

→ Tätigkeitsbericht 2023



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



**Ich fürchte mich vor dem Tag, an dem die Technologie unsere
Menschlichkeit übertrifft.**

Auf der Welt wird es nur noch eine Generation aus Idioten geben.

Albert Einstein

8. Tätigkeitsbericht des
Diözesandatenschutzbeauftragten

für

das Erzbistum Berlin

das Bistum Dresden-Meißen

das Bistum Erfurt

das Bistum Görlitz

das Bistum Magdeburg

den Katholischen Militärbischof

Berichtszeitraum 01.01.2023 bis 31.12.2023





Wir Fragen ChatGPT:

Hallo, Einstein sagte, auf der Welt wird es nur noch eine Generation von Idioten geben.

Hat das etwas mit der Digitalisierung und KI zu tun?

ChatGPT antwortet:

Die berühmte Aussage von Albert Einstein, dass es „nur noch eine Generation von Idioten geben wird“, wird oft auf verschiedene Weisen interpretiert. Es gibt keine klare Bestätigung, dass Einstein tatsächlich diese Worte gesagt hat, aber viele interpretieren sie als eine Warnung vor einer Gesellschaft, die ihre intellektuellen Fähigkeiten und kritischen Denkfähigkeiten vernachlässigt.

In Bezug auf die Digitalisierung und KI könnte man argumentieren, dass diese Technologien sowohl positive als auch negative Auswirkungen auf die intellektuelle Entwicklung der Gesellschaft haben können. Auf der einen Seite können sie den Zugang zu Bildung und Informationen erleichtern und die Menschen ermächtigen, Wissen zu erlangen und Probleme zu lösen. Auf der anderen Seite könnten sie auch dazu führen, dass Menschen sich zu sehr auf Technologie verlassen und ihre eigenen kritischen Denkfähigkeiten vernachlässigen.

Es ist wichtig, dass wir uns bewusst darüber sind, wie wir Technologie nutzen und wie sie unsere intellektuelle Entwicklung beeinflusst. Eine ausgewogene Herangehensweise, die sowohl die Vorteile als auch die Risiken berücksichtigt, ist entscheidend, um sicherzustellen, dass wir nicht in die Falle fallen, die Einstein möglicherweise angedeutet hat.

Antwort generiert von ChatGPT 3.5

Bei KI-Systemen wissen wir in der Regel nicht, wie die KI auf ein bestimmtes Ergebnis gekommen ist. Es liegt dann an uns, mit unserem Sachverstand die Ergebnisse zu bewerten.

Verlassen wir uns ungeprüft auf die Ergebnisse der KI-Systeme, würden wir nicht merken, wie wir mit nicht korrekten Ergebnissen in eine falsche Richtung geleitet würden (manipuliert).



Inhaltsverzeichnis

Inhaltsverzeichnis	1
Vorwort	5
1 Entwicklung des Datenschutzes	7
1.1 Entwicklung des Datenschutzes in Europa	7
1.1.1 Neuer Angemessenheitsbeschluss für den Datenverkehr zwischen der EU und der USA.....	7
1.1.2 Empfänger müssen im Auskunftersuchen konkret benannt sein.....	8
1.1.3 Kopien im Auskunftsrecht (Art. 15 Abs. 3 DS-GVO / § 17 Abs. 3 KDG)	10
1.1.4 Patientenakte – Patient hat Recht auf unentgeltliche erste Kopie	11
1.1.5 Personenbeziehbarkeit pseudonymer Daten	13
1.1.6 Personalausweise mit Fingerabdrücken sind erlaubt.....	14
1.1.7 EuGH festigt DS-GVO-Grundsätze: Klarstellung bei Haftung und Schadensersatz	16
1.2 Entwicklung des Datenschutzes in Deutschland	18
1.2.1 Gesetze zur Digitalisierung des Gesundheitswesens	18
1.2.2 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses - § 26 BDSG entspricht nicht den Anforderungen von Art. 88 DS-GVO.....	22
1.2.3 Vorratsdatenspeicherung ist endgültig rechtswidrig	24
1.2.4 Ansprüche nach DS-GVO wegen eigenmächtiger Verarbeitung von Kundendaten auf privatem Account	25
1.2.5 Datenschutz im Land Sachsen-Anhalt.....	27
1.3 Entwicklung des Datenschutzes in der Kirche	28
1.3.1 Auswirkungen der Änderung der kirchlichen Grundordnung	28
1.3.2 Datenschutz und Aufgebot zur kirchlichen Eheschließung	29
1.3.3 Das „Löschen“ ist eine Verarbeitung im Sinne des KDG	32
2 Datenschutz allgemein.....	33
2.1 Recht am eigenen Bild und Betreuung	33
2.2 Maß- und zwecklose Datenerhebung bei Schuleingangsuntersuchungen	35
2.3 Werbesendungen von Wohltätigkeitsorganisationen.....	38
3 Datenschutzaufsicht.....	41
3.1 Rechtsform und Unabhängigkeit der kirchlichen Datenschutzaufsicht	41



3.2 Wirksame Einreichung einer Datenschutzbeschwerde	42
3.3 Vor-Ort-Besuche der Datenschutzaufsicht	43
3.4 Prüffaktion der Datenschutzaufsicht	45
3.4.1 Prüfung eines Caritas Regionalzentrums	45
3.4.2 Prüfung eines Seniorenzentrum	48
3.4.3 Datenschutzüberprüfungen in Kindertageseinrichtungen – Ergebnisse, Entwicklungen und Hinweise	52
3.4.4 Webseiten-Check.....	56
3.5 Datenschutzvorfälle	58
3.5.1 Offener E-Mail Verteiler – Datenpanne mit Wiederholungsgarantie.....	58
3.5.2 Keine Auskunft unter dieser Nummer I	60
3.5.3 Keine Auskunft unter dieser Nummer II.....	62
3.5.4 Kostenzuschüsse für dienstliche Erreichbarkeit über private Geräte.....	64
4 Datenschutzvorfälle im Gesundheitswesen	66
4.1 Dauerbrenner: Falsche versandte Patientenunterlagen.....	66
4.2 Beschwerden wegen fehlender oder verspäteter Erfüllung von Auskunftersuchen ..	66
4.3 Plastischer Chirurg nutzt Fotos von Patientin für Schulungszwecke	67
4.4 Verlorene Unterlagen	69
4.5 Videoüberwachung.....	70
5 Datenschutz in Kita und Schule	72
5.1 Verarbeitungstätigkeiten in Kindertagesstätten	72
5.1.1 Ein Verzeichnis für Verarbeitungstätigkeiten – nicht nur lästiges Übel.....	72
5.1.2 Inhalt eines Verarbeitungsverzeichnisses in Kindertageseinrichtungen	73
5.2 Datenschutzvorfälle	77
5.2.1 Enkeltrick in der Kita.....	77
5.2.2 Zugriff auf Kinderakten	78
5.2.3 Speichermedien auf Abwegen	79
6 Datenschutz im Beschäftigungsverhältnis.....	79
6.1 Im Interessenkonflikt – Betriebsratsvorsitzender als Datenschutzbeauftragter	79
6.2 Offboarding – Löschung personalisierter E-Mail-Konten von Beschäftigten.....	81
6.3 Anspruch auf Entfernung einer Abmahnung aus einer Personalakte	82



6.4 Zeitwertkonten – Musterberechnung.....	85
7 Technischer Datenschutz.....	87
7.1 E-Mail-Postfach gehackt - was können Sie jetzt tun	87
7.2 QR-Codes - Bequemlichkeit mit Tücken?	89
7.2.1 Vorsichtsmaßnahmen	92
7.3 Das A-B-C beim E-Mailversand.....	93
7.3.1 Das A-B-C mit Outlook	94
7.3.2 Wie sieht es bei den Empfängern aus?.....	98
7.4 Phishing/Cyber-Attacke – Ausbreitung gestoppt.....	99
Die Kirchliche Datenschutzaufsicht Ost.....	103
KDSA Ost als Dienststelle.....	103
Organigramm	103
Unsere Aufgaben und Befugnisse	103
Öffentlichkeitsarbeit.....	104
Auszug aus unseren Veranstaltungen 2023.....	105
Anhang.....	107
Muster Verarbeitungsverzeichnis Aufnahmevertrag.....	107
Microsoft Windows 10 Versionsinformationen.....	108
Abkürzungen	109





Vorwort

Im Berichtsjahr feierten die Datenschutzgesetze ihr fünfjähriges Bestehen.

Am 25. Mai 2018 trat die Datenschutzgrundverordnung in Kraft, die international als „Goldstandard“ der Datenschutzgesetzgebung gilt. Aufgrund des Artikel 91 dieser Verordnung durften die Kirchen ihre eigenen Datenschutzgesetze beibehalten, sofern sie diese mit den Regelungen der DS-GVO in Einklang gebracht haben. Die Kirchen haben diese Möglichkeit genutzt. Für die Katholische Kirche gilt seitdem das Kirchliche Datenschutzgesetz (KDG), welches inhaltlich den gleichen Standard besitzt wie die europäische Verordnung.

Die Einführung eines neuen Gesetzes im kirchlichen Bereich hat auch hier zu einer hohen Aufmerksamkeit für das Thema Datenschutz gesorgt. Insbesondere die Möglichkeit für die Aufsichtsbehörden nun Bußgelder gegen kirchliche Einrichtungen verhängen zu können, hat bei vielen Institutionen dazu geführt, sich intensiv mit dem Datenschutz zu befassen.

Das neue Gesetz führte in vielerlei Hinsicht aber gar keine Neuerungen ein. Das war vielen häufig nur deshalb nicht klar, weil sie die alte Regelung bis dahin nicht wahrgenommen hatten.

Panikmache und Angst vor hohen Bußgeldern haben sich nicht bestätigt.

Viele Einrichtungen haben nach außen erkennbare Verpflichtungen wie die Bestellung von Datenschutzbeauftragten oder Datenschutzhinweise auf der Homepage umgesetzt. Es darf jedoch unterstellt werden, dass nicht alle Verantwortlichen die Regelungen tatsächlich als erforderlich zum Schutz von Persönlichkeitsrechten akzeptiert haben. Gelegentlich scheint man sich den Regelungen ergeben zu haben, um mit ein bisschen Datenschutzkosmetik Ärger zu vermeiden.

Dies wird insbesondere dort deutlich, wo professionelle externe Datenschutzbeauftragte sich darauf spezialisiert haben, nicht primär einen erforderlichen Datenschutzstandart bei ihren Kunden zu etablieren, sondern im Falle eines Datenschutzvorfalls diese Klienten rechtlich zu beraten und gegenüber der Aufsicht zu vertreten. Bei solchermaßen vertretenen Verantwortlichen nahm die Bereitschaft, einen effektiven Datenschutz zu



realisieren und dadurch gegebenenfalls Einschränkungen hinzunehmen, schon wieder deutlich ab.

Um diesem Trend entgegenzuwirken, hat die KDSA-Ost zur Feier des fünfjährigen Bestehens des KDG eine Themenwoche veranstaltet. In dieser Woche wurden einem breiten Publikum verschiedene Gebiete des Datenschutzes und der Datensicherheit in Vorträgen, Workshops und offenen Videokonferenzen nahegebracht.

Mit der Einführung von anlasslosen aber angemeldeten Prüfungen verschafft sich unsere Aufsicht einen Überblick über die Umsetzung von Datenschutzregeln in den Einrichtungen. Darüber hinaus soll damit die Präsenz der Aufsicht in der Fläche demonstriert werden. Dabei geht es nicht darum, nach Datenschutzfehlern zu fahnden, sondern darum, die Ansprechbarkeit und Unterstützungsbereitschaft der Aufsicht deutlich zu machen.

Um Beratung und Unterstützung geht es auch bei den zunehmend ausgeweiteten und angenommenen Angeboten von Videoveranstaltungen, in denen für alle Interessierten die Möglichkeit geschaffen wird, Fragen zum Datenschutz zu klären. Diese Veranstaltungen werden teilweise zu konkreten Themen als Vortragsveranstaltung angeboten und teilweise als offene Videosprechstunden, in denen Teilnehmende ihre Fragen zum Datenschutz mit der Aufsicht besprechen können. Darüber hinaus werden weiterhin themenspezifische Präsenzveranstaltungen angeboten.

Im Ergebnis bleibt nach fünf Jahren KDG trotz gelegentlich anzutreffender Defizite festzustellen, dass das Thema Datenschutz in den Bistümern und Einrichtungen nicht nur angekommen, sondern auch etabliert ist.



1 Entwicklung des Datenschutzes

1.1 Entwicklung des Datenschutzes in Europa

1.1.1 Neuer Angemessenheitsbeschluss für den Datenverkehr zwischen der EU und der USA

Die Europäische Kommission teilte in ihrer Pressemitteilung vom 10. Juli 2023 mit, dass sie den Angemessenheitsbeschluss für den **Datenschutzrahmen EU-USA** angenommen hat. Demnach sind jetzt Datenübermittlungen von Europa in die USA wieder möglich, wenn die datenempfangenden Stellen nach diesem Beschluss zertifiziert worden sind. Das neue Datenschutzabkommen, mit dem Namen **EU-U.S. Data Privacy Framework**, soll somit die USA als Drittland mit einem angemessenen Datenschutzniveau legitimieren.

Neu in diesem Abkommen ist, dass der vorab viel kritisierte Zugriff der US-Geheimdienste auf die Daten aus der EU auf ein notwendiges und verhältnismäßiges Maß beschränkt ist. Bei den bisherigen Angemessenheitsbeschlüssen hatten die US-Geheimdienste weitreichende Zugriffsmöglichkeiten, was von dem Europäischen Gerichtshof (EuGH) bemängelt wurde, da dies nicht den Standards der DS-GVO entsprochen habe.

Im Weiteren soll ein neues Gericht zur Datenschutzüberprüfung aufgebaut werden, an das sich die EU-Bürger bei Zweifeln wenden können.

Weitere Neuerungen in diesem Abkommen sind:

- Personenbezogene Daten sind zu löschen, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind
- Personenbezogene Daten werden bei der Weitergabe an Dritte gemäß dem Angemessenheitsbeschluss geschützt
- Kostenlose und unabhängige Streitbeilegungsmechanismen und Schiedsstelle



Was müssen Einrichtungen beachten, die sich jetzt bei der Übermittlung personenbezogener Daten auf § 40 Abs. 1 KDG berufen möchten?

Sich voreilig bei der Datenübermittlung in die USA auf den Angemessenheitsbeschluss zu berufen wäre faktisch falsch. Die datenempfangende Stelle muss zuerst ein Selbstzertifizierungsverfahren durchlaufen und dieses nachweisen können. Im Weiteren müssen Dokumente, wie die Datenschutzhinweise(-erklärung) und das Verarbeitungsverzeichnis, des Verantwortlichen dementsprechend angepasst werden. Nicht zu vergessen sind damit auch Änderungen im Auskunftsrecht und bei Auftragsverarbeitungsverträgen.

