, wenn die Mitgliedschaft in der katholischen Kirche für die Erfüllung der arbeitsvertraglichen Verpflichtungen zwingend erforderlich ist. Das ist zumindest dann nicht der Fall, wenn auf vergleich-

baren Positionen Personen beschäftigt sind, die der katholischen Kirche nicht angehören.

Die Gehaltsstellen erhalten Informationen von Finanzbehörden nur für ordnungsgemäße Berechnung und Abwicklung der Steuerpflicht. Eine Weitergabe dieser Daten für andere Zwecke ist untersagt

Die Kirchen erhalten Austrittsmitteilungen von Standesämtern oder Amtsgerichten nur für die Pflege ihrer Mitgliederlisten. Eine Verarbeitung dieser Daten für arbeitsrechtliche Zwecke ist ausgeschlossen.

Fazit:

Die Kirchenmitgliedschaft ist ein personenbezogenes Datum, welches gem. § 53 Abs. 1 KDG für Zwecke des Beschäftigungsverhältnisses grundsätzlich verarbeitet werden darf. Die Tatsache des Kirchenaustritts von Beschäftigten darf aber nur dann zu arbeitsrechtlichen Zwecken verarbeitet werden, wenn der Arbeitgeber die Information darüber auf rechtmäßigem Weg erlangt hat. Dies dürfte praktisch nur dann der Fall sein, wenn Beschäftigte diesen Sachverhalt selbst mitteilen.

6.2 Private Kontonummern von Beschäftigten

Im Berichtszeitraum hat uns ein Petent mitgeteilt, dass die Geschäftsleitung eines Verbandes einen möglichst bargeldlosen Geldverkehr innerhalb des Verbandes erreichen möchte. Alle Gelder sollten, so der Petent, als Vorschüsse an die Mitarbeiter überwiesen werden, wie z.B. die Bekleidungs- und Verpflegungsgelder einzelner Klienten. Geplant war, dass die Beschäftigten die Gelder für die Bezugsklienten beim Verband als Vorschuss beantragen und diese Gelder vom Verband auf die Privatkonten der Beschäftigten überwiesen werden.

Die Beschäftigten sollten die erhaltenen Gelder an die Klienten auszahlen bzw. sogar überweisen und am Ende des Monats dann eine Abrechnung erstellen und die Quittungen einreichen.

Bei der privaten Kontonummer von Beschäftigten handelt es sich um ein personenbezogenes Datum gem. § 4 Nr. 1 KDG. Ein solches personenbezo-

genes Datum darf nur verarbeitet werden, wenn einer der Gründe des § 6 Abs. 1 KDG dies rechtfertigt.

Die Angabe der privaten Kontonummer gegenüber der Arbeitgeberin ist erforderlich, um eine vertragliche Verpflichtung gem. § 6 Abs. 1 lit. c) KDG zu erfüllen. Sie ist auch erforderlich, um die Durchführung des Beschäftigungsverhältnisses zu gewährleisten.

Diese Erforderlichkeit bezieht sich aber darauf, Beschäftigten das für ihre Dienstleistung zustehende Entgelt zu überweisen. Die Erforderlichkeit bezieht sich ausschließlich auf diesen Zweck.

Wenn das private Konto von Beschäftigten zu anderen Zwecken verwendet werden soll, liegt in diesem Sachverhalt eine Zweckänderung, die nur rechtmäßig ist, wenn einer der Punkte des § 6 Abs. 2 KDG erfüllt ist. Eine Rechtfertigung durch einen der in § 6 Abs. 2 KDG genannten Gründe ist vorliegend nicht zu erkennen.

Die Nutzung der privaten Mitarbeiterkonten für die vom Verband verfolgten Zwecke wäre damit rechtswidrig.

Auch eine Einwilligung von Beschäftigten i. S. v. § 6 Abs. 2 lit. b) KDG käme für eine Rechtmäßigkeit nicht in Betracht.

Eine Einwilligung ist gem. § 4 Nr. 13 KDG eine freiwillig abgegebene Willenserklärung. Zwar kann im Beschäftigungskontext nicht generell davon ausgegangen werden, dass aufgrund des bestehenden Ungleichgewichts zwischen den Vertragspartnern eine Einwilligung nicht möglich ist, jedoch sind die Abhängigkeit von Beschäftigten sowie die Umstände des Einzelfalls besonders zu berücksichtigen. Eine Freiwilligkeit ist danach zu vermuten, wenn für die betroffene Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Beschäftigte gleichgelagerte Interessen haben.

Dies träfe vorliegend nicht zu.

Die vom Verband an die Beschäftigten ausgezahlten Gelder für die Klienten sind wie Fremdgeld zu behandeln. Dies führte dazu, dass im Falle einer Unterdeckung des Kontos nach der Rechtsprechung des BGH eine Vermö-

gensgefährdung i. S. v. § 266 StGB einträte. Beschäftigte wären deshalb in der freien Verfügbarkeit ihres Kontos eingeschränkt.

Auch wären Beschäftigte ggf. gezwungen, gegenüber dem Arbeitgeber ihre Vermögensverhältnis offenkundig zu machen. Damit wären sie verpflichtet, dem Arbeitgeber weitere personenbezogene Daten bekannt zu geben, für deren Verarbeitung der Arbeitgeber nicht berechtigt ist.

Ein rechtlicher oder wirtschaftlicher Vorteil für die Beschäftigten ist deshalb nicht zu erkennen.

Auch durch eine Einwilligung der Beschäftigten zu dem geschilderten Verfahren wäre eine Zweckänderung nicht zu rechtfertigen.

Der Verband hat uns in seiner Stellungnahme mitgeteilt, dass ein solches Vorgehen nicht eingeführt wird und man derzeit an anderen Lösungswegen arbeite. Ob dies auf unser Tätigwerden zurückzuführen war, blieb offen.

6.3 DS-GVO-Mindeststandards in Betriebsvereinbarungen

Betriebsvereinbarungen, mit denen Fragen zur Verarbeitung von Mitarbeiterdaten geregelt werden, müssen den Vorgaben der europäischen DS-GVO entsprechen und dürfen keine Umgehung der allgemeinen Datenschutzvorschriften bedeuten, entschied der EuGH am 19.12.2024.[47] Demnach ist der Spielraum für Arbeitgeber und Betriebsräte bei der Ausgestaltung von Datenschutz-Betriebsvereinbarungen sehr begrenzt.

Hintergrund: Eine Arbeitgeberin hatte auf Grundlage einer „Duldungs-Betriebsvereinbarung“ probeweise die cloudbasierte Software „Workday“ eingeführt. Ein betroffener Arbeitnehmer zog vor Gericht und machte Schadensersatz geltend. Er war der Meinung, dass die Betriebsvereinbarung keine ausreichende bzw. gültige Rechtsgrundlage für eine Datenverarbeitung gewesen sein könne. Das Bundesarbeitsgericht wandte sich an den Europäischen Gerichtshof (EuGH).

47 EuGH, Urteil vom 19.12.2024 -C-65/23

Entscheidungsgrundsätze des EuGHs

Rechtsgrundlage: Betriebsvereinbarungen können eine spezifische Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungskontext darstellen. Sie müssen jedoch die Anforderungen der DS-GVO erfüllen und dürfen keine Umgehung der allgemeinen Datenschutzvorschriften bewirken.

Vereinbarkeit mit der DS-GVO: Der EuGH stellte klar, dass nationale Rechtsvorschriften oder Kollektivvereinbarungen, die auf Art. 88 Abs. 1 DS-GVO basieren, nicht nur die Anforderungen von Art. 88 Abs. 2 DS-GVO erfüllen müssen, sondern auch die allgemeinen Bestimmungen der DS-GVO, insbesondere Art. 5, Art. 6 Abs. 1 sowie Art. 9 Abs. 1 und 2 DS-GVO. Betriebsvereinbarungen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungskontext müssen daher stets im Einklang mit den Grundsätzen der DS-GVO stehen.

Erforderlichkeit der Datenverarbeitung: Der EuGH räumt den Parteien einer Betriebsvereinbarung einen gewissen Spielraum bei der Beurteilung der Erforderlichkeit der Datenverarbeitung ein. Die Verarbeitung personenbezogener Daten muss dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sein. Durch die Betriebsvereinbarung muss gewährleistet sein, dass nur die für den jeweiligen Zweck erforderlichen Daten verarbeitet werden. Nicht-DS-GVO-konforme Datenverarbeitungen können nicht über eine „Betriebsvereinbarung“ legitimiert werden.

Gerichtliche Kontrolle: Der EuGH betont, dass die gerichtliche Kontrolle nicht eingeschränkt werden darf. Auch wenn die Datenverarbeitung auf einer Kollektivvereinbarung basiert, sind nationalen Gerichte verpflichtet, die Einhaltung aller Voraussetzungen und Grenzen der DS-GVO zu überprüfen. Die gerichtliche Kontrolle umfasst gänzlich auch die Erforderlichkeitserwägungen.

Fazit und Handlungsempfehlung:

Die Entscheidung des EuGHs ist nicht überraschend. Das EuGH-Urteil zeigt, dass Betriebsvereinbarungen nur eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten sein können, wenn sie den gesetzlichen Anforderungen entsprechen.