Umfangreiche Anwendungshinweise hat die Datenschutzkonferenz der Länder (DSK) veröffentlicht.¹ Auch für kirchliche Einrichtungen können diese Hinweise nützlich sein.

Ausblick

Trotz vieler positiver Stimmen aus Politik und Wirtschaft ist die erste Klage gegenüber dieser (Neu-)regelung beim EuGH anhängig.

1.1.2 Empfänger müssen im Auskunftersuchen konkret benannt sein

Werden personenbezogene Daten offengelegt, dann muss der Verantwortliche über **die konkrete Identität des Empfängers** Auskunft erteilen, so die Auffassung des EuGHs².

Nach Ansicht des EuGHs hat der für die Datenverarbeitung Verantwortliche dabei grundsätzlich auf Anfrage des Betroffenen die konkrete Identität des Empfängers der offengelegten Daten mitzuteilen. Lediglich dann, wenn der Empfänger (noch) nicht identifiziert werden kann oder der Antrag offenkundig unbegründet oder exzessiv ist, kann sich die Mitteilung auf die Kategorien der Empfänger beschränken.

Die Entscheidung betraf die Auslegung des Art. 15 Abs. 1 lit. c) DS-GVO, der wortgleich mit § 17 Abs. 1 lit. c) KDG ist. Der Wortlaut dieser Vorschrift ist nicht eindeutig und lässt unterschiedliche Interpretationen zu:

¹ https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

² EuGH, Urteil vom 12.01.2023 - C-154/21



„...die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen...“

Danach bleibt offen, ob die betroffene Person Auskunft zu den konkreten Empfängern verlangen kann oder ob die Konkretisierung im Ermessen des Verantwortlichen liegt.

Das Auskunftsrechts hat für betroffene Personen eine erhebliche Bedeutung, da die Informationen, die sie erhalten, die Basis bilden können, um möglicherweise weitere Betroffenenrechte, wie z.B. das Recht auf Berichtigung nach § 18 KDG (Art. 16 DS-GVO) oder das Recht auf Löschung nach § 19 KDG (Art. 17 DS-GVO) geltend zu machen. Nur beim Vorliegen vollständiger Informationen, welche Daten zu welchen Zwecken verarbeitet werden, ist eine Prüfung möglich, ob die Verarbeitung korrekt erfolgt oder ob längst eine Löschung der Daten hätte erfolgt sein müssen.

Die Entscheidung des EuGHs sorgt nunmehr für Klarheit und Rechtssicherheit. Die Konturen des Auskunftsanspruchs werden somit weiter geschärft. Die Entscheidung bedeutet jedoch einen gewissen Mehraufwand im Rahmen der Beantwortung von datenschutzrechtlichen Auskunftsanfragen, da **die konkrete Identität eines jeden Empfängers mitgeteilt werden** muss. Entscheidend ist jedoch, dass auf der anderen Seite die Rechte von betroffenen Personen weiter erheblich gestärkt werden.

Umso mehr gilt der Rat: Die Beantwortung von Auskunftsersuchen und anderen datenschutzrechtlichen Begehren sollte daher stets mit dem Datenschutzbeauftragten abgestimmt werden.





1.1.3 Kopien im Auskunftsrecht – (Art. 15 Abs. 3 DS-GVO / § 17 Abs. 3 KDG)

Lange Zeit umstritten war, welchen konkreten Anforderungen eine „Kopie“ von personenbezogenen Daten im Rahmen des Auskunftsanspruches nach Art. 15 Abs. 3 DS-GVO (§ 17 Abs. 3 KDG) unterliegt. Der Wortlaut der Norm lautet:

„Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.“

Streitig war, ob hierunter eine exakte Kopie (originalgetreue Reproduktion) durch einen 1:1 Scan/Kopie von sämtlichen Unterlagen zu verstehen ist oder eine Tabelle an aggregierten Informationen ausreicht.

In seinem Urteil vom 04.05.2023³ erläutert der Europäische Gerichtshof (EuGH) den Inhalt und den Umfang des Auskunftsrechts der betroffenen Person über ihre personenbezogenen Daten, die Gegenstand der Verarbeitung sind.

Nach Ansicht des EuGHs bedeutet das Recht, eine „Kopie“ der personenbezogenen Daten zu erhalten, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten ausgehändigt wird.

Der Anspruch nach § 15 Abs. 3 DS-GVO impliziert das Recht, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die diese Daten enthalten, zu erlangen, wenn dies unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch die DS-GVO verliehenen Rechte zu ermöglichen, wobei insoweit die Rechte und Freiheiten anderer zu berücksichtigen sind.

Im Übrigen stellt der Gerichtshof klar, dass sich der im Sinne des Art. 15 Abs. 3 Satz 3 DS-GVO verwendete Begriff „Informationen“ ausschließlich auf personenbezogene Daten bezieht, von denen der für die Verarbeitung Verantwortliche gemäß Satz 1 dieses Absatzes eine Kopie zur Verfügung stellen muss.

³ EuGH; Urteil vom 04.05.2023 – AZ. C-487/21



Der EuGH entschied mit dem Urteil (Rdz. 28), dass ein recht weites Verständnis vom Begriff der „Kopie“ anzulegen sei, also „dass diese Bestimmung der betroffenen Person das Recht verleiht, eine originalgetreue Reproduktion ihrer personenbezogenen Daten im Sinne einer weiten Bedeutung zu erhalten, die Gegenstand von Vorgängen sind, die als Verarbeitung durch den für diese Verarbeitung Verantwortlichen eingestuft werden müssen.“

Die Kopie müsse nach Ansicht des Gerichts alle personenbezogenen Daten enthalten, die Gegenstand der Verarbeitung sind, sich also nicht nur auf ein Dokument als solches beziehen. Die Daten sind daher vollständig und originalgetreu wiederzugeben. In bestimmten Situationen, z. B. bei Freitextfeldern bedarf es einer Erklärung des Kontextes der Datenverarbeitung, *„damit die betroffene Person eine transparente Auskunft und eine verständliche Darstellung dieser Daten erhalten kann.“*

1.1.4 Patientenakte – Patient hat Recht auf unentgeltliche erste Kopie

Auf Vorlage des BGH hatte sich der EuGH mit Fragen der Auslegung der DS-GVO zu beschäftigen und traf eine Entscheidung, die den Arbeitsalltag in vielen Arztpraxen/Kliniken verändern könnte: Patienten bekommen eine kostenlose erste Kopie der Patientenakte⁴. Lange war diese Frage umstritten.

Der klagende Patient aus Deutschland befand sich bei der beklagten Zahnärztin in zahnärztlicher Behandlung. Er hatte den Verdacht, dass die Ärztin Fehler bei der Behandlung gemacht hatte. Um damit verbundene Haftungsansprüche geltend zu machen, verlangte er eine Kopie seiner Patientenakte.

Das Recht der Patienten auf Einsichtnahme in ihre Patientenakte beim Arzt ist seit Jahren geklärt. Der Anspruch ergibt sich aus §§ 630f, 630g des Bürgerlichen Gesetzbuches (BGB). Hiernach ist der behandelnde Arzt verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichem Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder

⁴ EuGH, Urteil vom 26.10.2023 - Az. C-307/22



elektronisch zu führen. Patienten ist auf Verlangen Einsicht in ihre Patientenakte zu gewähren, zudem können sie elektronische Abschriften verlangen.

Ungeklärt war bisher hingegen die Frage, wer die Kosten für Kopien der Patientenakte zu tragen hat. Die Zahnärztin war der Meinung, dass der klagende Patient dafür aufkommen müsse. Der Patient sah das anders. Er war der Ansicht, er habe Anspruch auf eine unentgeltliche Kopie aufgrund von Art. 15 DS-GVO und rief die deutschen Gerichte an.

Das Gericht der 1. Instanz und die Berufungsinstanz gaben dem Kläger Recht. Beide Entscheidungen beruhten auf einer Auslegung der Art. 12 Abs. 5 und Art. 15 Abs. 1 und 3 DS-GVO. Der mit der Revision befasste BGH legte die Sache dem EuGH zur Entscheidung vor. Seiner Auffassung nach hängt die Entscheidung des Rechtsstreits davon ab, wie die genannten Bestimmungen der DS-GVO auszulegen seien.

Der EuGH entschied zugunsten des Patienten. Er urteilte, dass in der DS-GVO das Recht des Patienten verankert sei, eine erste Kopie der Patientenakte zu erhalten, ohne dass ihm dafür zusätzliche Kosten entstehen. Der Patient muss sein Verlangen zudem auch nicht begründen.

Nur wenn der Patient bereits eine Kopie der Akte erhalten habe und eine weitere wünscht, dann, so der EuGH, könne der Verantwortliche ein Entgelt für die Zurverfügungstellung verlangen.

Der EuGH begründet die Pflicht der Ärztin, unentgeltlich eine Kopie der Patientenakte zur Verfügung zu stellen, mit ihrer Stellung. Als behandelnde Ärztin sei sie als Verantwortliche im Sinne der DS-GVO für die Verarbeitung der personenbezogenen Daten des Patienten einzuordnen.

Der EuGH urteilte, dass der Patient eine vollständige Kopie der Dokumente verlangen darf, die sich in der Patientenakte befinden, wenn dies für das Verständnis erforderlich sei. Dies schließt Daten aus der Patientenakte ein, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.



1.1.5 Personenbeziehbarkeit pseudonymer Daten

Das Gericht der Europäischen Union (EuG) entschied, dass pseudonymisierte Daten, die an einen Empfänger übermittelt werden, nicht als personenbezogene Daten gelten, wenn der Datenempfänger nicht über die Mittel verfügt, die betroffenen Personen zu re-identifizieren⁵.

Gegenstand des Verfahrens

Der einheitliche Abwicklungsausschuss (Single Resolution Board, SRB) ist die Abwicklungsbehörde für bedeutende Banken und andere grenzüberschreitende Gruppen innerhalb der europäischen Bankenunion.

Der Entscheidung lag eine Klage des SRB zugrunde. Der SRB nutzte ein elektronisches Formular, mit dem Interessenten ihre Ansichten/Meinungen äußern konnten und leitete die erhaltenen Antworten an eine Beratungsfirma weiter.

Vor der Weitergabe der Antworten ersetzte der SRB den Namen jedes Antwortenden durch eine 33-stellige eindeutige Identifikationsnummer.

Nach einer Reihe von Beschwerden entschied der Europäische Datenschutzbeauftragte, dass es sich bei diesen Daten lediglich um pseudonymisierte Daten handele, die als personenbezogene Daten gemäß DS-GVO gelten. Diese habe der SRB ohne Datenschutzinformation an die betroffenen Personen gem. Art 13 DS-GVO weitergegeben.

Der SRB betrachtete seinerseits die Bereitstellung dieser Information als nicht erforderlich, da die übermittelten Daten seiner Ansicht nach anonymisiert waren und daher für den Datenempfänger nicht als personenbezogene Daten betrachtet werden konnten.

Anonym oder Pseudonym

Das EuG entschied, dass übermittelte Daten beim Empfänger dann nicht als personenbezogene Daten betrachtet werden könnten, wenn der Datenempfänger nicht die Möglichkeit hat, die betroffenen Personen zu identifizieren. Sofern der Datenempfänger weder über zusätzliche Informationen verfüge, die es ihm ermöglichen, die betroffenen Personen wieder zu iden-

⁵ EuG, Urteil vom 26.04.2023 -T-557/20



tifizieren, noch rechtliche Mittel habe, um auf solche Informationen zuzugreifen, könnten die übermittelten Daten nicht mehr nur als pseudonymisiert gelten, sondern müssten vielmehr als anonymisiert betrachtet werden. Sie fallen in diesem Fall nicht unter die Kategorie personenbezogener Daten. Die Tatsache, dass der Datenübermittler über die Mittel zur Re-Identifizierung der betroffenen Personen verfügt, ist irrelevant und bedeutet nicht, dass die übermittelten Daten automatisch auch personenbezogene Daten für den Empfänger sind.

Das Gericht stellte ferner fest, dass persönliche Ansichten oder Meinungen zwar personenbezogene Daten darstellen können, dies aber nicht generell gilt. Stattdessen ist eine Einzelfallbewertung erforderlich, *„die auf der Prüfung der Frage beruht, ob eine Ansicht aufgrund ihres Inhalts, ihres Zwecks oder ihrer Wirkung mit einer bestimmten Person verbunden ist“*.

Fazit:

Die Abgrenzung zwischen pseudonymisierten und anonymisierten Daten spielt in der Praxis eine große Rolle, da nur anonymisierte Daten nicht unter den Anwendungsfall der DS-GVO (und auch des KDVG) fallen. Bei einer Anonymisierung muss eine erhebliche Sorgfalt darauf verwendet werden, um der Rechenschaftspflicht zu genügen: Alle Entscheidungen zur Annahme einer Anonymisierung sollten dokumentiert und begründet werden. Darüber hinaus sollten im Rahmen des Datenschutzmanagements Leitlinien zur Prüfung und Umsetzung von Anonymisierungen etabliert sein.

Die Entscheidung ist im Internet abrufbar⁶.

1.1.6 Personalausweise mit Fingerabdrücken sind erlaubt

Fingerabdrücke dürfen nach einem Gutachten des Europäischen Gerichtshofs (EuGH) auf Personalausweisen gespeichert werden. Damit werde nicht gegen das Recht auf Privatleben im Hinblick auf die Verarbeitung personenbezogener Daten verstoßen, sagte Generalanwältin Laila Medina am 29.06.2023 in ihren Schlussanträgen.

⁶ <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62020TJ0557>



Hintergrund des laufenden Verfahrens ist eine Klage des Vereins Digitalcourage (eine Datenschutzorganisation) vor dem Verwaltungsgericht Wiesbaden. Der Kläger beanstandete, dass ihm ohne Fingerabdrücke kein neuer Personalausweis ausgestellt wird. Das Gericht hat sich in einem Beschluss⁷ vom 13.01.2022 der Argumentation des Klägers angeschlossen und Zweifel an der Gültigkeit der EU-Verordnung angemeldet, auf dem das deutsche Personalausweisgesetz basiert. Aus diesem Grund hat das Gericht dem EuGH mehrere Fragen für eine Vorabentscheidung vorgelegt (vgl. auch Tätigkeitsbericht 2022, Punkt 1.1.2).