Unternehmen müssen sicherstellen, dass ihre Betriebsvereinbarungen der DS-GVO entsprechen und regelmäßig überprüft werden. Eine gründliche Prüfung auf datenschutzrechtliche Konformität ist unerlässlich. Unternehmen und Betriebsräte sollten eng mit Datenschutzexperten zusammenarbeiten, um die Rechte der Beschäftigten zu wahren.

6.4 Kein Beweisverwertungsverbot durch Betriebsvereinbarung

Können Betriebsparteien (Arbeitgeber/Mitarbeitervertretung) in einer Dienstvereinbarung ein Verwertungsverbot für Erkenntnisse festschreiben, die ein Arbeitgeber unter Verstoß datenschutzrechtlicher Vorschriften erlangt hat?

Das Bundesarbeitsgericht (BAG) hat den Betriebsparteien eine solche Regelungsmacht abgesprochen. Zuletzt hat das Gericht mit Urteil vom 29.06.2023[48] festgestellt, dass die Ausgestaltung des gerichtlichen Verfahrens, zu denen auch die Regelung von Beweisverboten gehört, allein dem Gesetzgeber zusteht. Die Arbeitsgerichte treffen diesbezügliche Entscheidungen nach Abwägung des Interesses des Arbeitgebers an der Verwertung und dem entgegenstehenden Interesse von Arbeitnehmern an der Nichtverwertung. Leitend geworden ist dabei die pointierte Aussage des BAG "Datenschutz ist kein Tatenschutz".[49] Damit wurde eine Verwertbarkeit regelmäßig bejaht.

Problematisch ist in diesem Zusammenhang, dass es sich hierbei um eine Auslegung von Vorgaben der DS-GVO handelt. Hierbei könnte durchaus Anlass bestehen, eine unionsrechtskonforme Auslegung des nationalen Prozessrechts zu prüfen bzw. durch den EuGH prüfen zu lassen. Das LAG Niedersachsen hat genau eine solche Notwendigkeit erkannt und dem EuGH sinngemäß folgende Fragen mit Vorlagenbeschluss vom 08.05.2024 vorgelegt.[50]

- Ob sich aus dem Unionsrecht (namentlich der EU-Grundrechtecharta und der DS-GVO) ein Beweisverwertungsverbot ergibt

48 BAG, Urteil vom 29.06.2023– 2 AZR 196/22
49 BAG, Urteil vom 23.08.2018 – 2 AZR 133/18
50 LAG Niedersachsen, Beschluss vom 08.05.2024 – 8 Sa 688/23

oder ob es dem nationalen Gesetzgeber obliegt, hierzu Regelungen zu treffen und

- ob ggf. eine Verwertung rechtswidrig erlangter Daten nur dann ausscheidet, wenn es sich um eine besonders schwerwiegende Verletzung datenschutzrechtlicher Vorschriften handelt oder
- ob ein Verwertungsverbot auch schon bei weniger schwerwiegenden datenschutzrechtlichen Verstößen anzunehmen ist.

Der im Oktober 2024 erschienene Referentenentwurf für ein Beschäftigtendatenschutzgesetz (BeschDG) sieht in § 11 ein Beweisverwertungsverbot vor. Gem. § 11 Abs. 2 des Entwurfs des BeschDG sollen Betriebsparteien selbst Verwertungsverbote in ihre Betriebsvereinbarungen aufnehmen können.

Die Frage der Verwertungsmöglichkeit von datenschutzwidrig erlangten Beweismitteln ist damit zunächst wieder offen. Entscheidet der EuGH, dass nationale Prozessvorschriften im Lichte der DS-GVO als europäische Norm auszulegen sind, dürfte dies künftig zu Beweisverwertungsverboten führen.

6.5 Datenschutzvorfälle

6.5.1 Kündigungsgrund am schwarzen Brett

In einer Kinderbetreuungseinrichtung wurde ein Mitarbeitender fristlos entlassen. Die fristlose Kündigung war das Ergebnis eines Fehlverhaltens, welches auch strafrechtliche Konsequenzen für den ehemaligen Beschäftigten nach sich zogen. Das strafrechtliche zu bewertende Verhalten resultierte jedoch nicht aus der Betreuung bzw. der pädagogischen Arbeit mit den Kindern.

Im Rahmen eines Elternvertretertreffens wurden diese von der Leitung über die Kündigung sowie die Umstände, die dazu führten, informiert. Im Weiteren wurde ein Protokoll über das Treffen und die besprochenen bzw. mitgeteilten Inhalte angefertigt und an den Infowänden in der Einrichtung ausgehängt. Eltern, Betreuer und Abholende wurde somit der Grund für die fristlose Kündigung des Beschäftigten offenbart.

Daraufhin hat sich der Beschäftigte bei uns beschwert. Unsere Dienststelle hat gleich mehrere Datenschutzverletzungen feststellen können. Bereits die Mitteilung des Kündigungsgrundes an die Elternvertreter war nicht erforderlich und damit unrechtmäßig. Es wäre nach unserer Auffassung ausreichend gewesen, die Elternvertreter darüber zu informieren, dass der Beschäftigte entlassen worden ist und die Entlassung nicht aus der Arbeit mit den Kindern resultierte.

Folglich war auch die Offenbarung des Kündigungsgrunds durch den Aushang des Protokolls nicht rechtmäßig, da nun auch die Eltern, Betreuer und Abholende über die Angelegenheit Bescheid wussten.

Letztendlich ist auch eine Meldung an die Datenschutzaufsicht bzw. an unsere Dienststelle unterblieben. Weder der Trägerverband, noch die Leitung sowie die anderen Mitarbeitenden der Einrichtung haben erkannt, dass die Offenbarung eines Kündigungsgrundes eines ehemaligen Mitarbeitenden eine Datenschutzverletzung darstellt.

Gegenüber der Verantwortlichen haben wir die Datenschutzverletzungen beanstandet und Auflagen zur Verbesserung des Datenschutzes ausgesprochen. Da es sich jedoch nicht um einen unerheblichen Verstoß handelte und der Betroffene dadurch erheblich diskreditiert worden ist, wurde auch eine Geldbuße im unteren vierstelligen Bereich verhängt.

Die verantwortliche Stelle hat im Nachgang den Vorfall zusammen mit uns aufgearbeitet und selbst erkannt, dass datenschutzrechtliche Mängel vorhanden sind. Bereits im Anhörungsverfahren sind Maßnahmen zur Verbesserung des Datenschutzes ergriffen und umgesetzt worden.

7 Technischer Datenschutz

7.1 „Firm-App“ – Datenschutzrechtliche Überprüfung lohnt sich

In einem Amtsblatt wurde auf eine neue „Firm-App“ des Bonifatiuswerkes hingewiesen, die ab Pfingsten 2023 in den Online-Stores verfügbar sein sollte.

Mit der Firm-APP soll die Firmvorbereitung deutlich erleichtert werden, hieß es in einer Pressemitteilung. Die App richtet sich in erster Linie an alle haupt- und ehrenamtlichen Mitarbeitenden in der Firmpastoral sowie an alle Firmbewerberinnen und Firmbewerber.

Die App bietet unter anderem eine Kommunikationsmöglichkeit mit den Firmgruppen, eine Kalenderfunktion, Gebete, umfangreiches katechetisches Material sowie Informationen zum Bonifatiuswerk und den Firmprojekten des Hilfswerks.

Die KDSA-Ost nahm diese Information zum Anlass diese Anwendung zu prüfen. Ähnlich wie bei einem Website-Check wurde eine allgemeine Datenverkehrs-Analyse (aus technischer Betrachtung) durchgeführt. Es ging dabei nicht primär um die Vollständigkeit und Rechtmäßigkeit von Verarbeitungszwecken.

Die Prüfaktion umfasste unter anderem auch den Einsatz von Cookies, Tracking-Tools sowie Datenübertragungen im Hinblick auf ihre Übereinstimmung mit den Informationspflichten.

Nach einer ersten Überprüfung im November 2023 wurden alle Bistümer aus dem Zuständigkeitsbereich der KDSA-Ost darüber informiert, dass eine Überprüfung der „Firm-App" ergeben hat, dass diese, zumindest in Teilen, den gesetzlichen Vorgaben nicht vollständig entspricht.

Auf das Ergebnis unserer Untersuchung der App wurde der Betreiber hingewiesen. Gleichzeitig wurde er aufgefordert, eine Nachbesserung vorzunehmen.

Im 2. Quartal 2024 haben wir eine erneute Überprüfung der im App-Store verfügbaren Version vorgenommen und sind zu dem Ergebnis gelangt, dass die Anwendung aus unserer Einschätzung noch nicht datenschutzkonform eingesetzt werden kann.

Ausschlaggebend für die Beurteilung war das Ergebnis einer erneuten Datenverkehrs-Analyse. Hierbei wurde festgestellt, dass in der überprüften Version Verbindungen zu „Drittanbieterhosts“ (ohne Wissen der Nutzer) hergestellt wurden. Es handelte sich um die Problematik, die u.a. auch bei Website-Überprüfungen auffällig ist.

Diese Analyse-Ergebnisse stellten wir dem Betreiber der Anwendung erneut zur Verfügung, der die App umgehend nachbesserte. Bei einer nochmaligen Datenverkehrs-Analyse konnten keine datenschutzrelevanten Auffälligkeiten festgestellt werden.