Seit dem 02.08.2021 ist in der Bundesrepublik jeder verpflichtet, beim Beantragen eines neuen Personalausweises seine Fingerabdrücke im Einwohnermeldeamt abnehmen zu lassen. Deutschland hat damit eine Verordnung der EU umgesetzt. Die Abdrücke werden laut Bundesinnenministerium nur auf dem Ausweis gespeichert, nicht aber in einer zentralen Datenbank. Das ist nach Ansicht der Generalanwältin rechtmäßig. Es gebe keine gleichermaßen geeignete Methode, die weniger in die Privatsphäre eingreife, um das Ziel des authentischen Identitätsnachweises zu erreichen. Zudem seien die biometrischen Daten hinreichend vor Missbrauch geschützt, so die Generalanwältin. Darüber hinaus biete die VO hinreichende und geeignete Maßnahmen, die sicherstellten, dass die Erfassung, Speicherung und Verwendung biometrischer Identifikatoren wirksam vor Missbrauch oder Fehlgebrauch geschützt seien. Ferner enthalte die VO 2019/1157 keine Rechtsgrundlage für die Einrichtung oder Aufrechterhaltung nationaler Datenbanken oder einer zentralen Datenbank auf EU-Ebene. Sie führt in ihren Schlussanträgen weiter aus, dass das EU-Parlament und der Rat in dem Gesetzgebungsverfahren, das zum Erlass der VO 2019/1157 geführt hat, nicht zur Durchführung einer Folgenabschätzung nach Art. 53 Abs. 10 DS-GVO verpflichtet gewesen seien. Die DS-GVO und die VO 2019/117 seien Rechtsakte des Sekundärrechts, die in der Hierarchie der Quellen des Unionsrechts gleichrangig seien. Außerdem ergebe sich aus der DS-GVO an keiner Stelle, dass die Verpflichtung zur Durchführung einer Folgenabschätzung für den Unionsgesetzgeber verbindlich sei.

⁷ VG Wiesbaden, Beschluss vom 13.01.2022 -6 K 1563/21



Ein Urteil war bis Redaktionsschluss noch nicht ergangen. Die Richter folgen der Einschätzung der Generalanwälte oft, ob in diesem Fall auch, bleibt abzuwarten.

1.1.7 EuGH festigt DS-GVO-Grundsätze: Klarstellung bei Haftung und Schadensersatz

Im Jahr 2023 hat der EuGH gleich vier Entscheidungen zu Auslegungsfragen der DS-GVO über die Regelungen zum Schadensersatz, zur Haftung und zu notwendigen Schutzmaßnahmen getroffen, allein 3 im Dezember. Grund genug, die vier Urteile jeweils kurz zusammenzufassen.

1. In der Entscheidung (AZ: C-340/21⁸ Natsionalna agentsia za prihotide) führt der EuGH aus, dass eine Datenschutzverletzung allein nicht ausreicht, um die Unangemessenheit der Sicherheitsmaßnahmen eines Datenverarbeiters festzustellen. Gerichte müssen dann prüfen, ob die Schutzmaßnahmen der jeweiligen Datenhalter geeignet waren und diese konkret beurteilen. Hierbei hätten die Verantwortlichen die Beweislast zu tragen, dass sie die Daten genügend geschützt hätten. Auch wenn Dritte (wie z. B. Hacker) sich unbefugten Zugang verschaffen, kann die betroffene Stelle ersatzpflichtig sein, außer sie weist nach, dass sie in keinerlei Hinsicht für den Schaden verantwortlich ist. Die Befürchtung eines Missbrauchs personenbezogener Daten kann als immaterieller Schaden anerkannt werden, so der EuGH.

2. Mit der Entscheidung in der Sache C-456/22⁹ (Gemeinde Ummendorf) stärkt der EuGH das Recht auf Schadensersatz für immaterielle Schäden, indem er die Anwendung einer Bagatellgrenze für solche Schäden ausschließt. Dies stärkt den Anspruch auf Schadensersatz für Betroffene. Betroffene müssen dennoch nachweisen, dass durch die Verletzung der DS-GVO ein immaterieller Schaden entstanden ist. Für einen Schadensersatzanspruch sind das Vorliegen eines Schadens, ein Verstoß gegen die DS-GVO und ein Kausalzusammenhang erforderlich (kumulativ).

3. In der Entscheidung vom 04.05.2023¹⁰ (Österreichische Post) hat der EuGH bereits ausgeführt, dass der Betroffene mehr als ein „subjektives Un-

⁸ EuGH, Urteil vom 14.12.2023 - C-340/21

⁹ EuGH, Urteil vom 14.12.2023 - C-456/22

¹⁰ EuGH, Urteil vom 04.05.2023 - C 300/21



mutgsgefühl“ darlegen muss. Denn nicht jeder Verstoß gegen die DS-GVO reicht automatisch für einen Anspruch auf immateriellen Schadensersatz (Art. 82 DS-GVO) aus. Betroffene müssen in solchen Fällen auch immer einen Schaden nachweisen, auch wenn der nicht „erheblich“ sein muss, so der EuGH. Einer von einzelnen Gerichten geforderten Erheblichkeitsschwelle, entsprechend der Rechtsprechung des BGH zu Fällen, die nicht vom Unionsrecht beeinflusst sind und in denen eine Geldentschädigung wegen Persönlichkeitsrechtsverletzung nur bei einem schwerwiegenden Eingriff in Betracht kommt, hat der EuGH eine Absage erteilt.

Würde der Ersatz eines immateriellen Schadens von einer Erheblichkeitsschwelle abhängig gemacht, könnte dies die Kohärenz der mit der DS-GVO eingeführten Regelung beeinträchtigen. Die graduelle Abstufung einer solchen Schwelle, von der die Möglichkeit, Schadenersatz zu erhalten, abhängt, könnte je nach Beurteilung durch die angerufenen Gerichte unterschiedlich hoch ausfallen. Es widerspräche den Regelungen der DS-GVO den Ersatz eines immateriellen Schadens im Sinne des Art. 82 DS-GVO davon abhängig zu machen, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat.

Da § 50 Abs. 1 KDG und Art. 82 Abs. 1 DS-GVO nahezu wortgleich sind, ist die hier referierte Gesetzesauslegung uneingeschränkt auch für den Anwendungsbereich des KDG maßgebend.

4. Der EuGH hat in einer weiteren Entscheidung vom 21.12.2023¹¹ (Krankenversicherung Nordrhein) entschieden, dass der von Art. 82 DS-GVO gewährte Schadensersatzanspruch nur Ausgleichs- nicht aber Sanktionscharakter hat. Das bedeutet, dass der Anspruch nicht dem Zweck dient, die verantwortliche Stelle von Datenschutzverletzungen abzuhalten, sondern dass lediglich materielle und immaterielle Einbußen des von Datenschutzverletzungen Betroffenen ausgeglichen werden sollen. Dementsprechend spielt die Schwere der Rechtsverletzung für die Höhe des Schadensersatzes keine Rolle. Hat eine schwere Verletzung nur geringe Folgen, folgt daraus nur geringer Schadensersatz und umgekehrt können kleine Rechtsverletzungen auch zum Ersatz großer Schäden verpflichten.

Die Haftung des Verantwortlichen setzt zudem ein Verschulden voraus. Interessant ist hier die Umkehr der Beweislast, wonach der Verantwortliche

¹¹ EuGH, Urteil vom 21.12.2023 - C-667/21



beweisen muss, dass ihm kein Verschulden zuzurechnen ist. Beachtenswert ist, dass der Grad des Verschuldens die Höhe des Schadensersatzes nicht beeinflussen soll. Die Ausführungen des Gerichtshofs lassen den Schluss zu, dass ein Mitverschulden des Betroffenen den Schadensersatzanspruch nicht mindert.

Auswirkungen:

Die Urteile dürften weitreichende Auswirkungen auf die Praxis der Datenverarbeitung haben und betonen die Notwendigkeit eines effektiven Datenschutzmanagements. Durch das Ausschließen einer Bagatellgrenze für immaterielle Schäden bestätigt der EuGH das Recht auf Schadensersatz auch für geringfügige immaterielle Beeinträchtigungen und stärkt damit die Rechte von betroffenen Personen bei Datenschutzverletzungen weiter.

Unternehmen/Einrichtungen sollten ihre Datenschutzstrategien überdenken und sicherstellen, dass effektive Sicherheitsmaßnahmen implementiert und regelmäßig überprüft werden. Dies umfasst auch eine genaue Dokumentation, um die Geeignetheit dieser Maßnahmen beweisen zu können. Mitarbeiter sollten regelmäßig geschult werden, um das Bewusstsein für Datenschutz und die Risiken von Datenschutzverletzungen zu erhöhen.

1.2 Entwicklung des Datenschutzes in Deutschland

1.2.1 Gesetze zur Digitalisierung des Gesundheitswesens

Der Bundestag hatte in seiner Sitzung am 14.12.2023 das „Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens“ (Digital-Gesetz – DigiG) sowie das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten“ (Gesundheitsdatennutzungsgesetz – GDNG) verabschiedet. Am 02.02.2024 fand der 2. Durchgang im Bundesrat statt.

Mit dem DigiG als Artikelgesetzes soll fast ausschließlich das Fünfte Buch Sozialgesetzbuch (SGB V) erweitert, ergänzt oder geändert werden. Es sieht vor, dass die Krankenkassen ab dem 15. Januar 2025 verpflichtet sind, ihren Versicherten eine elektronische Patientenakte (ePA) zur Verfügung zu stel-



len, sofern die Versicherten nicht nach vorheriger Information innerhalb einer Frist von sechs Wochen gegenüber ihrer Krankenkasse widersprechen (Opt-Out-Regelung).

Bisher galt: Die ePA ist gemäß § 341 Abs. 1 SGB V eine versichertengeführte elektronische Akte, die den Versicherten von den Krankenkassen auf Antrag zur Verfügung gestellt wird. Die Nutzung ist für die Versicherten **freiwillig**. Das heißt, dass Bürgerinnen und Bürger derzeit nur dann eine ePA nutzen können, wenn sie diese aktiv bei ihrer Krankenkasse beantragen und ihr ausdrückliches Einverständnis abgeben. Eine Verpflichtung zur Anlage und Nutzung einer ePA bestand bisher nicht.

In der ePA können medizinische Befunde und Informationen aus Untersuchungen und Behandlungen gespeichert werden.

Das E-Rezept soll künftig mittels ePA-App abrufbar sein. Hierneben sollen aus der App heraus Gesundheitskarten, PINs und weitere Papiere beantragt werden können. Auch eine proaktive Information über das E-Rezept durch die Kassen gegenüber den Versicherten soll innerhalb der App erfolgen. Zudem soll das elektronische Rezept (E-Rezept) ab dem 1. Januar 2024 als verbindlicher Standard etabliert werden. Umfangreicher genutzt werden sollen die Telemedizin und Digitale Gesundheitsanwendungen (DiGA).

Neben der verpflichtenden Opt-Out-Regelung ist bedenklich, dass erst ab dem 1. Januar 2030 die Zugriffe und die versuchten Zugriffe auf personenbezogene Daten der versicherten Personen beziehbar protokolliert werden.

Entwurf des Gesundheitsdatennutzungsgesetz (GDNG)

Zusammen mit dem DigiG wurde auch der Entwurf des GDNG im Bundeskabinett verabschiedet.

Insbesondere das GDNG ist im Kontext des European Health Data Space (EHDS) zu sehen. Und es soll in erster Linie dazu dienen, die Nutzung von Daten zu Forschungs- und Innovationszwecken zu vereinfachen.

Einige Kernpunkte

- Eine **zentrale Datenzugangs- und Koordinierungsstelle für die Nutzung von Gesundheitsdaten** soll bürokratische Hürden abbauen und den Zugang zu Forschungsdaten erleichtern. Es sollen Daten



aus verschiedenen Datenquellen miteinander verknüpft werden können. Die Zugangsstelle soll als zentrale Anlaufstelle für Datennutzende fungieren.

- Die **federführende Datenschutzaufsicht für länderübergreifende Forschungsvorhaben** soll auf **alle Gesundheitsdaten** ausgeweitet werden. Die datenschutzrechtliche Aufsicht für länderübergreifende Forschungsvorhaben im Gesundheitswesen wird durch eine(n) Landesdatenschutzbeauftragte(n) koordiniert.
- Das **Forschungsdatenzentrum Gesundheit (FDZ)** beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) wird weiterentwickelt. Für die Antragsberechtigung ist nicht mehr ausschlaggebend, wer beantragt, sondern wofür. Entscheidend sind die im Gemeinwohl liegenden Nutzungszwecke. Das FDZ kann pseudonymisierte Daten mit den Krebsregisterdaten sowie Daten weiterer gesetzlich geregelter medizinischer Register verknüpfen, wenn dies für den antragsgemäßen Forschungszweck **erforderlich** ist und die Interessen der Versicherten hinreichend gewahrt werden.
- Für die **Datenfreigabe aus der ePA** wird ein **Opt-Out-Verfahren** eingeführt, um die Nutzung der Daten aus der ePA zu den zulässigen Zwecken des FDZ zu verbessern. Es wird eine einfache Verwaltung der Widersprüche eingerichtet, damit Patientinnen und Patienten über die Freigabe ihrer Daten für die Forschung oder weitere Zwecke an das FDZ entscheiden können.
- **Kranken- und Pflegekassen dürfen Daten verarbeiten**, wenn dies nachweislich dem individuellen Schutz der Gesundheit der Versicherten dient, zum Beispiel der Arzneimitteltherapiesicherheit oder der Erkennung von Krebserkrankungen oder seltenen Erkrankungen.

Der Gesetzesentwurf wurde im Gesundheitsausschuss des Bundestages beraten. U.a. wurden folgende Punkte von den geladenen Experten kritisiert.

1. Kritisch gesehen wurde, dass Kranken- und Pflegekassen künftig auf Grundlage der ihnen vorliegenden Abrechnungsdaten eigenständig Risikoeinschätzungen vornehmen und die Versicherten individuell beraten sollen. Es sei eine Kernaufgabe von Behandelnden gesundheitliche Risiken zu



beurteilen, so die Kritiker. Sie sprachen sich zudem für ein Opt-In-Verfahren bei dieser Form der Beratung aus. Eine Datenverarbeitung durch Kranken- und Pflegekassen und eine individuelle Ansprache dürfen nur nach vorheriger ausdrücklicher Einwilligung der Versicherten erfolgen.

2. Auch zu dem Ziel, Gesundheitsdaten, wenn auch pseudonymisiert, zusammenzuführen und der Forschung zur Verfügung zu stellen, gab es Kritik. Dass die Datenfreigabe aus der Patientenakte zu Forschungszwecken über ein Widerspruchsverfahren (Opt-Out) geregelt werden soll, wurde ebenfalls gerügt. Die Daten würden dann aus der elektronischen Patientenakte weitergeleitet und mit weiteren Daten im Forschungsdatenzentrum (FDZ) verknüpft. Angeführt wurde, dass das Teilen von Daten, von dem vor allem privatwirtschaftliche Unternehmen anstatt die Gemeinschaft profitieren, Machtasymmetrien verstärken und sich daher aus Sicht der digitalen Zivilgesellschaft gegen das Gemeinwohl richten könnte. Laut GDNG-Entwurf würden der Forschung „ausschließlich Daten übermittelt, die zuverlässig automatisiert pseudonymisierbar sind“. Fachleute kritisieren jedoch, dass sich solche Daten mit relativ geringem Aufwand wieder einer einzelnen Person zuordnen lassen. Einige wenige Datenpunkte reichten dafür aus, etwa das Alter einer Versicherten, die Postleitzahl des Wohnortes oder der Geburtstag eines Kindes.

3. Sozialverbände befürchten Interessenskonflikte, wenn sowohl die zentrale Datenzugangs- und Koordinierungsstelle als auch das Zentrum beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) angesiedelt sind, das wiederum das Bundesministerium für Gesundheit beaufsichtigt. Der Verbraucherzentrale Bundesverband (vzbv) fordert in seiner Stellungnahme zum Gesetzesentwurf, die zentrale Datenzugangs- und Koordinierungsstelle „schnellstmöglich“ in eine eigenständige Institution zu überführen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat in ihrer Stellungnahme vom 14. August 2023¹² ihre Bedenken dargelegt.

¹² https://datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf



1.2.2 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses – § 26 BDSG entspricht nicht den Anforderungen von Art. 88 DS-GVO

Der Europäische Gerichtshof (EuGH) hat eine Entscheidung zu § 23 Abs. 1 S. 1 HDSIG gefällt. Diese Vorschrift entspricht § 26 des BDSG und ist deshalb für die Anwendung der Regelung demnächst zu beachten.

Zunächst sind für das Beschäftigungsverhältnis die Regelungen des Art. 88 DS-GVO anzuwenden. Diese Vorschrift enthält aber eine Öffnungsklausel, die es nationalen Gesetzgebern erlaubt, spezifischere Vorschriften für die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis zu erlassen. Der deutsche Gesetzgeber hat dies mit der Einführung von § 26 BDSG getan. Bislang ist das Bundesarbeitsgericht auch davon ausgegangen, dass § 26 BDSG mit der DS-GVO konform geht:

„Die richtige Anwendung des Unionsrechts ist insoweit derart offenkundig, dass für vernünftige Zweifel kein Raum bleibt. Auch die bisherigen fachgerichtlichen Instanzentscheidungen sowie das datenschutz- und arbeitsrechtliche Schrifttum stellen so gut wie einheitlich nicht infrage, dass der nationale Gesetzgeber von der Öffnungsklausel des Art. 88 DS-GVO in zulässiger Weise Gebrauch gemacht hat.“¹³

Das Verwaltungsgericht Wiesbaden¹⁴ hatte diesbezüglich jedoch Zweifel und legte dem EuGH ein Vorabentscheidungsverlangen vor. Das Gericht fragt, ob eine Vorschrift auch dann als eine spezifischere Vorschrift i. S. d. DS-GVO anerkannt werden kann, wenn die Voraussetzungen des Art. 88 Abs. 2 nicht erfüllt sind. Danach muss diese spezifische Vorschrift gemäß Art. 88 Abs. 2 DS-GVO geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen enthalten.

¹³ BAG, Beschluss vom 07.05.2019 - 1 ABR 53/17

¹⁴ VG Wiesbaden, Beschluss vom 21.12.2020 - 23 K 1360/20.WI.PV



Der EuGH stellt dazu fest:

„(Es) ergibt sich aus dem Wortlaut von Art. 88 DSGVO, dass dessen Abs. 2 dem Ermessen der Mitgliedstaaten, die den Erlass „spezifischerer Vorschriften“ nach Abs. 1 dieses Artikels beabsichtigen, einen Rahmen setzt. So dürfen sich diese Vorschriften zum einen nicht auf eine Wiederholung der Bestimmungen der DSGVO beschränken, sondern müssen auf den Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen.“¹⁵

Damit entspricht § 23 Abs. 1 HDSIG nicht den Anforderungen an eine „spezifischere Vorschrift“ gem. Art. 88 Abs. 1 DS-GVO. Entgegen der Rechtsansicht des BAGs dürfte dies damit auch für den gleichlautenden § 26 BDSG gelten.

Schon im Vorgriff auf diese mögliche Antwort hatte das Verwaltungsgericht Wiesbaden gefragt, ob eine solche Norm, die den Anforderungen an Art. 88 Abs. 2 DS-GVO nicht genügt, anwendbar bleiben kann. Die klare Antwort des EuGHs: Nein!¹⁶

Diese Entscheidung mag zunächst dramatisch klingen, die praktische Relevanz ist jedoch überschaubar.

Regelmäßig werden als bestehende gesetzliche Ermächtigungsgrundlagen Art. 6 Abs. 1 lit. b) DS-GVO (Datenverarbeitung zur Erfüllung eines Vertrages) oder Art. 6 Abs. 1 lit. f) DS-GVO (berechtigtes Interesse) ausreichen. Nicht zuletzt wird die Einwilligungsvariante nach Art. 6 Abs. 1 lit. a) DS-GVO auch hier zur Verfügung.

Auswirkungen im Anwendungsbereich des KDG

Für die Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses gem. § 53 KDG hat diese Entscheidung keine Auswirkungen. Diese Vorschrift leitet sich nicht aus der Öffnungsklausel des

¹⁵ EuGH, Urteil vom 30.03.2023 - C-34/21 (Rn. 65)

¹⁶ EuGH, Urteil vom 30.03.2023 -C-34/21



Art. 88 DS-GVO ab. Die kirchliche Regelung hat ihre Berechtigung aufgrund des in Art. 91 DS-GVO geregelten Rechts der Kirchen und Religionsgemeinschaften eigene Datenschutzregelungen fortzuführen, wenn diese mit der DS-GVO in Einklang stehen. Dies ist im Hinblick auf diese Vorschrift der Fall, da die Regelungen des § 53 KDG den Wertungen der DS-GVO, wie sie sich aus Art. 6 DS-GVO ergeben, entsprechen.

1.2.3 Vorratsdatenspeicherung ist endgültig rechtswidrig

Die deutsche Regelung zur Vorratsdatenspeicherung ist in vollem Umfang unvereinbar mit der Datenschutzrichtlinie für elektronische Kommunikation und darf daher nicht mehr angewendet werden. Dies hat das Bundesverwaltungsgericht (BVerwG)¹⁷entschieden. Es folgte damit den Vorgaben des EuGHs und beendete jahrelange Diskussionen.

Das Gericht hatte zuvor den Europäischen Gerichtshofs¹⁸ angerufen (vgl. Punkt 1.2.4.unser Tätigkeitsbericht 2022). Unter Berücksichtigung der Entscheidung des EuGHs kam des BVerwG zu dem Schluss, dass das Telekommunikationsgesetz (TKG) eine anlasslose, flächendeckende sowie personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vorschreibt. Dies genüge schon deshalb nicht den unionsrechtlichen Anforderungen, weil keine objektiven Kriterien bestimmt werden, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen.

Bei der Speicherung von Telefondaten (Anrufer, Adressat, Datum und Dauer der Verbindung, Zeitpunkt der Versendung und des Empfangs einer Nachricht, genutzte Funkzellen) fehle es an der vom EuGH geforderten strikten Begrenzung der allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten auf den Zweck des Schutzes der nationalen Sicherheit.

IP-Adressen dürften laut EuGH zwar zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gespeichert werden. Die TKG-Regelung enthalte aber keine solche Beschrän-

¹⁷ BVerwG, Urteil vom 14.08.2023 -6 C 6.22

¹⁸ EuGH, Urteil vom 20.09.2022 -C 793/19; C 794/19



kung. Dies gilt laut BVerwG sowohl für die früheren als auch für die aktuellen Regelungen.

Eine unionsrechtskonforme Auslegung scheidet wegen des vom EuGH hervorgehobenen Grundsatzes der Bestimmtheit und Normenklarheit aus. Aufgrund des Anwendungsvorrangs des Unionsrechts dürfe die Regelungen im TKG daher nicht angewendet werden.

1.2.4 Ansprüche nach DS-GVO wegen eigenmächtiger Verarbeitung von Kundendaten auf privatem Account

Die Berufung über eine Klage auf Geltendmachung von Ansprüchen nach der DS-GVO wegen eigenmächtiger Verarbeitung von Kundendaten auf privatem Account hatte Erfolg. Die Nutzung von Kundendaten auf privaten Endgeräten ist unzulässig.

Das Landgericht (LG) Baden-Baden¹⁹ hat ein Unternehmen dazu verurteilt, einer Kundin die Namen ihrer Mitarbeiter zu benennen, die ihre, in dem Unternehmen erhobenen Kundendaten privat verarbeitet haben. Zudem ist das Unternehmen dazu verurteilt worden, ihren Mitarbeitern die fortgesetzte Verwendung der personenbezogenen Kundendaten auf ihren privaten Kommunikationsgeräten zu untersagen.

Der Hintergrund: Eine Kundin hatte von einem Unternehmen einen Fernseher und eine Wandhalterung gekauft. Dabei sei ihr Name und ihre Anschrift erfasst worden. Einige Tage später habe sie die Wandhalterung wieder zurückgesandt. Versehentlich sei ihr in der Folge der wesentlich höhere Kaufpreis für den Fernseher erstattet worden. Nachdem das Versehen bemerkt worden ist, schrieb eine Mitarbeiterin über ihren privaten Account eines sozialen Netzwerks noch am selben Tag eine Nachricht an die Kundin und machte sie auf das Versehen aufmerksam und bat um Rückmeldung. Darüber hinaus erhielt die Kundin ebenfalls noch an diesem Tag über Instagram eine weitere Nachricht, in der sie aufgefordert wurde, sich mit dem ‚Chef‘ der Instagram-Nutzerin in Verbindung zu setzen.

¹⁹ LG Baden-Baden, Urteil vom 24.08.2023 -Az. 3 S 13/23



Die Kundin hat mit ihrer gegen das Unternehmen gerichteten Klage die Auskunft begehrt, mitzuteilen, an welche Mitarbeiter ihre personenbezogenen Daten herausgegeben oder übermittelt wurden. Sie hat darüber hinaus beantragt, die Beklagte zu verurteilen, den Mitarbeitern die Nutzung der personenbezogenen Daten der Kundin auf privaten Kommunikationsgeräten zu untersagen.

Das Amtsgericht (AG) hat die Klage abgewiesen. Zur Begründung hat es unter anderem ausgeführt, der Auskunftsanspruch bestehe nicht, da Mitarbeiter eines Unternehmens keine „Empfänger“ im Sinne von Art. 15 Abs. 1 lit. c) DS-GVO, Art. 4 Nr. 9 DS-GVO seien. Die begehrte Verurteilung, den Mitarbeiter der Beklagten die Nutzung der personenbezogenen Daten der Kundin auf ihren privaten Kommunikationsgeräten zu untersagen, sei nicht begründet.

Hiergegen hat sich die Berufung der Klägerin gerichtet, mit der sie ihre erstinstanzlichen Anträge weiterverfolgt hat.

Das Berufungsgericht ist der Ansicht des AG nicht gefolgt. Das LG vertritt die Auffassung die DS-GVO sehe einen Auskunftsanspruch der Kundin nach Art. 15 Abs. 1 lit. c) DS-GVO vor, der sich auch darauf erstreckt, der klagenden Kundin die Mitarbeiter der Beklagten als Empfänger im Sinne von Art. 4 Nr. 9 DS-GVO zu benennen, denen gegenüber die personenbezogenen Daten der Klägerin offengelegt worden sind und die diese dann privat verarbeitet haben, indem sie diese auf einem privaten Account eines sozialen Netzwerks genutzt haben.

Grundsätzlich sind Arbeitnehmer eines für die Datenverarbeitung Verantwortlichen nicht als Empfänger anzusehen. Dies gelte aber nach der Rechtsprechung des Europäischen Gerichtshofs²⁰ nur dann, wenn sie unter der Aufsicht des Verantwortlichen und im Einklang mit seinen Weisungen die Daten verarbeiteten.

Im zu entscheidenden Fall hatte zumindest eine Mitarbeiterin der Beklagten den Kontakt zu einer Kundin eigenmächtig über ihren privaten Account hergestellt. Für die Kundin sei die Bekanntgabe der Mitarbeiternamen erforderlich, um die Rechtmäßigkeit der Verarbeitung ihrer personenbezo-

²⁰ EuGH, Urteil vom 22.06.2023 -C-579/21 (Rn. 75)



genen Daten zu überprüfen und ggf. weitere nach der DS-GVO zustehende Ansprüche gegen die Mitarbeiter geltend machen zu können. Aus diesen Gründen bestehe nach Ansicht des Gerichts ein Anspruch auf Nennung der Mitarbeiternamen.

Die Abwägung der in Rede stehenden Rechte und Freiheiten der Kundin einerseits und des Mitarbeiters andererseits führe nach der Auffassung des Gerichts dazu, dass das Interesse der Mitarbeiter, anonym zu bleiben, nicht schutzwürdig sei und gegenüber den Interessen der Kundin auf Geltendmachung ihrer Ansprüche nach der DS-GVO zurückzustehen habe.

Der Kundin stehe zudem ein Anspruch darauf zu, dass das beklagte Unternehmen ihren Mitarbeitern, die bei der Beklagten erhobene personenbezogene Daten der Klägerin auf privaten Kommunikationsgeräten verwendet haben, die fortgesetzte Verwendung untersage (§§ 823 Abs. 2, 1004 BGB analog i. V. m. Art. 6 Abs. 1 DS-GVO). Die Beklagte sei als mittelbare Handlungsstörerin verantwortlich und verpflichtet, die ihren Weisungen unterliegenden Mitarbeiter dazu anzuhalten, die weisungswidrige Verwendung der in dem Unternehmen erhobenen personenbezogenen Daten der Kundin zu unterlassen.

Das Urteil ist rechtskräftig.

1.2.5 Datenschutz im Land Sachsen-Anhalt

Auch im Land Sachsen-Anhalt ist der Landesbeauftragte für Datenschutz vom Landtag zu wählen. Die Amtszeit des letzten gewählten Landesbeauftragten in Sachsen-Anhalt ist bereits im Jahr 2018 abgelaufen. Seitdem sieht sich der Landtag nicht in der Lage, einen Nachfolger zu wählen, mit dem Ergebnis, dass diese Behörde seit nunmehr über fünf Jahren nur kommissarisch geleitet wird.

Ursprünglich sah die Landesverfassung vor, dass für die Wahl des oder der Landesbeauftragten eine zweidrittel-Mehrheit im Landtag erforderlich ist. Nachdem ein erster Kandidat in drei Wahlgängen gescheitert ist, weil er dieses Quorum nicht erreicht hat, zog er seine Kandidatur zurück. Der Landtag hat daraufhin die Landesverfassung geändert. Nunmehr reicht für die Wahl die Mehrheit der Mitglieder des Landtages.



Doch trotz dieser Reduzierung des Quorums konnte sich ein weiterer Kandidat, der kommissarische Leiter der Behörde, im letzten Jahr nicht durchsetzen, weil er die erforderliche Stimmenzahl nicht erreichte. So wird die Behörde weiterhin vom kommissarischen Leiter geführt. Dessen fachliche Kompetenz gilt als unbestritten. Jedoch fehlt es an einer Legitimierung durch eine Wahl, wie sie die Landesverfassung vorschreibt. Die Unabhängigkeit des Landesbeauftragten für Datenschutz wird damit zumindest infrage gestellt. Der Landesregierung und dem Landtag scheint diese Tatsache aber nicht wichtig zu sein, was vermuten lässt, dass auch der Datenschutz insgesamt von diesen Gremien eher als lästige Pflichtaufgabe betrachtet wird.