Die KDSA konnte somit „Grünes Licht“ für den Einsatz der Firm-App geben.

7.2 Messenger – und immer wieder gestellte Fragen

Es geht im folgenden Beitrag nicht um eine datenschutzrechtliche Betrachtung, sondern vielmehr um die Einordnung der Nutzung von Diensten zur Verteilung/Verbreitung von Informationen. Hier wird das Wort „Informationen“ absichtlich verwendet, weil es eine weitreichendere Bedeutung beinhaltet, als „nur“ personenbezogene Daten.

Immer wiederkehrende Fragen (und nicht nur bei uns), die gerne gestellt werden:

- Welchen Messanger können wir bedenkenlos nutzen?
- Können wir für unsere Kommunikation WhatsApp verwenden?

Bei diesen u. ä. Fragen machen es sich Anfragende oft einfach. Sie wünschen sich in der Regel eine „Flatrate-Antwort“, die auf alle ihre Belange passen soll. Bei Fragen nach einem Konzept, einem Verwendungszweck u. ä. bleiben die Antworten häufig vage.

Kurz vorweg: Auch im Berichtszeitraum konnte es von uns keine Empfehlung zur Nutzung von WhatsApp im betrieblichen Umfeld geben. Beispiele für alternative Lösungen wären: Communicare, Threema, Wire, Signal. Möchte man indes „Herr“ über seine Daten im eigenen Verantwortungsbereich bleiben, wäre eine eigene lokale Lösungen die beste Idee.

Wenn in diesem Abschnitt „Alternativen“ von Anwendungen oder Beispiele genannt werden, handelt es sich nicht automatisch um „Rundum Sorglos Empfehlungen“! Vielmehr soll damit lediglich deutlich gemacht werden, dass es durchaus alternative Möglichkeiten gibt. Jeder Verantwortliche ist hier selbst gefragt und in der Pflicht zu prüfen, ob die rechtlichen Anforderungen passen und die Anwendung mit seiner IT- und Informationssicherheits-Strategie konform ist.

Es gibt mehr oder weniger datenschutzfreundlichere Anwendungen. Unabhängig vom Dienst, auf den die Entscheidung fällt, sind rechtliche Aspekte wie Datenschutz und Informationssicherheit sowie die betrieblichen Anweisungen immer zu beachten.

Der Einsatz eines Messengers soll in der Regel eine schnelle und einfache Kommunikation ermöglichen, d. h. sofort Nachrichten zu senden und zu empfangen. Sie bieten u.a. die Möglichkeit, Gruppen zu erstellen, in denen mehrere Personen gleichzeitig kommunizieren können.

Es werden somit Informationen an Empfänger verteilt, die diese wiederum weiterverbreiten können. Das ist ähnlich wie mit einer E-Mail. Ein Mitarbeiter erhält auf sein betriebliches Postfach eine Nachricht. Diese möchte er zu Hause weiterbearbeiten und leitet sie an seine private E-Mail-Adresse weiter. Weil die Nachricht so interessant ist, sendet er sie von seinem privaten E-Mail-Account an weitere Personen. (Wir kennen bestimmt noch die Ketten-E-Mails bzw. die Oldschool-Kettenbriefe.)

In der folgenden Abbildung ist eine Einzel-/Gruppen-Kommunikation beispielhaft dargestellt. Eine Person sendet eine Nachricht (eine Information) an vier weitere Empfänger. Ab diesem Zeitpunkt sind die Daten in der Regel beim Empfänger auch lokal vorhanden und fließen ggf. in die jeweiligen Backupdienste. Wie diese dann mit der Information/den Daten umgehen, entzieht sich dem Einfluss des Versenders.

Das Weiterleiten von Nachrichten, wie E-Mails, Nachrichten von Messenger-Diensten (z. B. WhatsApp, Facebook Messenger), Sprachnachrichten ist „kinderleicht“ und schnell erledigt.

Der Absender der ursprünglichen Nachricht hat jedoch keine Kontrolle mehr über den Verbleib der darin enthaltenen Daten.

Wo sind meine Daten? Die korrekte Beantwortung dieser Frage kann u. U. schwer bis fast aussichtslos werden! Dies kann bei der Erfüllung eines Auskunftsersuchens durchaus zum Problem werden.

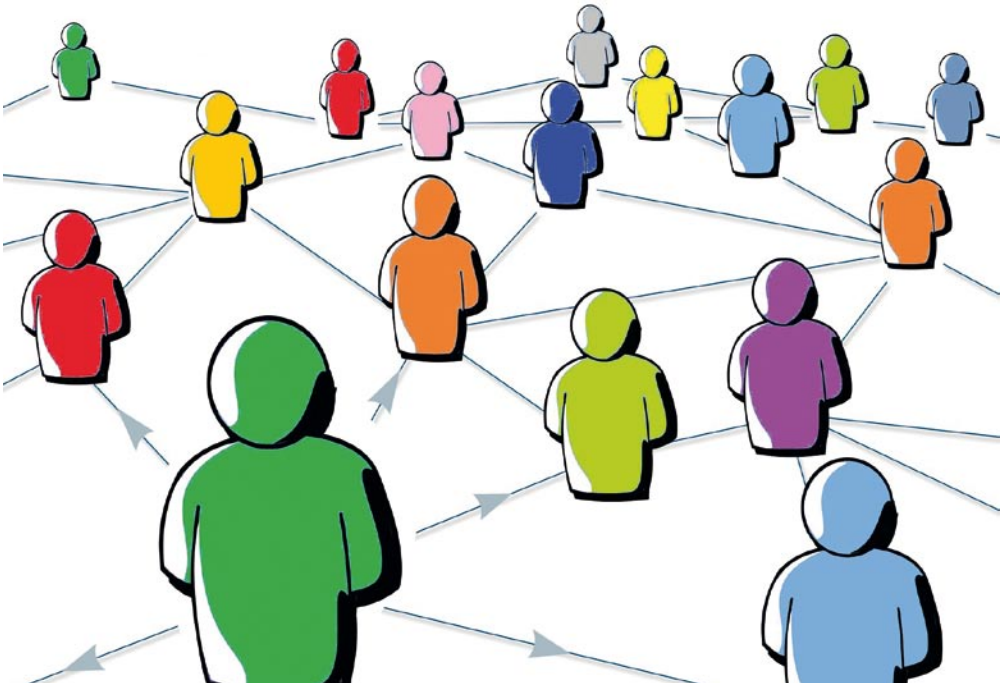
Scheidet eine Person aus dem Verteilerkreis aus, wie in der Abbildung gut erkennbar ist, ist diese Personen zwar nicht mehr an der Kommunikation beteiligt, aber noch immer im Besitz der bis dahin erhaltenen Daten.

Zusammenfassung:

Es gibt Anwendungen, die allen rechtlichen Anforderungen entsprechen. Ein Bruch der Informationssicherheitskette hängt nicht immer von der Anwendung ab. Datenpannen entstehen in der Regel bei der Nutzung solcher Systeme.

Der Verantwortliche kann sich nicht von seiner Verantwortung bezüglich der ihm anvertrauten Daten exkulpieren. Alle Rechte von Betroffenen sollten schon aus diesem Grund immer bei der Bewertung und der Auswahl einer Anwendung Berücksichtigung finden.

Generell gilt: Werden Daten, egal ob per E-Mail, per Messengerdienst etc. weitergeleitet, wird es schwierig den Verbleib und auch die Löschung von Daten, mit entsprechendem Nachweis, belegen zu können.



7.3 Zentraler Datenspeicher – Private Cloud

Ich hole mir meine Daten zurück – oder es muss nicht immer eine „Externe Cloud“ sein!

Aus dieser Idee heraus wird beispielhaft ein Systemvorschlag (Schemaplan) mit einer flexibel machbaren Varianten als „Denkanstoß/Architektur-Vorschlag“ für ein dediziertes zentrales System vorgestellt. Mit diesem können Standard-Dienste, wie Benutzerverwaltung, Chats, Kalender bis hin zum Dokumenten- und E-Mail-Archiv abgebildet werden. Zudem ist das System skalierbar und berücksichtigt Remote-Arbeitsplätze sowie dezentrale Standorte.

Abgrenzung: Es handelt sich grundsätzlich nur um ein Mustervorschlag ohne tiefgreifende Details zur Umsetzung und Konfiguration. Technische Details sind nicht Bestandteil der schematischen Darstellung (z.B. TIER, Netztrennung, etc.).

Die nachfolgenden Informationen beziehen sich auf die Abbildungen auf Seite 97: Zentraler Datenspeicher (A, B, C).

Ausgangslage

An einem Haupt- oder Nebenstandort arbeiten überwiegend (der Standard) Mitarbeitende mit betrieblichen Geräten in einem lokalen Netzwerk (meinlocal.lan). In der Regel handelt es sich bei den Arbeitsplätzen um Notebooks mit Dockingstation und Bildschirm, was eine höhere Flexibilität ermöglicht.

Der zentrale Datenserver (im Bild schwarzes Storage-System) ist die zentrale Stelle mit Benutzerverwaltung, Anwendungen, Datenfreigaben und dergleichen. Alle Daten befinden sich auf dem Datenserver und sind für den Betrieb (verantwortliche Stelle) verfügbar.

Variante (A)

Auf den betrieblichen Geräten (Arbeitsplatz) ist die entsprechende Software für die Erledigung der Arbeitsaufgaben eingerichtet.

Zusätzlich verfügen die Arbeitsplätze über ein VPN-Client. Damit ist ein „Remote Arbeiten“ von „Extern“ möglich. Voraussetzung dafür ist eine

Internetverbindung und eine Freischaltung/Genehmigung für Gerät und Mitarbeiter. Daten, welche lokal auf dem System bearbeitet werden, falls kein Internet vorhanden ist, könnten im Nachgang auf das zentrale System übertragen werden.

Variant (B)

Bei dieser Variante gibt es ein zusätzliches System für das „Arbeiten von Extern“ (Remote), den Terminalserver. Benötigte Anwendungen sind auf dem Terminalserver-System (TMS) eingerichtet.

Remote-Benutzer benötigen „nur“ einen VPN-Client, den sie je nach Freigabe auch auf „nicht“ betrieblichen Geräten einrichten könnten. Im Gegensatz zur Variante (A) sind die benötigten Anwendungen auf dem Terminalserver-System integriert und auf dem Remote-Arbeitsplatz nicht erforderlich.

Für die betrieblichen Aufgabenerfüllung wird eine VPN-Verbindung hergestellt, mit der eine Verbindung zum Terminalserver aufgebaut wird. Eine Datenverarbeitung inkl. E-Mail-Verkehr etc. verbleibt auf dem TMS. Der Remote-Arbeitsplatz verhält sich wie ein verlängerter Monitor mit Eingabegerät zur Bedienung des TMS.

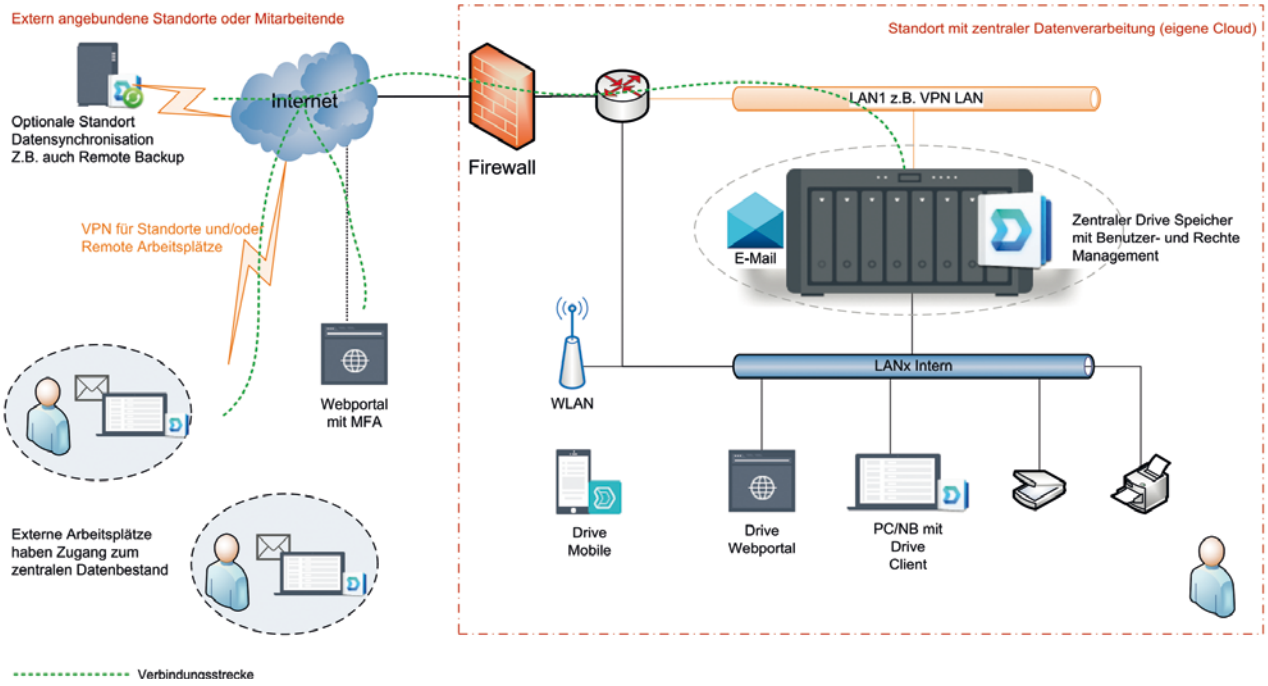
Variante (C)

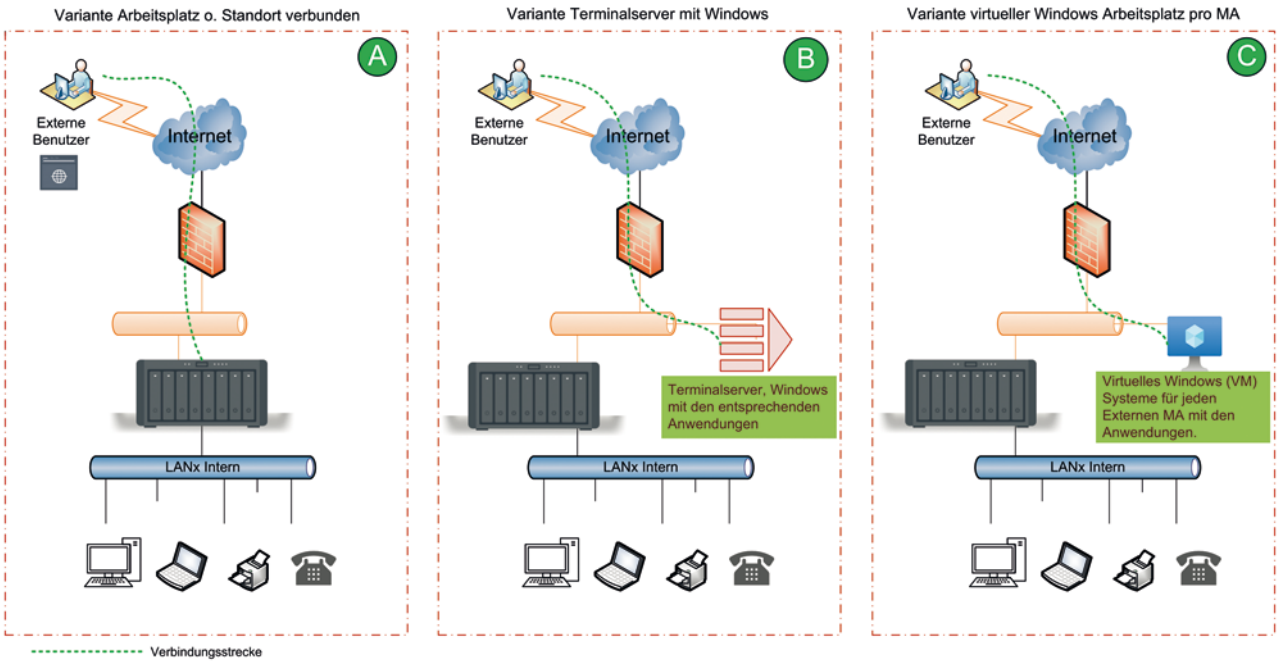
Bei dieser Variante gibt es ähnlich wie bei Variante (B) ein zusätzliches System, auf dem eigenständige virtuelle Arbeitsplätze betrieben werden können. Externe Mitarbeitende erhalten somit ihr eigenes virtuelles System mit den entsprechenden Anwendungen. Eine Verbindung wird wie bei Variante (B) hergestellt, mit der sich der Benutzer mit seinem virtuellen System verbindet.

Kurz zusammengefasst:

Technisch und organisatorisch müssen alle Systeme (Cloud, OnPrem, …) administriert werden. Die Verantwortlichkeiten können nicht ausgelagert werden. Das betrifft u.a. auch die Verantwortung für Datensicherungen und Verfügbarkeiten. Jede Variante hat je nach Einsatzzweck und benötigter Ressourcen seine Vorteile. Mit allen ist es möglich standortunabhängig und damit flexibel zu arbeiten.

Mit Variante (C) ist es am besten möglich einen Arbeitsplatz individuell zu gestalten. Man kann u.a. auch separate Wiederherstellungspunkte erstellen. Wird ein virtueller Arbeitsplatz nicht mehr benötigt, ist ein problemloses Entfernen möglich.