Derzeit gibt es keine Erkenntnisse darüber, ob das Land Bemühungen unternimmt, diesen landesverfassungs- und europarechtswidrigen Zustand zu beseitigen.

Die Verweigerungshaltung des Landes Sachsen-Anhalt ist über das Datenschutzrecht hinaus gefährlich, weil sich den Menschen im Land schwer vermitteln lässt, dass sie sich an Gesetze halten müssen, wenn sich der Gesetzgeber darüber hinwegsetzt.

1.3 Entwicklung des Datenschutzes in der Kirche

1.3.1 Auswirkungen der Änderung der kirchlichen Grundordnung

Die deutschen Bischöfe haben in der Vollversammlung des Verbandes der Diözesen Deutschlands am 22.11.2022 eine neue Rahmenordnung für eine Grundordnung erlassen. Dort formuliert Artikel 3 Abs. 2: „Vielfalt in kirchlichen Einrichtungen ist eine Bereicherung. Alle Mitarbeitenden können unabhängig von ihren konkreten Aufgaben, ihrer Herkunft, ihrer Religion, ihres Alters, ihrer Behinderung, ihres Geschlechts, ihrer sexuellen Identität und ihrer Lebensform Repräsentantinnen und Repräsentanten der unbedingten Liebe Gottes und damit einer den Menschen dienenden Kirche sein.“

Mit dieser neuen Grundordnung stellt die Kirche das Arbeitsrecht auf ein völlig neues Fundament. Aufgrund dieser neuen Ordnung hat die Religions-



oder Kirchenzugehörigkeit von Beschäftigten für Entscheidungen in ihrem Arbeitsverhältnis künftig grundsätzlich unberücksichtigt zu bleiben.

In Einstellungsgesprächen wird die Abfrage der Religionszugehörigkeit weitgehend unzulässig sein, ebenso wie das Erfragen von Familienstand und anderen personenbezogenen Daten, die nicht direkt mit der Fähigkeit zur Erfüllung der ausgeschriebenen Stelle in Verbindung stehen.

Auch soweit im kollektiven Arbeitsrecht in der MAVO die Angabe der Religionszugehörigkeit gefordert wird, sind diese Regelungen an der neuen Grundordnung zu messen und dementsprechend aus datenschutzrechtlichen Gründen unzulässig.²¹

Im Beschäftigungskontext ist die Angabe der Religionszugehörigkeit nach Verabschiedung der neuen Grundordnung grundsätzlich nur noch im Rahmen der Gehaltsabrechnung für die entsprechende Kirchensteuerabführung erforderlich. Die dort Tätigen haben über Veränderungen der Steuerpflicht (z. B. aufgrund Kirchenaustritts) Stillschweigen gegenüber Dritten zu bewahren.

1.3.2 Datenschutz und Aufgebot zur kirchlichen Eheschließung

Der Codex Juris Canonici legt fest, dass vor einer Eheschließung festzustellen ist, „dass der gültigen und erlaubten Eheschließung nichts im Wege steht“ (Can. 1066).

Can. 1067 verpflichtet die Bischofskonferenz für das Aufgebot Normen zu erlassen. Das Aufgebot ist die öffentliche Ankündigung einer beabsichtigten Eheschließung zur Aufdeckung eines etwa bestehenden Hindernisses. Dieser Verpflichtung ist die deutsche Bischofskonferenz mit der Partikularnorm zu Can. 1067 CIC (zuletzt geändert am 24.09.2002) nachgekommen.



²¹ siehe dazu Ullrich in AVR von A bis Z, Aktuelle Information, Aus der Kirche 1/2023 (Seite 9)



Gleichzeitig verpflichtet Can. 1069 alle Gläubigen, ihnen bekannte Hindernisse dem Pfarrer oder dem Ordinarius vor der Eheschließung mitzuteilen.

Das Aufgebot erfolgt nach der Partikularnorm zu Can. 1067 CIC (A.I.1.) durch Vermeldung im Sonntagsgottesdienst **oder** durch Aushang unter Angabe des Namens, des Vornamens und des Wohnsitzes der beiden Brautleute.

Jeder Geistliche mit allgemeiner Traubefugnis hat die Befugnis, aus gerechtem Grund vom Aufgebot zu dispensieren (Partikularnorm zu Can. 1067 CIC A.I.4).

Diese Regelungen haben ihren Ursprung in einer Zeit, in der die Menschen ihr Leben im Wesentlichen an ihrem Geburtsort oder zumindest in derselben Region verbracht haben. Mit zunehmender Mobilität der Menschen und überwiegend anonymer Lebensverhältnisse in Großstädten und Ballungsräumen geriet auch der Zweck des Aufgebotes in den Hintergrund. Da die aufgebauten Brautleute in ihrem Lebensumfeld weniger bekannt sind, können auch Eehinderungsgründe durch Dritte über sie nicht vorgebracht werden. Das Aufgebot erfüllt damit seine Funktion nicht mehr.

Auch im staatlichen Recht bestand bis 1998 aufgrund des damaligen Ehegesetzes die Pflicht, ein Aufgebot zu bestellen. In der Praxis wurden aber die meisten Eehinderungsgründe in den Akten beim Standesamt überprüft.

Die Verpflichtung für ein Aufgebot wurde 1998 mit der gänzlichen Aufhebung des Ehegesetzes obsolet. Der Gesetzgeber entschied sich, das Aufgebot abzuschaffen, „dessen öffentlicher Aushang nicht erforderlich und datenschutzrechtlich bedenklich ist“.²²

Für den kirchlichen Bereich stellt das Handbuch des katholischen Kirchenrechts fest, dass „das Aufgebot in der Praxis nicht mehr zur Aufdeckung von Hindernissen (führt) und verfehlt somit seinen ursprünglichen Zweck“.²³

²² BT-Drs. 13/4898

²³ Altaus in Haering, Rees, Schmitz, Handbuch des katholischen Kirchenrechts, S. 1276



Wenn der Zweck einer Verarbeitung aber weggefallen ist, stellt sich die Frage, ob die Verarbeitung personenbezogener Daten datenschutzrechtlich noch zulässig ist.

Bei der Partikularnorm handelt es sich um eine kirchliche Rechtsvorschrift, die den Regelungen des KDG dann vorgehen, wenn sie das Datenschutzniveau des KDG nicht unterschreiten.

Die Partikularnorm trifft keine Aussagen zum Datenschutz. Der Zweck der Norm wird in der Praxis nicht erreicht. Damit ist eine Erforderlichkeit für die Verarbeitung nicht gegeben.

Soweit die Partikularnorm für Geistliche die Möglichkeit vorsieht, aus gerechtem Grund vom Aufgebot zu dispensieren, ist ein solcher gerechte Grund in der Einhaltung des kirchlichen Datenschutzgesetzes zu sehen. Die Geistlichen sind deshalb gehalten, eine Einwilligung der Brautleute vor einem Aufgebot einzuholen. Wird die Einwilligung nicht erteilt, ist Dispens zu erteilen.

Willigen die Brautleute in die Verarbeitung ihrer personenbezogenen Daten in Form eines Aufgebotes ein, reicht die Einwilligung nur soweit, wie es der Zweck erfordert. Die Partikularnorm stellt es ins Ermessen des Pfarrers, ob das Aufgebot durch Vermeldung im Gottesdienst oder im Aushang der Gemeinde erfolgt. Im Gottesdienst halten sich Personen auf, die größtenteils zu der Gemeinde gehören. Eine Vermeldung des Aufgebotes dort erfüllt somit seinen Zweck eher, als eine Veröffentlichung im Aushang der Gemeinde, da auf die dortigen Veröffentlichungen auch Personen Einblick haben, die mit der Gemeinde nichts zu tun haben. Insofern ist die Veröffentlichung in der Messe als milderes Mittel der Veröffentlichung im Aushang vorzuziehen.

Dieser Betrachtungsweise stehen die Regelungen des CIC nicht entgegen, da dort die Ausgestaltung des Aufgebotes der Bischofskonferenz überlassen wird. Die Partikularnorm sieht einen Dispens ausdrücklich vor. Der Zweck dieser Normen wird effektiver und datenschutzkonform umgesetzt, wenn von den Brautleuten die Vorlage von Unterlagen des Standesamtes verlangt wird, aus denen ggf. Ehehindernisse hervorgehen.

1.3.3 Das „Löschen“ ist eine Verarbeitung im Sinne des KDG

Ein zentrales Recht der Datenschutzgesetze besteht in dem „Recht auf Löschung“. Nach Art. 17 DS-GVO und § 19 KDG kann eine betroffene Person vom Verantwortlichen verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, wenn diese insbesondere für die Zwecke, für die sie erhoben worden sind, nicht mehr erforderlich sind. Datenschutzrechtliche Vorschriften sind also verletzt, wenn personenbezogene Daten vom Verantwortlichen länger als nötig gespeichert bleiben.



Wie ist es aber, wenn personenbezogene Daten vorzeitig gelöscht werden? Zunächst steht fest, dass es sich sowohl bei der Speicherung als auch bei der Löschung um eine Verarbeitung im Sinne der gesetzlichen Vorschriften handelt.

Weiterhin stellt sich die Frage, wann eine Löschung als zu früh zu betrachten ist. Nach der gesetzlichen Regelung dann, wenn der Verantwortliche aufgrund von normierten Vorschriften zur weiteren Speicherung verpflichtet gewesen wäre.

Das schützt jedoch nicht zwingend die Betroffenen. Maßgeblich dafür, ob diese in ihren Rechten verletzt sind, ist der jeweilige Schutzzweck der Norm.

Aufbewahrungsfristen, die im Steuer- oder Handelsrecht oder in Förderungsrichtlinien festgeschrieben sind, dienen primär staatlichen Interessen, wie der der Sicherung von Staatseinnahmen oder des Wirtschaftsverkehrs oder der Einhaltung von Subventionsrichtlinien. Ein Schutz personenbezogener Daten ist damit nicht beabsichtigt, so dass damit kein Beschwerderecht gem. § 48 KDG (Art. 77 DS-GVO) begründet werden kann. Dazu stellt das Datenschutzgericht der Deutschen Bischofskonferenz fest: „Das Recht auf informationelle Selbstbestimmung, dessen Schutz das Datenschutzrecht nach § 1 KDG dient, kann durch eine Löschung von gespeicherten Daten nicht verletzt sein, weil durch Löschung der datenschutzrechtlich rechtfertigungsbedürftige Persönlichkeitseingriff ja gerade beendet wird.“²⁴

²⁴ Urteil des DSG-DBK 04/2022 vom 03.01.2023

**Fazit:**

Damit bleibt festzustellen, dass eine Beschwerdebefugnis auf der Grundlage des KDG (der DS-GVO) betroffenen Person nur bei einer Überschreitung von Aufbewahrungspflichten zusteht. Also dann, wenn eine Verarbeitung dieser personenbezogenen Daten nicht mehr erforderlich ist. Eine Beschwerdebefugnis bei einer Unterschreitung scheidet hingegen aus.

2 Datenschutz allgemein

2.1 Recht am eigenen Bild und Betreuung

Im Berichtszeitraum erreichte uns die Frage, welche Punkte zu beachten sind, wenn von betreuten Personen Fotos veröffentlicht werden sollen, z. B. in einem Werbeflyer einer Einrichtung oder auf einer Webseite.

In Deutschland gilt das Recht am eigenen Bild und gehört zum Schutz der Persönlichkeitsrechte eines Menschen. Es besagt: Jeder ist frei, darüber zu entscheiden, ob und wie jemand sein Bild verwendet. Die rechtliche Grundlage ist § 1 Abs. 1 des Grundgesetzes (GG). Auf einer anderen Ebene greift das Kunsturhebergesetz (KUG), das neben dem Schutz von Kunstwerken auch das Recht am eigenen Bild regelt. Mit diesen Gesetzesbestimmungen wird Missbrauch vorgebeugt.

Zulässig ist die Veröffentlichung unabhängig von den gesetzlich geregelten Fällen (z. B. §§ 23 und 24 KUG) dann, wenn der Betroffene hierzu seine **Einwilligung erteilt** hat.

Problematisch kann bei betreuten Personen die Einwilligungsfähigkeit sein. Einwilligungsfähig ist der betreute Mensch, wenn er hinsichtlich des Gegenstandes seiner Einwilligung -also der Veröffentlichung eines bestimmten Bildnisses- einsichts- und urteilsfähig ist. Betreute müssen verstehen können, in welchem Umfang und auf welche Art und Weise das Veröffentlichen erfolgen soll. Sie müssen zudem übersehen können, welche Folgen das Veröffentlichen für ihn haben könnte. Die Einwilligungsfähigkeit der Betreuten ist daher konkret und bezogen auf den Einzelfall zu prüfen. Ist diese gegeben, muss sie zwingend eingeholt werden.



Ist ein Mensch, dessen Bildnis veröffentlicht werden soll, hinsichtlich der Entscheidung für oder gegen eine Veröffentlichung als nicht einsichtsfähig anzusehen, stellt sich die Frage, ob eine stellvertretene Einwilligung in Betracht kommt. Das Erteilen einer Einwilligung durch einen Betreuer ist nicht per se ausgeschlossen.

Eine stellvertretende Einwilligung in das Veröffentlichende eines Bildnisses eines Betreuten setzt aber voraus, dass der Aufgabenkreis des Betreuers bzw. die Vollmacht eines Bevollmächtigten ein derartiges Handeln umfasst. Hiervon kann ausgegangen werden, wenn eine Betreuung für Angelegenheiten der Personensorge oder für alle Angelegenheiten besteht. Besteht die Betreuung nur für die Vermögenssorge, Gesundheitsvorsorge oder Wohnungsangelegenheiten dann eher nicht.

Bei dem Entschluss für oder gegen das Erteilen einer Einwilligung muss sich der Betreuer auch bei dieser Entscheidung am Wohl der betreuten Person orientieren. Gem. § 1901 Abs. 3 BGB hat sich der Betreuer nach den Wünschen des betreuten Menschen zu richten, sofern diese dessen Wohl nicht zuwiderlaufen und sich mit diesem zu besprechen. Konstellationen, in denen eine Veröffentlichung gegen den Willen des Betreuten seinem Wohl entspricht und mithin seinen Interessen dient, sind kaum ersichtlich. Wünscht der Betreute keine Veröffentlichung scheidet eine Erteilung einer Einwilligung generell aus.

Es gibt aber auch keinen Grund, betreuten Menschen wegen abstrakten Gefahren von Missbrauch, die heutzutage bei jeder Veröffentlichung von Bildnissen bestehen, etwas zu verwehren, für das sich jeder nicht betreute Mensch frei entscheiden kann. Das gilt jedoch nicht, wenn sich aus der Sicht des Betreuers für den Betreuten durch die Veröffentlichung eine konkrete, erhebliche Gefährdung dessen Interessen ergibt, z. B. wenn sein Aufenthaltsort geheim gehalten werden muss.

Was gilt jedoch, wenn der Betreute aufgrund seines Zustands nicht mehr in der Lage ist seine Wünsche zu äußern? Sofern der Betreuer aufgrund seines ihm übertragenen Aufgabenkreises entscheiden darf, ob ein Foto veröffentlicht werden darf, hat er sich am mutmaßlichen Willen der betreuten Person zu orientieren. Sofern ein mutmaßlicher Wille nicht erkennbar ist, hat eine Erteilung einer Einwilligung zur Veröffentlichung zu unterbleiben,



sofern es nicht dem Wohl der betreuten Person entspricht. Dies dürfte nur in Ausnahmefällen der Fall sein, z. B. bei Abgängigkeit einer dementen Person aus einer Einrichtung, um die Suche nach dieser durch das Veröffentlichen eines Fotos zu unterstützen.

Es besteht auch die Möglichkeit den Aufgabenkreis des Betreuers um den Aufgabenbereich „Personensorge“ (oder auch kleinteiliger, ggf. nur konkret für diesen Bereich Bild- und Filmaufnahmen, da das auch der Erforderlichkeit eher genügen könne) erweitern zu lassen. Die muss jedoch beim zuständigen Amtsgericht anregt werden, § 1901 Abs. 5 S. 2 BGB. Wird dem stattgegeben, stände im Zweifel einer ersetzenden Einwilligung durch den gesetzlichen Betreuer nichts entgegen. Aber auch in diesem Fall muss dies dem tatsächlichen (oder mutmaßlichen) Willen des Betreuten entsprechen.

Fazit:

Im Ergebnis ist festzuhalten, dass das Anfertigen und Veröffentlichen eines Bildnisses einer betreuten Person entweder seiner Einwilligung bzw. die seines Betreuers bedarf, wenn der Betreute als nicht einsichtsfähig anzusehen ist. Der Betreuer hat sich am Wohl der betreuten Person und mithin auch nach dessen Wünschen zu orientieren. Im Zweifel sollte auf eine Veröffentlichung lieber verzichtet werden.

2.2 Maß- und zwecklose Datenerhebung bei Schuleingangsuntersuchungen

Unsere Dienststelle ist eine Aufsicht spezifischer Art gem. Art. 91 Abs. 2 DS-GVO. In erster Linie wacht unsere Dienststelle über die Einhaltung der Vorschriften des Kirchlichen Datenschutzes. Jedoch gibt es immer wieder Berührungspunkte mit staatlichen Vorschriften. Im Schulbereich sind das u.a. die Schulgesetze der Länder sowie in dieser Angelegenheit auch die Gesetze der Gesundheitsämter (Gesundheitsdienstgesetze).

In der Vergangenheit gab es Hinweise von Sorgeberechtigten und kirchlichen Schulträgern, dass besonders im Rahmen von Schuleingangsuntersuchungen (SEU) personenbezogene Daten erhoben werden, die für den Zweck der Feststellung der Schulfähigkeit nicht erforderlich scheinen.



Demnach sah sich unsere Dienststelle auch im Rahmen des Informationsfreiheitsgesetzes dazu veranlasst nachzufragen, welche Daten in diesem Zusammenhang erhoben werden.

Die Schuleingangsuntersuchungen fallen in die Zuständigkeit der Gesundheitsämter bzw. in die der Landesverwaltungsämter. Bei der Durchführung von SEU werden personenbezogene Daten und personenbezogene Daten besonderer Kategorie des Kindes sowie auch der Sorgeberechtigten verarbeitet. Die Verarbeitung personenbezogener Daten besonderer Kategorie darf im KDG sowie auch in der DS-GVO nur unter bestimmten Voraussetzungen erfolgen. Vorrangiges Ziel der Schuleingangsuntersuchungen ist es, die Schulfähigkeit eines Kindes festzustellen. Dazu werden Angaben zur Entwicklung, frühere Erkrankungen und ggf. sonstige Besonderheiten des Kindes benötigt. Alle Angaben, die lediglich hilfreich, aber nicht erforderlich sind, dürfen nicht erhoben werden.²⁵

So werden bei einigen Ämtern u.a. Angaben zur Schwangerschaft und zum Geburtsverlauf erhoben. Dabei soll die Mutter Angaben über ihre Erkrankungen in der Schwangerschaft, zum Geburtsverlauf und zur Art der Geburt machen. Es wird auch sehr umfangreich danach gefragt, in welchem Land Mutter, Vater und Kind geboren sind sowie welcher Nationalität die Eltern angehören. Begründet wurde dies u.a. damit, dass diese Faktoren einen „enormen Einfluss auf die Gesundheit und Entwicklung eines Kindes haben und daher unerlässlich sowohl für die ärztliche Beurteilung als auch für die daraus abgeleiteten Empfehlungen eventueller (Förder-) Maßnahmen sind“. Lassen sich die gesundheitliche Entwicklung des Kindes aus den gesundheitlichen Angaben der Mutter ableiten?

Eine kursorische Nachfrage bei betroffenen Sorgeberechtigten hat ergeben, dass der Fragebogen auch ohne die Beantwortung der Fragen zu Schwangerschaft und Geburtsverlauf vom Gesundheitsamt akzeptiert worden ist.

Unter Umständen kann es hilfreich sein, zu wissen, dass es während Schwangerschaft und Geburt Vorkommnisse gab, die einen Einfluss auf die

²⁵ L & D Niedersachsen, 26. Tätigkeitsbericht 2020, Punkt. 5.3



Entwicklung des Kindes haben können (z.B. Frühgeburt). Eine über die notwendigen Daten hinausgehende freiwillige Angabe wäre daher für diese Fragen zu begrüßen.

In den Hinweisen zur Datenerhebung zum Elternfragebogen den Sorgeberechtigten waren jedoch kein Zweck und keine Rechtsgrundlage genannt, die die Angaben zu Erkrankungen der Mutter in der Schwangerschaft sowie zur Art der Geburt und Geburtsverlauf rechtfertigen. Gem. Art. 13 DS-GVO hat die Gesundheitsbehörde die Betroffenen bei Erhebung der personenbezogenen Daten u.a. auch über die Zwecke der Verarbeitung zu unterrichten. Eine reine Erklärung oder Darlegung, dass diese Angaben erforderlich sind, ist keine ausreichende Rechtsgrundlage.

Bei anderen Ämtern wurde anlässlich der SEU danach gefragt, wie lange das Kind gestillt wurde und ob Eltern oder auch Geschwister Allergien hätten. Auch diese Fragen beschränken sich nicht auf das erforderliche Maß zu beurteilen, ob das Kind eingeschult werden kann. Zwar waren diese Fragen freiwillig, jedoch schließt die Situation, in der sich die Eltern einzuschulender Kinder befinden, eine Freiwilligkeit aus. Im dazugehörigen Handbuch war auch dargelegt, dass diese Daten aus dem Fragebogen auch für Zwecke der Gesundheitsberichtserstattung dienen und folglich für die reine Schuluntersuchung nicht erforderlich sind.

Dem zuständigen Verwaltungsamt wurde aufgrund unserer Anfrage die Empfehlung ausgesprochen, die Fragen für die Gesundheitsberichtserstattung (statistische Zwecke) gesondert auf einen Fragebogen zu erheben. Die Unabhängigkeit dieser Angaben für statistische Zwecke von der Schuluntersuchung kann somit besser von den betroffenen Eltern nachvollzogen werden.

Erfreulicherweise gibt es auch Länder, die in der Vergangenheit dieses Thema bereits thematisiert hatten und ihre Fragebögen dementsprechend gestaltet haben. So sind diese Fragen, die über den reinen Zweck hinausgehen, deutlich als freiwillig gekennzeichnet oder werden auf gesonderten Bögen erhoben.

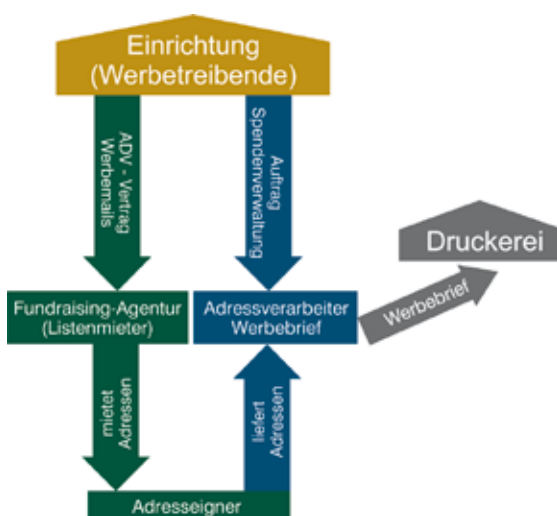
2.3 Werbesendungen von Wohltätigkeitsorganisationen

Kirchliche Wohltätigkeitsorganisationen starten regelmäßig Spendenauf-rufe, um deren Aufgaben und Projekte zu finanzieren. Die Spendenauf-rufe sollen eine Vielzahl von Menschen erreichen, unabhängig von ihrem Glau-ben. Neben Spendenaufrufen im Fernsehen, Internet oder sozialen Medien erhalten viele Personen auch Spendenbitten als Briefe von den kirchlichen Einrichtungen. Dabei handelt es sich keinesfalls um Postwurfsendungen, die eine Vielzahl von Personen erreichen soll, sondern um die gewerbsmä-ßige Nutzung von Adressen.

In einem an uns herangetragenem Fall enthielt die Spendenbitte den Na-men, das Geschlecht und die Anschrift der betroffenen Person. Als Absen-der war zweifelsfrei ein Caritasverband zu erkennen, da der Brief das Logo, die Anschrift, Kontaktdaten wie Telefon- und Faxnummer und sogar ein Foto sowie die digitale Unterschrift des Vorstandes enthielt.

Dieser Verband hatte einen Dienstleister damit beauftragt ein Weihnachts-mailing mit einer Spendenbitte für Obdachlose zu verschicken. Das klingt erstmal nicht weiter ungewöhnlich. Da uns der Petent jedoch mitteilte der Nutzung seiner personenbezogenen Daten durch diese Einrichtung für Spendenbitten bereits im Vorjahr widersprochen zu haben, schauten wir uns das gesamte Konstrukt sowie die Widerspruchsregelung genauer an.

Die Rechtsbeziehung gestaltete sich wie folgt:



Der Caritasverband beauftragt eine Fundraising-Agentur mit dem gesamten Management des Weihnachtsmailings. Der Inhalt und auch die Form dieses Mailings wird dabei durch die Fundrai-sing-Agentur gestaltet. Zwischen beiden Parteien wurde ein Auftragsdatenverarbeitungsvertrag geschlossen, wonach die Caritas der Auftraggeber und die Fundraising-Agentur der Auftragnehmer ist. Gegenstand dieses Vertrages ist die Verarbei-tung und Nutzung personenbezogener Daten für



Marketingmaßnahmen durch die Fundraising-Agentur nach Weisung des Caritasverbandes. Datenschutzrechtlich verantwortlich ist durch den ADV-Vertrag die Caritas.

Um einen besonders großen Personenkreis mit einem solchen Mailing zu erreichen, mietet die Fundraising-Agentur im Namen des Verantwortlichen weitere Adressen bei einem sog. Adresseigner an. Der Adresseigner übermittelt die Adressen nicht an die Fundraising-Agentur, sondern an einen weiteren Auftragnehmer des Verantwortlichen. Dieser Auftragnehmer hatte mit dem Caritasverband ebenfalls einen Vertrag geschlossen. Die Caritas beauftragte diesen Dienstleister mit der gesamten Spendenverwaltung, dem Einpflegen der Adressen auf den Werbebriefen sowie dem Aussortieren der Adressen, bei denen ein Widerspruch vorliegt.

Die nun fertigen Werbebriefe werden von dem Dienstleister an eine Druckerei geschickt, die wiederum von der Fundraising-Agentur beauftragt worden ist, diese Werbebriefe zu drucken und über den Postversand zu verteilen.

Berücksichtigung der Rechtsansprüche

In dem oben genannten Fall war der Caritasverband der Meinung, dass Widersprüche an den Adresseigner zu richten sind. Der Werbebrief enthielt im Kleingedruckten am rechten Seitenrand die Information woher die personenbezogenen Daten des Adressaten stammen und das dorthin auch die Widersprüche zu richten sind. Eine erkennbare Möglichkeit, Widerspruch beim Werbetreibenden und offensichtlichen Absender des Briefes - der Caritas - einzulegen, war nicht benannt.

Unsere Dienststelle hat daraufhin festgestellt, dass Widersprüche auch an die kirchliche Einrichtung (dem Werbetreibenden) gerichtet werden können und dass kirchliche Einrichtungen Maßnahmen etablieren müssen, um Widersprüche zu berücksichtigen. Der Caritasverband verarbeitet zwar in dieser Konstellation die personenbezogenen Daten nicht selbst, legt aber als Werbetreibender den Zweck und die Mittel der Marketingmaßnahmen fest. Zudem entscheidet die Organisation über die Werbebotschaft und den Empfängerkreis. Zusammen mit dem Adresseigner ist die kirchliche Einrichtung gemeinsamer Verantwortlicher nach § 28 KDG. Somit kann die



betroffene Person ihre Rechte (z.B. Widerspruch gegen die Verarbeitung, Auskunftsrechte etc.) gegenüber jedem der Verantwortlichen geltend machen.

In diesem Verfahren hatte der Verband als Verantwortlicher keine geeigneten Maßnahmen getroffen, um geltend gemachte Rechtsansprüche zu berücksichtigen. Ein Betroffener, der keine Werbesendungen von speziell dieser kirchlichen Einrichtung erhalten möchte, verbindet den Widerspruch nicht damit, dass er keine Werbesendung von dem Adresseigner bekommen möchte, sondern eben damit, dass er keine Werbung von der Caritas erhält. Das komplizierte Rechtskonstrukt sowie die gemeinsame Verantwortlichkeit sind in der Regel den betroffenen Bürgern nicht klar.

Sperrdateien

Unklar war in diesem Zusammenhang auch, ob einer der Verantwortlichen sog. Sperrdateien führen und diese dem weiteren Verantwortlichen übermitteln darf. Geht z.B. der Widerspruch beim Adresseigner ein, so wird der Betroffene bei dem Adresseigner gesperrt, d.h. er erhält keine Werbesendung mehr von diesem. Für den Fall, dass sich die werbetreibende Einrichtung vom Adresseigner trennt, gab es keine Lösung. Bei der Beauftragung eines neuen Adresseigners, der sich wiederum Adresslisten anmietet, kann der Betroffene wieder unerwünschte Werbepost erhalten. Um die Betroffenenrechte zu wahren, kann eine Sperrdatei aufgrund von § 23 Abs. 3 KDG (Widerspruch gegen Direktwerbung) in Verbindung mit § 19 Abs. 3 lit. b) KDG zur Berücksichtigung von Widersprüchen betroffener Personen und zur Sicherstellung der Beachtung des geltend gemachten Rechtsanspruchs zulässig sein.