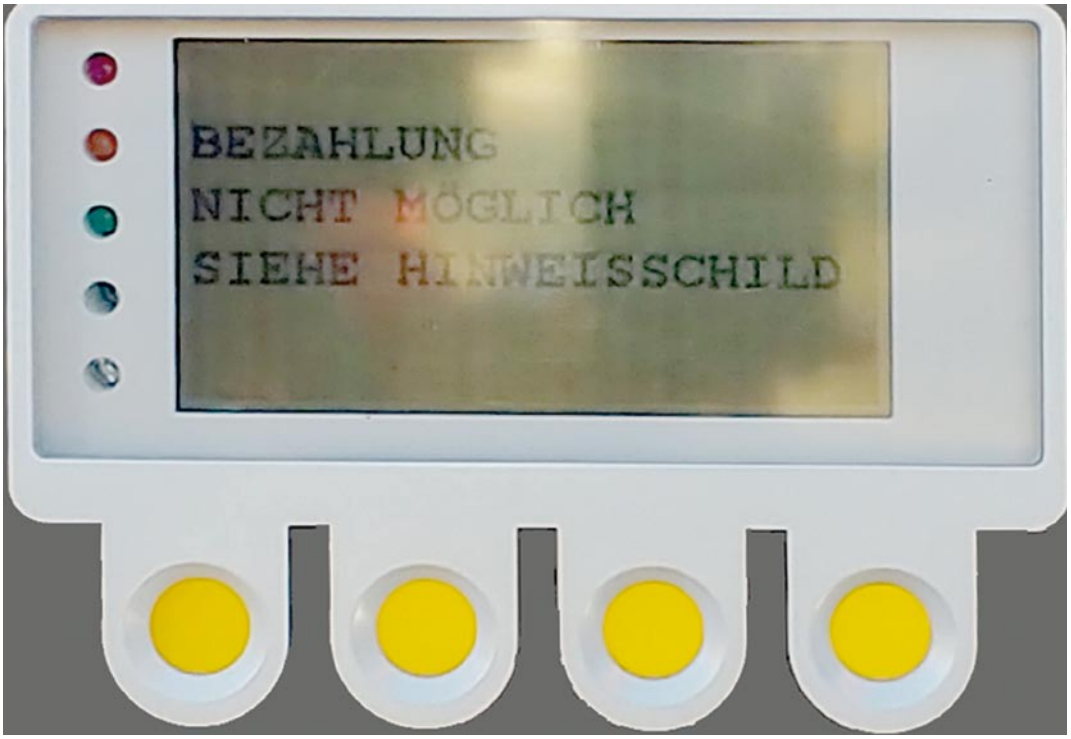


7.4 QR-Code – normale Bezahlung nicht möglich

In der heutigen digitalen Welt sind Cyberkriminalität und Betrug an der Tagesordnung. Eine der neuesten Methoden, die von Kriminellen verwendet wird, ist das sogenannte „Quishing“, eine Kombination aus „QR-Code“ und „Phishing“. Diese Methode wird zunehmend auch bei Parkautomaten eingesetzt und stellt eine ernsthafte Bedrohung für ahnungslose Nutzer dar.

Unser Tätigkeitsbericht 2023 enthält im Pkt. 7.2 den Beitrag „QR-Codes – Bequemlichkeit mit Tücken?“ allgemeine Informationen zu QR-Codes. Drei unterschiedliche Codes, statisch und dynamisch, sind dort abgebildet. An den Beispielen wurde u.a. die Funktionsweise erläutert und auf das Gefahrenpotential hingewiesen.

Obwohl Quishing gerade bei Parkautomaten ein bekanntes „Futter“ für Kriminelle ist, gibt es Betreiber von öffentlichen Parkplätzen, die den Parkplatz-Gästen keine andere Bezahlvariante anbieten, wie das Beispiel zeigt. Hier ist zu lesen „BEZAHLUNG NICHT MÖGLICH SIEHE HINWEISSCHILD“.



Der einzige Hinweis der zu sehen war, ist die Bezahlfunktion per App. Alle Bar-/ oder Kartenzahler sind in dem Fall von der Nutzung des Parkplatzes ausgeschlossen.

An solchen o.ä. Automaten ist schnell einmal der QR-Code mit einem Quishing-Code überklebt. Nutzer, die den Code scannen, landen dann auf einer Anwendung, die persönliche Bezahldaten abfischt (Phishing). Aber das ist noch nicht alles, denn sobald ein zuständiger Kontrolleur die Parkzeiten kontrolliert, erhält der abgefischte Parker noch einen Zahlungsbeleg für nicht bezahltes Parken.

7.4.1 Wie funktioniert Quishing bei Parkautomaten?

- **Manipulation des Parkautomaten:** Kriminelle bringen einen gefälschten QR-Code über dem echten QR-Code des Parkautomaten an. Dies kann durch einfache Aufkleber oder durch das Anbringen eines neuen Displays geschehen.
- **Scannen des QR-Codes:** Nutzer, die den QR-Code scannen, um ihre Parkgebühren zu bezahlen oder Informationen zu erhalten, werden auf eine gefälschte Webseite geleitet.
- **Eingabe persönlicher Daten:** Auf der gefälschten Website werden die Nutzer aufgefordert, ihre Zahlungsinformationen oder andere persönliche Daten einzugeben, oft unter dem Vorwand, dass dies zur Bearbeitung ihrer Zahlung erforderlich sei.
- **Datenmissbrauch:** Die gesammelten Daten werden dann von den Kriminellen verwendet, um finanzielle Transaktionen durchzuführen oder Identitätsdiebstahl zu begehen.

Risiken und Folgen

Die Risiken, die mit Quishing verbunden sind, sind erheblich. Nutzer können nicht nur Geld verlieren, sondern auch Opfer von Identitätsdiebstahl

werden. Darüber hinaus kann das Vertrauen in digitale Zahlungsmethoden und die Nutzung von Parkautomaten beeinträchtigt werden, was zu einem Rückgang der Nutzung solcher Systeme führen kann.

Schutzmaßnahmen

Um sich vor Quishing zu schützen, sollten Nutzer folgende Vorsichtsmaßnahmen beachten:

- **Überprüfen Sie die QR-Codes:** Achten Sie darauf, ob der QR-Code unbeschädigt oder manipuliert aussieht. Wenn Sie Zweifel haben, verwenden Sie die offizielle App oder Website des Parkdienstes.
- **Verwenden Sie sichere Zahlungsmethoden:** Nutzen Sie Zahlungsmethoden, die zusätzlichen Schutz bieten, wie z.B. digitale Wallets oder Kreditkarten mit Betrugsschutz.
- **Melden Sie verdächtige Aktivitäten:** Wenn Sie einen verdächtigen QR-Code oder eine betrügerische Website entdecken, melden Sie dies umgehend den zuständigen Behörden oder dem Parkdienstleister.

Fazit:

Quishing ist eine ernsthafte Bedrohung, die Nutzer von Parkautomaten und anderen digitalen Zahlungsmethoden betrifft. Durch Aufklärung und Vorsicht können Nutzer jedoch das Risiko, Opfer eines solchen Betrugs zu werden, erheblich reduzieren. Es ist wichtig, wachsam zu bleiben und sich der potenziellen Gefahren bewusst zu sein, um sicher und geschützt zu bleiben.

Hier können Sie selbst noch einmal die drei unterschiedlichen QR-Codes aus unserem Tätigkeitsbericht 2023 (Pkt.7.2) probieren: https://www.kdsa-ost.de/aktuelles/qr-codes-echt-oder-quishing.html .

7.5 Wer auf den Schutz seiner Daten achtet, zahlt drauf

Das Thema Datenschutz gewinnt heutzutage in der digitalen Welt immer mehr an Bedeutung. Viele Menschen sind sich aber auch der Risiken bewusst, die mit der Nutzung von Einkaufs-Apps und anderen digitalen Diensten verbunden sind. Ein Verzicht, gerade auf die immer stärker beworbenen Einkaufs-Apps, kann u.U. zu finanziellen Nachteilen führen.

Welche Vorzüge bieten Einkaufs-Apps?

Einkaufs-Apps bieten zahlreiche Vorteile, die für viele Nutzer attraktiv sind:

- Bequemlichkeit: Nutzer können bequem von zu Hause aus einkaufen, ohne in Geschäfte gehen zu müssen. Dies spart Zeit und Aufwand.
- Rabatte und Angebote: Viele Apps bieten exklusive Rabatte, Sonderaktionen und Treueprogramme, die es den Nutzern ermöglichen, Geld zu sparen.
- Personalisierte Empfehlungen: Einkaufs-Apps nutzen Algorithmen, um personalisierte Produktempfehlungen zu geben, die auf den Vorlieben und dem Kaufverhalten der Nutzer basieren.
- Einfache Preisvergleiche: Nutzer können Preise schnell vergleichen und die besten Angebote finden, was zu Einsparungen führen kann.

Demgegenüber stehen Datenschutzbedenken.

Auf der anderen Seite gibt es berechtigte Bedenken hinsichtlich zum Schutz der persönlichen Daten:

- Risiko des Datenmissbrauchs: Einkaufs-Apps sammeln oft eine Vielzahl von Daten, einschließlich persönlicher Informationen, Kaufhistorie und Standortdaten. Diese Daten können missbraucht oder ohne Zustimmung weitergegeben werden (freiwillige Überwachung).
- Zielgerichtete Werbung: Die gesammelten Daten werden häufig verwendet, um zielgerichtete Werbung zu schalten, was für viele Nutzer als invasiv empfunden wird.

- Sicherheitsrisiken: Es besteht das Risiko von Datenlecks und Cyberangriffen, bei denen persönliche Informationen in die falschen Hände geraten können.
- Kontrollverlust: Es kann zu einem Kontrollverlust aller bis dahin übermittelten Daten führen.

Fazit:

Die Entscheidung, Einkaufs-Apps zu nutzen oder darauf zu verzichten, ist oft ein Balanceakt zwischen den Vorteilen, die sie bieten, und den Bedenken hinsichtlich der Herausgabe der persönlichen Daten. Einige Nutzer entscheiden sich bewusst gegen die Nutzung dieser Apps, um ihre Daten zu schützen, während andere bereit sind, persönliche Informationen preiszugeben, um von den finanziellen Vorteilen zu profitieren.

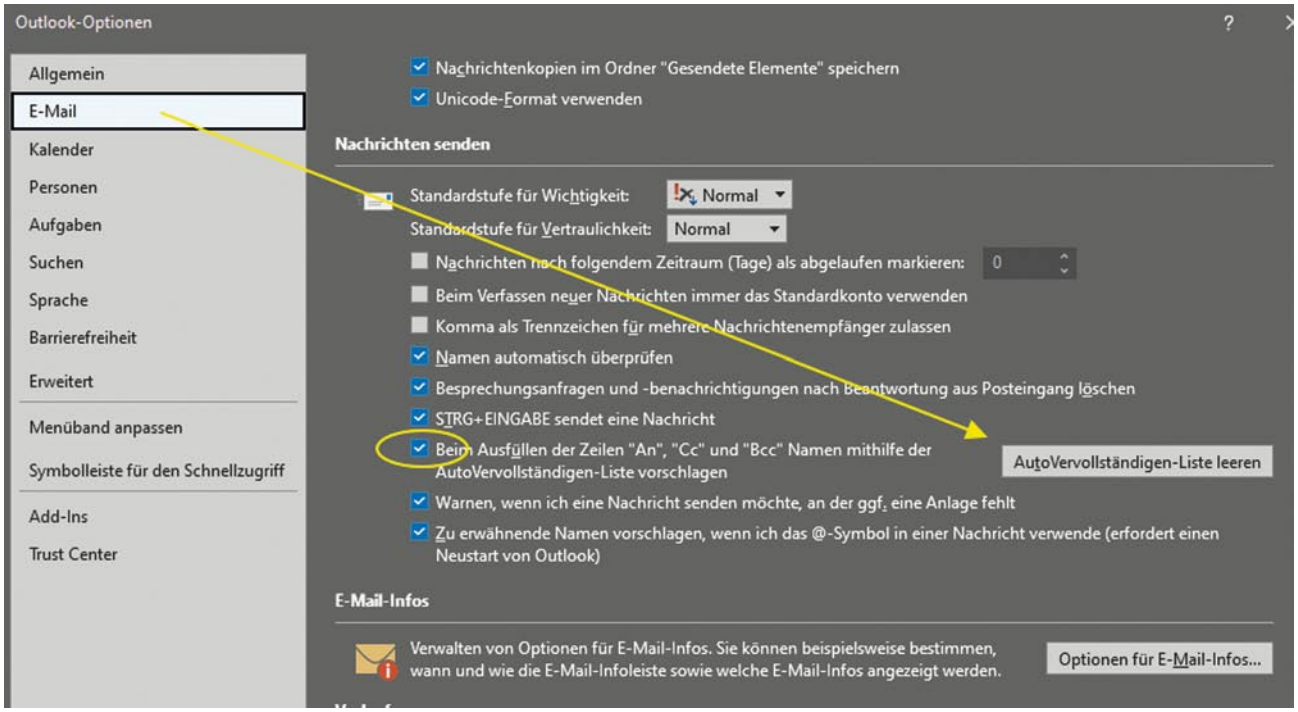
Zwang oder Vorteil? Nutzer ohne die entsprechenden Geräte kommen erst gar nicht in den Genuss oder die Verlegenheit, solche Einkaufs-Apps zu nutzen und die rabattierten Preise zu erhalten.

7.6 Outlook und die automatische E-Mail-Vervollständigung

Outlook bietet eine praktische Funktion zur automatischen E-Mail-Vervollständigung, die den Nutzern hilft, schneller und effizienter zu kommunizieren. Wenn Sie eine neue E-Mail verfassen und mit der Eingabe einer E-Mail-Adresse beginnen, schlägt Outlook automatisch Kontakte vor, die in Ihrem Adressbuch gespeichert sind oder die Sie zuvor kontaktiert haben. Die automatische Vervollständigung basiert auf dem bisherigen E-Mail-Verlauf.

Mit der Zeit wird diese Verlaufsliste immer länger. Nicht mehr aktuelle Empfänger werden dabei immer wieder vorgeschlagen. Des Weiteren kann es beim Tippen der Empfänger schnell zu Verwechslungen mit der Folge kommen, dass falsche Empfänger ausgewählt werden und diese Nachrichten erhalten, die nicht für sie bestimmt sind, was im weiteren Verlauf zu einer Datenpanne führen kann.

Tipp: Im Laufe der Zeit kann es durchaus sinnvoll sein, den Adressen-Verlauf hin und wieder zu löschen. Die entsprechende Option ist unter „Datei – Optionen und E-Mail“ zu finden.



7.7 Praxistipps für datenschutzkonformes Schwärzen

Gerade im Rahmen von Auskunftsersuchen in Verbindung mit der Forderung auf Erhalt einer Datenkopie nach § 17 Abs. 3 KDG bzw. Art. 15 Abs. 3 DS-GVO stehen Verantwortliche häufig vor der Frage, wie sie die personenbezogenen Daten Dritter, die in den herauszugebenden Unterlagen enthalten sind, datenschutzkonform entfernen bzw. unkenntlich machen können. Das Entfernen oder Unkenntlich machen ist insbesondere vor dem Hintergrund relevant, dass nach der weiten Auffassung zum Begriff der Datenkopie, sämtliche Schriftstücke herauszugeben sind, die einen Bezug zur auskunftssuchenden Person aufweisen. Die entsprechenden Stellen werden dann häufig geschwärzt.

Beim „Schwärzen" handelt es sich um eine Maßnahme des technischen und organisatorischen Datenschutzes. Dabei können Verantwortlichen gelegentlich Fehler unterlaufen, wodurch Persönlichkeitsrechte der Betroffenen verletzt werden können. Der Verantwortliche ist dann in der Pflicht – sofern schützenswerte personenbezogene Daten offenbart werden – die Datenpanne gemäß § 33 KDG (Art. 33 DS-GVO) der zuständigen Aufsichtsbehörde zu melden.

Damit es gar nicht erst zu Verstößen kommt, sollten Beschäftigte, die mit Schwärzungen und der Veröffentlichung bzw. Herausgabe von Dokumenten betraut sind, über mögliche Fehlerquellen und Lösungen informiert sein.

PDF- und Office-Datei trotz Schwärzung vollständig lesbar

Viele PDF- und Office-Anwendungen bieten die Möglichkeit, Textstellen schwarz zu markieren oder mit Formen abzudecken, z. B. mit einem intransparenten farbigen Balken. Überdeckt ist aber nicht gleich anonymisiert, Textpassagen sind häufig weiterhin vollständig auslesbar. Nutzende müssen dazu nur die vermeintlich geschwärzten Inhalte aus der Datei markieren und in einen Texteditor kopieren und schon ist alles wieder lesbar. Wichtig ist daher, dass Daten nicht nur optisch, sondern auch technisch tatsächlich entfernt werden.

Fehler vermeiden

Bevor mit dem Schwärzen begonnen wird, ist es ratsam, eine Sicherungskopie der Datei zu erstellen, um notfalls weiterhin auf das Original zurückgreifen zu können.

Digitale Schwärzung

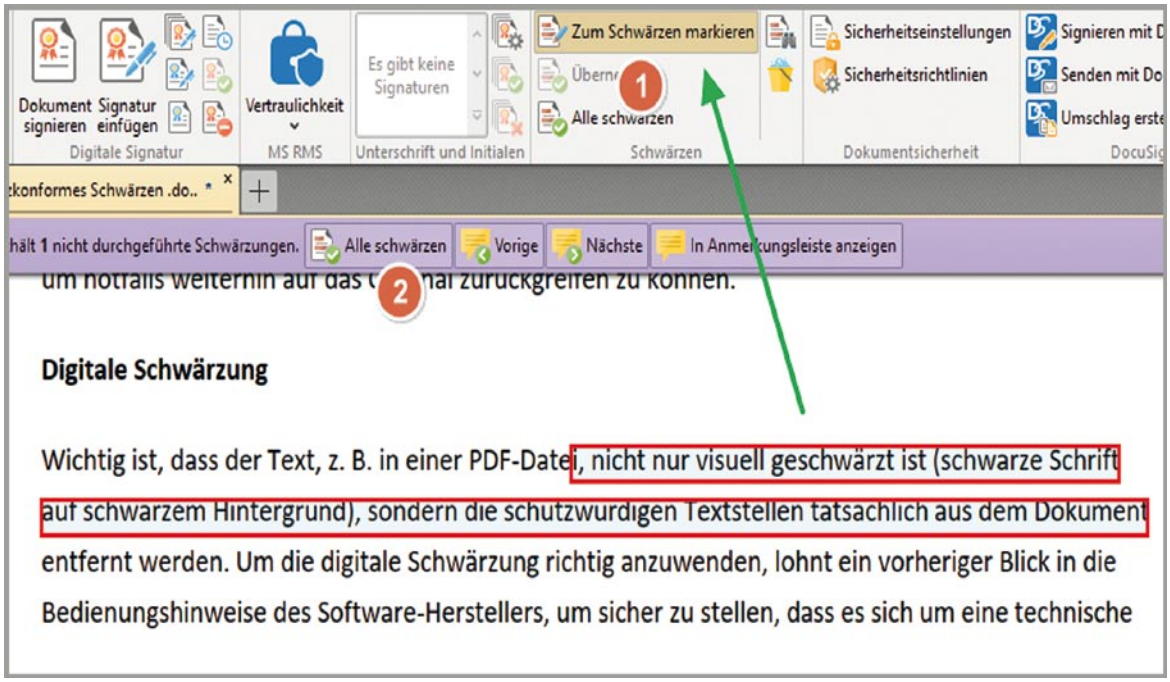
Wichtig ist, dass der Text, z. B. in einer PDF-Datei, nicht nur visuell geschwärzt ist (schwarze Schrift auf schwarzem Hintergrund), sondern die schutzwürdigen Textstellen tatsächlich aus dem Dokument entfernt werden. Um die digitale Schwärzung richtig anzuwenden, lohnt ein vorheriger Blick in die Bedienungshinweise des Software-Herstellers, um sicher zu stellen, dass es sich um eine technische und nicht nur optische Schwärzung handelt, denn nicht in jeder Anwendung ist eine Funktion zum sicheren „Schwärzen“ Integriert.