Die betroffenen Personen sind bei der Widerspruchsbestätigung darüber zu informieren, dass ihre Daten in einer solchen Sperrdatei verarbeitet werden, um den Widerspruch nachhaltig zu erfüllen.

Fazit:

Kirchliche Hilfs- und Wohltätigkeitsorganisationen sind auf Spenden angewiesen. Diese finanzieren einen bestimmten Teil ihrer Arbeit. Es ist auch gerechtfertigt Personen mit Werbebriefen anzuschreiben, so lange die



datenschutzrechtlichen Bestimmungen eingehalten und die Informationspflichten erfüllt werden.

Trotzdem kann die datenschutzrechtliche Verantwortlichkeit nicht nur auf den Adressgeber abgestellt werden, sondern muss auch bei der jeweiligen Organisation Berücksichtigung finden.

Verbraucher, die keine unerwünschten Werbebriefe erhalten möchten, können sich auf die sog. Robinsonliste²⁶ eintragen. Dies ist eine Liste, die Verbraucher vor unaufgeforderten Werbeaufrufen und Telefonanrufen schützt. Seriöse Adressgeber gleichen ihre Adressen regelmäßig mit dieser Liste ab und setzen ggf. Sperrvermerke.

3 Datenschutzaufsicht

3.1 Rechtsform und Unabhängigkeit der kirchlichen Datenschutzaufsicht

Das KDG legt jedem Diözesanbischof die Pflicht auf, für den Bereich seiner Diözese einen Datenschutzbeauftragten als Leiter der Datenschutzaufsicht zu bestellen (§ 41 Abs. 1 KDG). Dieser übt seine Tätigkeit laut Gesetz in organisatorischer und sachlicher Unabhängigkeit aus. Die Dienstaufsicht ist dabei so zu regeln, dass die Unabhängigkeit nicht beeinträchtigt wird (§ 42 Abs. 1 KDG). Eine Regelung dazu, in welcher Rechtsform die Datenschutzaufsichten einzurichten sind, schreibt das Gesetz nicht vor.

Nur wenn die Kirchen eine unabhängige Aufsichtsbehörde etablieren, unterliegen sie nicht der staatlichen Datenschutzaufsicht.

Der Europäische Gerichtshof (EuGH) formulierte dazu:

„Die ... erforderliche Unabhängigkeit soll ... nicht nur die unmittelbare Einflussnahme in Form von Weisungen ausschließen, sondern auch, ... jede Form der mittelbaren Einflussnahme, die zur Steuerung der Entscheidungen der Kontrollstelle geeignet wäre.“²⁷

²⁶ <https://www.robinsonliste.de/>

²⁷ EuGH 16.10.2012 C-614/10



„...schon die bloße Gefahr einer politischen Einflussnahme auf die Entscheidung der Kontrollstelle ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen.“²⁸

Mit diesen deutlichen Vorgaben der Rechtsprechung ist es für eine Datenschutzaufsicht unvereinbar, egal in welcher Rechtsform sie organisiert ist, ein wie auch immer geartetes Kontrollgremium vorzusehen.

Im staatlichen Bereich sind die Datenschutzaufsichten in unterschiedlichen Rechtsformen organisiert. Allen gemeinsam ist aber, dass es über der Aufsicht kein Gremium gibt, welches die Datenschutzaufsicht kontrollieren oder ihr Vorgaben machen kann.

Auch die Kirchliche Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs ist in diesem Sinne unabhängig und weisungsfrei. Auch ohne oder gerade weil sie nicht als Körperschaft oder Anstalt organisiert ist, bestehen keine Aufsichtsgremien über dieser Einrichtung. Auch hat seit Bestehen dieser Aufsicht niemals ein Versuch der Einflussnahme durch kirchliche Stellen stattgefunden.²⁹

3.2 Wirksame Einreichung einer Datenschutzbeschwerde

Im Berichtsjahr sowie auch in den Jahren zuvor war eindeutig der Trend zu beobachten, dass sich Bürger bzw. betroffene Personen über Datenschutzverletzungen oder unrechtmäßige Datenverarbeitungen nicht nur bei unserer Aufsichtsbehörde zunehmend beschweren.

Normalerweise nutzen Petenten dafür unser Beschwerdeformular auf unserer Webseite, schicken uns ein Fax, eine E-Mail oder einen Brief. Auch durch Anrufe oder Übermittlung von anderen Aufsichtsbehörden werden uns Beschwerden sowie auch Datenschutzverstöße mitgeteilt. Denn nach § 48 Abs. 1 KDG hat jede betroffene Person das Recht auf Beschwerde bei der Datenschutzaufsicht, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen Vorschriften des KDG oder gegen andere Datenschutzvorschriften verstößt.

²⁸ EuGH 08.04.2014 – RS C-288/12 Rn. 53

²⁹ <https://artikel91.eu/2023/02/15/verwaltung-der-aufsicht-durch-die-beaufsichtigten/>



Zudem kann sich die betroffene Person grundsätzlich auch an jede Aufsichtsbehörde wenden, unabhängig davon, ob diese für die betroffene Person oder die verantwortliche Stelle zuständig ist oder nicht. Jede empfangende Behörde ist verpflichtet, die entsprechende Beschwerde oder den Vorfall an die zuständige Behörde zu übermitteln.

Ob wir den direkt erhaltenen oder übermittelten Vorfall dann als Datenschutzbeschwerde oder Prüfungsanregung einordnen, ist im Tätigkeitsbericht 2021 unter Punkt 3.1 nachzulesen. Nach den Verfahrensgrundsätzen aus § 4 KDS-VwVfG³⁰ kann die Aufsicht nach pflichtgemäßem Ermessen entscheiden, ob und wann sie tätig wird. Die Aufsicht ist jedoch verpflichtet tätig zu werden, wenn ein Amtsermittlungsgrundsatz besteht.

Ferner kommt es vor, dass uns E-Mails erreichen, in denen unsere E-Mail-Adresse ins CC-Feld eingetragen ist.

Die Abkürzung CC bedeutet „carbon copy“ – übersetzt Durchschrift. Den Inhalt der Mail bekommt der Adressat somit „nur“ zur Information oder Kenntnisnahme.

Somit ist unsere Aufsichtsbehörde nicht der eigentliche Adressat dieser E-Mail und hat lediglich eine Durchschrift bekommen. Erfolgt zudem keine direkte Ansprache und erfüllt das Anliegen nicht die Anforderungen, die an eine Beschwerde gestellt sind, so kann diese E-Mail nicht als Beschwerde angesehen werden. Objektiv betrachtet liegt der Datenschutzaufsicht damit eher ein Hinweis vor und keine Beschwerde. Die Datenschutzaufsicht wird den Absender darauf hinweisen, dass die Beschwerde konkretisiert und direkt an sie gerichtet werden muss, bevor diese gegenüber den Beschwerdegegner tätig werden kann.

3.3 Vor-Ort-Besuche der Datenschutzaufsicht

In einem Fall hat unsere Dienststelle eine Vor-Ort-Kontrolle des Büros einer MAV gegenüber der Vorsitzenden angekündigt. Der Termin sollte in vierzehn Tagen stattfinden. Die MAV-Vorsitzende teilte daraufhin mit, an diesem Tag verhindert zu sein. Die Aufsicht möge zwei weitere Termine zur Auswahl angeben. Im Rahmen eines Telefonates zwischen der Aufsicht und

³⁰ Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz



der MAV-Vorsitzenden sollte dann eine Terminabsprache stattfinden. Dabei stellte sich heraus, dass die Vorsitzende nicht bereit war, einen zeitnah akzeptablen Termin zu benennen. Auch war sie nicht bereit ihre Stellvertreterin oder ein anderes MAV-Mitglied diesen Termin wahrnehmen zu lassen. Der Aufsicht wurde im Ergebnis ein Termin in sechs Wochen angeboten.

Die Datenschutzaufsicht wacht gemäß § 44 Abs. 1 KDG über die Einhaltung der Vorschriften des Gesetzes über den kirchlichen Datenschutz sowie anderer Vorschriften über den Datenschutz und führt u.a. Untersuchungen in Form von Datenschutzüberprüfungen durch.

Gemäß § 44 Abs. 2 lit. b) KDG sind die in § 3 Absatz 1 genannten kirchlichen Stellen verpflichtet, im Rahmen ihrer Zuständigkeit die Datenschutzaufsicht bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihr ist dabei, insbesondere Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme. Der Datenschutzaufsicht ist zudem während der Dienstzeit zum Zwecke von Prüfungen Zutritt zu allen Diensträumen, die der Verarbeitung und Aufbewahrung automatisierter Dateien dienen, zu gewähren. Bei einem Verstoß gegen diese Bestimmungen kann nach § 51 Abs. 1 KDG die Datenschutzaufsicht eine Geldbuße verhängen.

Für die kirchlichen Einrichtungen, die unter den sachlichen Anwendungsbereich des KDG fallen, wird durch das KDG also eine Mitwirkungsverpflichtung vorgeschrieben. In dieser Vorschrift ist nicht vorgesehen, dass der Verantwortliche gem. § 4 Nr. 9 KDG ein Mitspracherecht hinsichtlich der Anweisungen der Aufsicht besitzt. Das Gesetz ist insoweit eindeutig als danach die Aufsicht **anweist** und der Verantwortliche **Folge leistet**. Keineswegs ist also die Aufsicht verpflichtet, diesbezügliche Vereinbarungen mit dem Verantwortlichen zu treffen.

Die Mitarbeitervertretung ist nach der h. M., der sich unsere Dienststelle anschließt, Teil des Verantwortlichen und nicht selbst Verantwortlicher i. S. d. § 4 Nr. 9 KDG. Nach dem vom Interdiözesanen Datenschutzgericht wiederholt anerkannten Funktionsträgerprinzip haftet der Verantwortliche für das Handeln von Beschäftigten. Dies gilt auch dann, wenn die Beschäftigten keine leitende Funktion innehaben.



Die Weigerungen, den Anweisungen der Datenschutzaufsicht zu folgen und der Datenschutzaufsicht während der Geschäftszeiten Zutritt zu gewähren, stellen je für sich einen Verstoß gegen die Bestimmungen des KDG dar.

Dem Geschäftsführer der Einrichtung als Verantwortlichem wurde deshalb die Verhängung eines Bußgeldes für den Fall angekündigt, dass sich die MAV weiterhin weigert, der Aufsicht zu dem angekündigten Termin Zutritt zum MAV-Büro zu verschaffen. Erst nach diesem Hinweis und den Ausführungen des Geschäftsführers gegenüber der MAV gegebenenfalls eine arbeitsrechtliche Klärung herbeizuführen und die MAV für eventuelle Bußgelder in Regress zu nehmen, führte dazu, dass der Termin wie geplant stattfinden konnte.

Unserer Aufsicht ist an einer konstruktiven Zusammenarbeit mit den Einrichtungen, die dem KDG unterliegen, und deren Mitarbeitern gelegen. Dies setzt aber gegenseitigen Respekt voraus. Wenn versucht wird, die Aufsicht „am langen Arm verhungern zu lassen“, wird das diesem Anspruch nicht gerecht. In einem solchen Fall werden dann die Mittel, die uns das Gesetz bietet, in einer Weise durchgesetzt, die eine Klärung der Verhältnisse gewährleistet.

3.4 Prüfkation der Datenschutzaufsicht

3.4.1 Prüfung eines Caritas Regionalzentrums

Auch in diesem Berichtszeitraum haben wir angekündigte Vorortprüfungen vorgenommen. So wurde wieder ein Caritas Regionalzentrum überprüft. Über das Regionalzentrum werden verschiedene Leistungen angeboten, wie z. B. eine allgemeine soziale Beratung, eine Schuldnerberatung sowie Migrationsberatung.

Die Prüfung hat folgende Ergebnisse ergeben:

Mitgeteilt worden ist, dass ein Verzeichnis für Verarbeitungstätigkeiten derzeit durch die Einrichtungsleitung gemeinsam mit dem betrieblichen Datenschutzbeauftragten erstellt wird. Eine Fertigstellung ist im ersten Quartal 2024 geplant. Dieses wird uns nach Fertigstellung vorgelegt.



IT Infrastruktur

Die Einrichtung arbeitet mit Microsoft 365 und nutzt als Datenablage einen MS SharePoint. Die Daten werden in der europäischen Cloud gespeichert. Zusätzlich gibt es noch ein Altsystem (Server). Die Daten vom Altsystem werden zu MS SharePoint migriert.

Es wurde der Hinweis erteilt, dass die alte Festplatte noch eine gewisse Zeit als Datensicherung aufbewahrt werden sollte, da es bei der Migration großer Datenmengen häufig zu Fehlern kommen kann, die erst zu einem späteren Zeitpunkt festgestellt werden.

Es wurde zusätzlich darauf hingewiesen, dass unbedingt eine Backup-Strategie und ein Fallback-Szenario erstellt werden sollte. Der Cloud-Anbieter ist nicht der Datenverantwortliche.

Technische Organisatorische Maßnahmen

Zum Gebäude der Einrichtung und damit zu den Räumen der einzelnen Berater ist kein freier Zutritt möglich. Es gibt eine Klingelanlage.

Es gibt ein Schlüsselprotokoll. Es gelten folgende Regelungen: Beim Verlassen des Büros sind diese abzuschließen. Akten, die zur Bearbeitung nicht benötigt werden, sind einzuschließen. Es gilt die Clean-Desk-Policy. Bildschirmschoner werden genutzt (Abschaltung nach 5 Minuten), zudem können Mitarbeitende ihre Arbeitsplätze aktiv sperren. Es gibt eine Dienst-anweisung, dass Klientenakten nicht auf den Schreibtischen liegen dürfen, wenn mit diesen nicht gearbeitet wird.

Der Drucker, welcher sich im Wartebereich befindet, ist passwortgeschützt.

Die Post wird zentral entgegengenommen und ungeöffnet über Postmappen an die Bearbeiter weitergegeben, wenn auf diesen der Namen und/oder der Zusatz "persönlich" vermerkt ist.

Für jeden Mitarbeitenden gibt es einen persönlichen Zugang zum IT-System (MS 365 Accounts) und je nach Abteilung die entsprechenden Berechtigungen (Zugriffsrechte).

Zugriffe auf Anwendungen, Eingaben, Änderungen und Löschungen von Daten werden protokolliert.



Papierakten werden in verschlossenen Schränken im Archiv gelagert. Dort steht auch eine Datentonne. Die Mitarbeiter sind angewiesen, sensible Unterlagen dort täglich zu entsorgen.

Es wurde darauf hingewiesen, dass im Archiv Maßnahmen gegen eine ungewollte Zerstörung oder Vernichtung von Daten getroffen werden müssen. So ist beispielsweise ein Feuerlöscher vorzuhalten. Der Brandschutz ist besonders in dem Bereich zu überprüfen.

Die private Nutzung von IT-Geräten und Handys ist untersagt. Ebenso die private Nutzung dienstlicher Geräte sowie auch die Nutzung der dienstliche E-Mailadresse zu privaten Zwecken.