Beachte! Vor jeder Änderung am Dokument, sollte unbedingt vorher eine Kopie des Originaldokuments erstellt werden. Eine korrekte „Schwärzung“ kann nach dem Speichervorgang nicht mehr rückgängig gemacht werden.

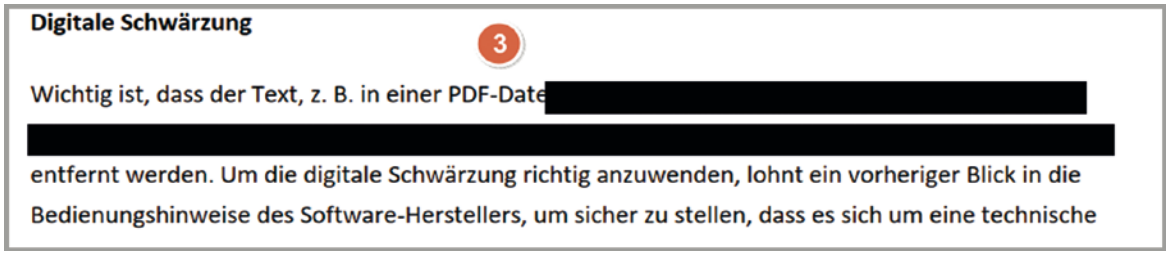
Online-Dienste, bei denen PDF-Dateien zur weiteren Bearbeitung auf Server des Anbieters hochgeladen werden, um danach mit Hilfe des Webbrowsers die entsprechenden Bereiche zu schwärzen, bringen unter Umständen datenschutzrechtliche wie auch sicherheitsrelevante Risiken mit sich.

Beispiel einer digitalen „Schwärzung“ an Hand eines Worddokuments mit Hilfe einer Software die sicheres „Schwärzen“ unterstützt. In einem ersten Schritt werden die betroffenen Stellen markiert und danach die „Schwärzung“ ausgeführt. Anschließend wird das überabeitete Dokument ausgedruckt oder als PDF (z.B. zur Weitergabe) gespeichert.

Personenbezogene Daten verbergen sich häufig auch in den Metadaten von Dateien, zum Beispiel wer zu welcher Uhrzeit Änderungen vorgenommen hat oder – vor allem bei Bilddateien – Angaben zum Urheber, der GPS-Position und zu Datum und Uhrzeit der Aufnahme. Unter Umständen können sogar Vorgängerversionen und ausgeblendete Kommentare aus Office-Dateien wiederhergestellt werden. Die Datei-Eigenschaften sollten daher stets überprüft werden. Es gibt Programme, die über Funktionen verfügen, um enthaltene Metadaten zu löschen.



(1) Die zu schwärzenden Stellen markieren, (2) Vorgang ausführen.



(3) Ergebnis

Metadaten werden bei Schwärzung oftmals vergessen.

Wichtig: Das geschwärzte Office-Dokument sollte nicht in seinem originalen Dateiformat weitergeben werden (z. B. docx). Die Datei sollte in ein PDF-Dokument umgewandelt werden. Der gesamte bereits anonymisierten Text kann auch kopiert und in ein neues Dokument eingefügt werden, welches dann weitergegeben werden kann. Das Speichern eines Office-Dokuments unter einem neuen Namen allein reicht nicht aus, um entsprechende Metadaten zu entfernen.

Händische Schwärzung - Schwarzer Stift nicht immer ausreichend

Steht keine Anwendung zur Verfügung, die eine elektronische Schwärzung ermöglicht, so können Dokumente ausgedruckt und händisch geschwärzt werden. Werden Papierdokumente mit einem Stift geschwärzt, muss sichergestellt sein, dass die Schrift tatsächlich unlesbar abgedeckt ist. Es kommt immer wieder vor, dass geschwärzte Passagen trotzdem noch erkennbar sind. Manchmal genügt es das jeweilige Blatt Papier gegen eine Lampe zu halten.

Dritte können z. B. an die geschwärzten Inhalte gelangen, indem sie mit Grafiksoftware den Farbkontrast erhöhen oder Filter einsetzen.

Schwärzen von Bildern

Sollen auf digitalen Fotos oder Screenshots beispielsweise Gesichter, Nummernschilder oder andere personenbezogene Daten unkenntlich gemacht werden, machen Verantwortliche mitunter von Unschärfeeffekten in Grafikprogrammen (Verpixelungen oder Reduzierung der Auflösung) Gebrauch. Dies ist jedoch unsicherer als eine Schwärzung, denn mit Hilfe von Künstlicher Intelligenz können verschwommene Inhalte durchaus rekonstruiert werden.

Mögliche Lösung

Sie legen in Ihrer Grafiksoftware über das jeweilige personenbezogene Datum ein anderes Motiv, z. B. einen schwarzen Balken oder einen anderen Bereich aus dem Bild. Auf Gesichter können auch digitale Farbkleckse verteilt und anschließend der Pixel-Effekt angewendet werden.

Wichtig ist zudem, dass das bearbeitete Bild dann in einem Dateiformat abgelegt wird, bei dem sich die Originalebene nicht wiederherstellen lässt. Hierfür bietet sich beispielsweise das JPG-Format an.

Fazit:

Grundsätzlich gibt es verschiedene Möglichkeiten, die herauszugebenden Unterlagen datenschutzkonform zu schwärzen, sodass keine schutzwürdigen Daten Dritter enthalten sind. Sowohl bei einer digitalen als auch bei einer händischen Schwärzung ist darauf zu achten, dass die geschwärzten personenbezogenen Daten tatsächlich nicht mehr ausgelesen bzw. rekonstruiert werden können. Bei digitalen Dateien sollten nur Formate verwendet werden, die keine Metadaten mit Informationen über Dritte enthalten. Um Datenpannen zu verhindern, sollten das Dokument bzw. die Bilder abschließend gründlich auf Schwärzungslücken geprüft werden.

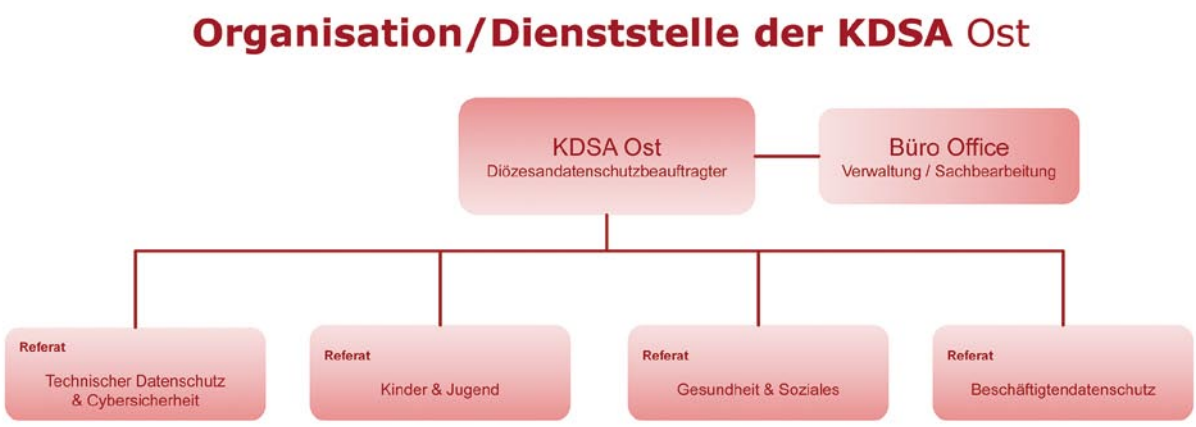
Verantwortliche sollten ihren internen Prozess zur Dokumentenherausgabe daher prüfen und ihre Beschäftigten sensibilisieren.

Die Kirchliche Datenschutzaufsicht Ost

KDSA Ost als Dienststelle

Die Kirchliche Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs mit Sitz in Schönebeck/Elbe unter Leitung des Diözesandatenschutzbeauftragten ist die zuständige Datenschutzaufsichtsbehörde für die ostdeutschen Bistümer und ihren Einrichtungen. Die kirchliche Datenschutzaufsicht ist oberste Dienstbehörde im Sinne des § 96 Strafprozessordnung und oberste Aufsichtsbehörde im Sinne des § 99 Verwaltungsgerichtsordnung.

Organigramm



Unsere Aufgaben und Befugnisse

Die kirchlichen Datenschutzaufsichtsbehörden haben zunächst die Aufgabe, die Einhaltung der Gesetze zum Datenschutz zu kontrollieren und bei Nichteinhaltung mit entsprechenden Sanktionen zu reagieren.
Bei Verstößen gegen die Bestimmungen des KDG sowie der KDG-DVO kann die Datenschutzaufsicht eine Geldbuße verhängen.

Im Rahmen des Zuständigkeitsbereichs ergeben sich eine Reihe von weiteren Aufgaben (§ 44 KDG). Dazu gehören u.a.

- Die Durchführung von Untersuchungen in Form von Datenschutzüberprüfungen auch auf der Grundlage von Informationen einer anderen Datenschutzaufsicht oder einer anderen Behörde.
- Die Durchführung von Untersuchungen im Rahmen der technischen und organisatorischen Maßnahmen sowie zum Stand der Technik (KDG-DVO).
- Die Bearbeitung gemeldeter Beschwerden und gemeldeter Datenschutzvorfälle.
- Die Erstellung eines jährlichen Tätigkeitsberichts welcher u.a. Entwicklungen des Datenschutzes im nichtkirchlichen Bereich enthält.

Eine weitere Aufgabe ist die Durchführung von Untersuchungen im Rahmen der technischen und organisatorischen Maßnahmen sowie zum Stand der Technik (KDG-DVO), u.a. auch das Verfolgen zu Entwicklungen der Informations- und Kommunikationstechnologie soweit sie sich die Informationssicherheit auswirken.

Öffentlichkeitsarbeit

Die Aufklärung und Sensibilisierung zum Schutz persönlicher Daten ist eine wichtige Aufgabe, damit frühzeitig erkannt wird, um was es beim Datenschutz geht. Durch die zunehmende Digitalisierung steigt die Gefahr der Verschmelzung von personenbezogenen Daten mit betrieblichen Daten bis hin zur Untrennbarkeit. Lösch- oder Änderungsbegehren hinsichtlich einzelner persönlicher Daten wird damit erschwert und die Gefahr, das persönliche Daten an unbefugte Dritte gelangen, steigt. Das ist z.B. bei den sich häufenden Cyber-Attacken der Fall, bei denen Daten an die Öffentlichkeit geraten, die genau genommen nach den geltenden Datenschutzbestimmungen (sobald der Zweck der Verarbeitung und ggf. die Aufbewahrungsfristen entfallen sind) nicht vorhanden sein dürften.

Um verstärkt Akzeptanz auf den Datenschutz im rechtlichen Sinne zu schaffen, führen wir zusätzlich zu aktuellen Themen auf unserer Website unter www.kdsa-ost.de öffentlichen Video-Sprechstunden und gemein-

same Diskussionsrunden zu Fragen rund um das Thema Datenschutz und Informationssicherheit durch.

Ein weiteres erfolgreich angenommen Angebot sind unsere fach- und anlassbezogenen Online-Veranstaltungen.

Mit unserem jährlichen Tätigkeitsbericht, den wir als Druckausgabe und Online bereitstellen, tragen wir u.a. dazu bei, dass Datenschutz und Informationsfreiheit im täglichen Leben und der damit verbundenen digitalen Welt Beachtung finden.

Auszug aus unseren Veranstaltungen 2024

TOMtalk?! Cyber-Attacke vs. Daten weg, wie vorbereitet?

Daten weg o. nicht verfügbar! Wir laden ein zum Dialog/Informations-Austausch - wie sind wir auf so ein Ereignis vorbereitet? Gibt es organisatorische Abläufe/Maßnahmen? Ist man schon betroffen und weiß es nicht?

Datenschutz in der Aufarbeitung von sexuellem Missbrauch

Datenschutz in der Aufarbeitung von sexuellem Missbrauch sowie der Anerkennung von Leid.

Auskunftsverlangen im Datenschutz, Datenverkehr - aber gesichert

Neben einem Bußgeld durch eine Datenschutzbehörde kann der Betroffene u.a. auch Schadensansprüche geltend machenen. Dabei spielen u.a. ein sicherer Transport sowie eine sichere Datenübermittlung der Daten eine Rolle.

Datenschutz im MAV-Büro

Aus dem Inhalt: Datenschutzkonzept der MAV, Elektronische Arbeitszeiterfassung, Aufbewahrungsfristen für MAV-Unterlagen, u.w. Themen.

Nachgefragt?! Datenschutz im Kindergarten

Eine offene Online-Sprechstunde für alle Kita-Mitarbeitende, in der Datenschutzgrundlagen in Kindereinrichtungen besprochen oder Themen aus einer erfolgten Datenschutzschulung reflektiert werden können.

Seminar Beschäftigtendatenschutz

Grundlagen des Datenschutzes, Verfahren mit Bewerbungsunterlagen, Kontrollaufgaben der MAV bei datenschutzrechtlichen Fragestellungen, Auskunftsanspruch Beschäftigter, Haftung für Datenschutzverstöße, u.w.

Nachgefragt?! Unsere regelmäßigen Videosprechstunden

Eine offene Online-Sprechstunde wo Sie Fragen zum Thema Datenschutz, Beschäftigtendatenschutz, Risiken, Technischer Datenschutz & Cybersicherheit stellen können oder mit uns darüber diskutieren möchten?

Anhang

Microsoft Versionsinformationen

Modern Lifecycle-Richtlinie von Microsoft - Im Rahmen dieser Richtlinie wird für ein Produkt Support angeboten.

Windows 10 Home und Pro, Windows 10 Enterprise and Education

Version	Startdatum	Enddatum
Version 22H2	18. Okt. 2022	14. Okt. 2025
Version 21H2	16. Nov. 2021	13. Juni 2023

Windows 11 Home und Pro

24H2	1. Okt. 2024	13. Okt. 2026
23H2	31. Okt. 2023	11. Nov. 2025
22H2	20. Sept. 2022	08. Okt. 2024

Windows 11 Enterprise LTSC 2024

	01. Okt. 2024	09. Okt. 2029

Microsoft Exchange

	Startdatum	Erweitertes Enddatum
Exchange Server 2016	01. Okt. 2015	14. Okt. 2025
Exchange Server 2019	22. Okt. 2018	14. Okt. 2025

Weitere Information zur Ausmusterung von Produkten:
https://learn.microsoft.com/de-de/lifecycle/

Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
ArbG	Arbeitsgericht
ArbZG	Arbeitszeitgesetz
AU	Arbeitsunfähigkeit
AV-Vertrag	Auftragsverarbeitungsvertrag
BAG	Bundesarbeitsgericht
BÄK	Bundesärztekammer
BBG	Behindertengleichstellungsgesetz
BDSG	Bundesdatenschutzgesetz
BeschDG	Beschäftigtendatenschutzgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationssicherheit
BFSG	Barrierefreiheitsstärkungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BITV	Barrierefreie-Informationstechnik-Verordnung
BMeldG	Bundesmeldegesetz
BVKJ	Berufsverband der Kinder- und Jugendärzt*innen
BT.-Drs	Bundestag-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CCC	Chaos Computer Club

DDG	Digitale-Dienste-Gesetz
DDSB	Diözesandatenschutzbeauftragten
DSK	Datenschutzkonferenz
DSK-DBK	Datenschutzgericht der Deutschen Bischofskonferenz
DS-GVO	Datenschutz-Grundverordnung
DVO	Kirchliche Dienstvertragsordnung
ELStAM	Elektronische Lohnsteuerabzugsmerkmale
ePA	elektronische Patientenakte
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
GrCH	Grundrechtecharta
GrO	Grundordnung des kirchlichen Dienstes
HTML	Hypertext Markup Language (Auszeichnungssprache für Webseiten)
http	Hypertext Transfer Protokoll (unverschlüsselt)
https	Hypertext Transfer Protokoll Secure (verschlüsselt)
IDSG	Interdiözesane Datenschutzgericht
IfSG	Infektionsschutzgesetz
KG	Kammergericht
KI	Künstliche Intelligenz
LAG	Landesarbeitsgericht
LG	Landgericht
KDG	Kirchliches Datenschutzgesetz

KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz
MAV	Mitarbeitervertretung
NIS	Netzwerk- und Informationssicherheit
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PKV	Private Krankenversicherung
RiLi	Richtlinie
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
TMG	Telemediengesetz
TOM	Technisch organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutzgesetz
VDD	Verbandes der Diözesen Deutschlands
VG	Verwaltungsgericht
VVT	Verzeichnis von Verarbeitungstätigkeiten

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und des Katholischen Militärbischofs
Badepark 4 • 39218 Schönebeck
Telefon: 03928 7179018
www.kdsa-ost.de • kontakt@kdsa-ost.de