Verarbeitung personenbezogener Daten von Klienten

Erwähnt worden ist, dass die Kommunikation mit Behörden schriftlich oder mit entsprechender Verschlüsselung der personenbezogenen Daten erfolgt, da diese meistens zur besonderen Kategorie personenbezogener Daten gehören. Als problematisch angesehen wurde, dass einige Behörden keine verschlüsselten Daten empfangen möchten/können.

Hinweis durch die KDSA: Auch staatliche Behörden müssen die Anforderungen, die sich aus den Datenschutzgesetzen ergeben, erfüllen. Bei Problemen kann die Datenschutz-Aufsichtsbehörde des Landes eingeschaltet werden.

Die Aufbewahrung/Speicherung der E-Mails im Rahmen der Kommunikation mit Klienten ist derzeit nicht geklärt und sollte unter Beachtung von Löschrufen sowie Doppelhaltung überprüft werden.

Verarbeitung von Personaldaten

Die Vorlage erweiterter Führungszeugnisse wird im Einstellungsverfahren verlangt (Ausnahme: Einstellung von reinen Verwaltungsmitarbeitern). Die Vorlage wird mit Datum in einer Excel-Liste notiert. Eine Kopie wird nicht angefertigt.

Bis zur Einführung der elektronischen AU wurden auch diese Bescheinigung in den Personalakten gespeichert.

Der Umgang mit personenbezogenen Daten von Bewerbern erfolgt datenschutzkonform.



Mitarbeitende nutzten auch dienstliche Kraftfahrzeuge. Dazu wird Einsicht in den Führerschein genommen, jedoch keine Kopie angefertigt.

Betroffenenrechte

Mit der Informationspflicht des Verantwortlichen geht das Recht des Betroffenen auf Auskunft über die Verarbeitung der sie betreffenden personenbezogenen Daten einher. Es wurde angegeben, dass es bisher keine Anfragen Betroffener zur Verarbeitung ihrer personenbezogenen Daten gegeben hat. Die Erstellung eines Merkblattes ist derzeit in der Bearbeitung.

Ergebnis:

Die Prüfung verlief insgesamt positiv. Es entstand der Eindruck, dass eine hohe Akzeptanz zur Umsetzung des kirchlichen Datenschutzes besteht. Die erteilten Hinweise wurden angenommen.

3.4.2 Prüfung eines Seniorenzentrum

Wie auch im letzten Berichtszeitraum haben wir im Jahr 2023 eine anlasslose Prüfung eines Seniorenzentrums vorgenommen. Geprüft haben wir auch in dieser Einrichtung die datenschutzrechtlich relevanten Abläufe im Zusammenhang mit dem Betrieb des Seniorenheimes, insbesondere die Verwaltung und Aufbewahrung der Bewohnerakten, der Pflegedokumentation und der Personalakten.

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

Weder ein Datenschutzkonzept noch ein VVT konnte vorgelegt werden. Es waren zudem keinerlei Unterlagen, wie z. B. Merkblätter zum Umgang mit Betroffenenrechten, Umgang/Meldungen von Datenpannen, Merkblatt zum Datenschutz, Verpflichtungserklärungen etc. vorhanden.

2. Auskünfte über Bewohner an Angehörige

Im Umgang mit Auskunftersuchen von Angehörigen und anderen Dritten hinsichtlich des Aufenthaltes und des Gesundheitszustandes von Bewohnern zeigten sich Unsicherheiten. Klare Anweisungen, wem und unter



welchen Bedingungen Auskünfte gegeben werden dürfen, waren nicht vorhanden.

3. Bewerbungsverfahren Bewohner

Ein Muster eines Aufnahmeantrages kann online über die Webseite der Einrichtung abgerufen werden. Danach werden unnötige Daten nicht erhoben. Der Heimvertrag wird in der „Abrechnungsakte“ aufbewahrt. Ein Blankovertragsformular konnte nicht vorgelegt werden, da die Erfassung digital erfolgt und ein Ausdruck eines Blankoformulars nicht möglich ist. Eine Prüfung konnte daher nicht erfolgen.

4. Pflegedokumentation

Die Pflegedokumentation erfolgt schriftlich in Papierform. Zudem existieren digitale Akten. Die Papierakten werden in den Wohneinheiten in den Dienstzimmern aufbewahrt. Die Rollschränke sind nicht abschließbar. Versichert wurde jedoch, dass keine unbefugten Personen Zugriff haben, da die Büros verschlossen werden, sofern sich darin kein Mitarbeiter aufhält.

Auf Nachfrage erklärte uns die Einrichtungsleiterin, dass die Bildschirme über eine Bildschirmsperre verfügen. Da die Besprechung in dem Dienstzimmer der Leiterin stattfand, konnten wir jedoch feststellen, dass dies nicht der Fall war. Die beiden vorhandenen Bildschirme waren die gesamte Zeit offen einsehbar. Auch eine Nachfrage bei einer Mitarbeiterin einer Wohneinheit der Einrichtung ergab, dass Bildschirmsperren nicht eingerichtet sind. Auch der Bildschirm dieser Mitarbeiterin konnte während des Gesprächs von uns eingesehen und so die Pflegedokumentation einer Bewohnerin zur Kenntnis genommen werden.

Angegeben wurde, dass Akten nach 10 Jahren vernichtet werden. Akten, die im aktuellen Geschäftsablauf nicht mehr benötigt werden, werden in einem Archiv gelagert. Das Archiv ist in einem Kellerraum untergebracht. Die Abwasserleitungen, die durch das Archiv verlaufen, sind neu und sollen nach der Ansicht der Leiterin sicher sein. Ein Feuerlöscher ist nicht vorhanden.

Nach Aussage der Leiterin gab es bisher kein Verlangen auf Einsichtnahme in die Pflegedokumentation. Der Ablauf des Verfahrens war jedoch nicht



bekannt. Nicht bekannt war zudem, wem unter welchen Voraussetzungen Einsicht zu gewähren ist (Bewohner/MDK/ Heimaufsicht/Angehörige/ Pflegversicherung/Hausarzt/Betreuer). Auch bezüglich der Frage nach der Möglichkeit nach dem Tod des Bewohners Einsicht in die Pflegedokumentation zuzunehmen waren keine Angaben möglich. Schriftlichen Regelungen sind nicht vorhanden.

Auf die Unterlagen hat die Heimleiterin, die Pflegeleitung und die Sekretärin Zugriff. Die Frage, warum die Sekretärin Zugriff auf die Pflegedokumentation haben muss, konnte nicht beantwortet werden.

5. Fotos

Eine Einverständniserklärung für Foto- und Filmaufnahmen wird mit dem Heimvertrag eingeholt. Ein Muster wurde uns übergeben. Dies entspricht jedoch nicht den Anforderungen an eine wirksame Einwilligungserklärung.

Die Einholung der Einwilligungserklärung für Mitarbeiter war in der Bearbeitung.

Fotos werden mit dienstlichen Kameras erstellt. Die darauf befindlichen Fotos werden zeitnah heruntergeladen und vor Ort ausgedruckt bzw. gespeichert. Die Karte wird gelöscht, da die Karte nur eine kleine Speicherkapazität hat. Die Speicherkarte und der Fotoapparat werden jedoch nicht getrennt voneinander aufbewahrt. Die Speicherkarte verbleibt im Apparat. Es besteht kein Löschkonzept für die Fotos. Der Apparat wird gesichert in einem abgeschlossenen Schrank gelagert.

6. Wunddokumentation (Fotos)

Die Wunddokumentation erfolgt durch die Wundschwester eines Sanitätshauses (externer Anbieter). Diese verfügt über eine eigene Fotoausrüstung. Der für dieses Auftragsverhältnis erforderliche Auftragsvertragsvertrag lag nicht vor.

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. Bei uns entstand der Eindruck dafür nicht sensibel zu sein. Nicht bekannt war, dass Datenpannen der Aufsicht zu melden (§ 33 KDG) sind.

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 der Leiterin nicht bekannt zu sein.

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 darauf hingewiesen, dass die Angabe der Gründe nicht erforderlich ist.
- Unklar war, ob es in der Einrichtung gestattet ist, dass Mitarbeitende während ihrer Dienste private Smartphones bei sich führen dürfen. Eine Anweisung, dass private Geräte nicht genutzt werden dürfen, d. h. keine Fotos oder Videos von Bewohnern erstellt werden dürfen, besteht nicht. Wir haben darauf hingewiesen, dass Bild- und Tonaufnahmen von den Bewohnern unzulässig sind und gerade in der jüngeren Vergangenheit in anderen Einrichtungen zu beobachten war, dass solche aber angefertigt und ins Internet gestellt wurden.

Ergebnis:

Die Prüfung verlief nicht zufriedenstellend. Aus dem Gespräch mit der Einrichtungsleiterin ergab sich der Eindruck, dass hier dringend Informations- bzw. Schulungsbedarf besteht. Es wurde festgelegt, dass folgende Unterlagen zu erstellen bzw. zu überarbeiten sind:

- Datenschutzkonzept, Verzeichnisses für Verarbeitungstätigkeiten, Hinweisblatt zum Umgang mit Betroffenenrechten, Umgang mit Datenpannen



- Überarbeitetes Muster der Foto-Einwilligung für die Bewohner (z. B. Hinweis auf die Folgen der Veröffentlichung der Fotos im Internet) und Muster der Fotoeinwilligung für die Mitarbeitenden
- Auftragsverarbeitungsvertrag Fotopflegedokumentation (Wundschwester)

Das Protokoll der Prüfung wurde der Einrichtungsleiterin und der Leitung der Trägergesellschaft übersandt. Letztere wurde aufgefordert, die erforderlichen Schritte zur Einhaltung des Datenschutzes einzuleiten, die fehlenden Dokumente zu erstellen und der Einrichtung zur Verfügung zu stellen. Wir werden im 1. Quartal dieses Jahres die Umsetzung prüfen.

3.4.3 Datenschutzüberprüfungen in Kindertageseinrichtungen – Ergebnisse, Entwicklungen und Hinweise

Im letzten Tätigkeitsbericht haben wir umfassend über eine Prüfkation berichtet, in der unsere Dienststelle die Benennung von betrieblichen Datenschutzbeauftragten in Kindertagesstätten und im Weiteren die gängigen Formulare zur Aufnahme sowie die Fotoeinwilligungserklärung überprüft hat. Da einige wenige Einrichtungen auf unsere Schreiben nicht reagierten, haben wir 2 dieser Einrichtungen vor Ort geprüft. Zu diesen Überprüfungen kamen im Bereich der Kindertageseinrichtungen weitere vor Ort Kontrollen aufgrund allgemeiner jährlicher Prüfkationen und in Folge von Datenschutzverletzungen dazu.

Standardmäßig prüfen wir in Kindertageseinrichtungen allgemeine Dinge zum Datenschutzmanagement, die Angaben von Daten beim Anmeldeprozess, die Fotoeinwilligungserklärungen sowie die IT Sicherheit. Je nach Anlass des Besuches oder Vorkommnissen können noch weitere Überprüfungsgebiete hinzukommen.

Ergebnisse der Überprüfungen, Entwicklungen und Hinweise

Anmelde- und Aufnahmeformulare

Soweit noch analoge Aufnahmeformulare in den Einrichtungen verwendet werden, gaben diese kaum Anlass für Beanstandungen. Nur in einer Einrichtung wurde der Umfang der Erwerbstätigkeit der Sorgeberechtigten sowie die Krankenversicherung des Kindes abgefragt. Im Tätigkeitsbericht



2022 unter Punkt 3.2.4 ist nachzulesen, warum wir in diesen Angaben keine Erforderlichkeit sehen.

Zu beobachten ist, dass Online-Anmeldungen über die Kommunen zunehmen. Bei diesen Systemen geben die Eltern bzw. Sorgeberechtigten nur einmal ihre persönlichen Daten ein und können dann unter den verfügbaren Einrichtungen auswählen. Bei einer positiven Platzvergabe werden automatisch weitere Anmeldungen bei verfügbaren Einrichtungen derselben Kommune storniert. Die Eltern müssen nicht auf unzähligen Anmeldeformularen ihre Daten hinterlassen und bei einer Platzzusage die anderen Anmeldungen wieder absagen.

Die elektronischen Anmeldedaten werden im Anschluss von der Kita-Verwaltungssoftware automatisch übernommen und ggf. ergänzt. Problematisch ist in diesem Zusammenhang noch die Datenlöschung zum Ende der Betreuungszeit. So müssen bestimmte personenbezogene Daten zum Erfüllen der gesetzlichen Aufbewahrungsfristen zwar weiter vorhanden sein, dürfen aber nicht mehr im Rahmen der Aufgabenerfüllung verarbeitet werden, da das Vertragsverhältnis beendet ist. Eine Datenspernung bzw. Einschränkung der Verarbeitung würde sich in diesem Fall anbieten, ist aber noch nicht bei allen Anwendungen implementiert.

Entwicklungsdokumentation

Eine überprüfte Einrichtung sah es nicht als erforderlich an, dass Fotos für die Entwicklungsdokumentation von den Sorgeberechtigten durch eine Fotoeinwilligungserklärung zu legitimieren sind. Die Einrichtung wollte darauf abstellen, dass der Betreuungsvertrag die rechtliche Grundlage für das Erstellen von Fotos ist. Unsere Dienststelle sieht jedoch für die Aufgabenerfüllung der Kindertageseinrichtungen das Erstellen von Fotos für nicht erforderlich an. Die Hauptaufgaben der Einrichtungen sind das Betreuen, die Förderung und der Schutz der Kinder.

Kindertageseinrichtungen können aber aufgrund ihrer sozialgesetzlichen Aufgaben, die sich aus § 26 SGB VIII in Verbindung mit landesrechtlichen Ausführungsgesetzen ergeben, verpflichtet sein Entwicklungsdokumentationen oder Sprachstandserhebungen (Sprachlerntagebücher) durchzuführen bzw. anzulegen. Und diese Dokumentationen können dann wiederum Fotos enthalten, um den Entwicklungsschritt zu untermalen. Diese Verarbeitung personenbezogener Daten muss dann aber durch eine Einwilli-



gungserklärung gem. § 6 Abs. 1 lit. b) KDG unter Beachtung der Wirksamkeitsvoraussetzungen nach § 4 Nr. 13 und § 8 KDG erlaubt worden sein, und nicht wie fälschlicherweise angenommen durch die Erfüllungspflichten, die sich aus dem Kinderbetreuungsvertrag ergeben.

Es ist auch nicht möglich, die Einwilligungserlaubnis über den Abschluss des Betreuungsvertrages einzuholen. Eine Wirksamkeitsvoraussetzung für eine gültige Einwilligung ist die Freiwilligkeit (§ 8, Abs. 8 KDG, Art. 7 Abs. 4 DS-GVO). Demnach darf die Erteilung einer Einwilligungserklärung nicht mit dem Betreuungsvertrag gekoppelt sein.

Ausdruck von Fotos

Fotos werden in den von uns überprüften Einrichtungen mit betrieblichen Endgeräten erstellt. Dabei ist zu beobachten, dass der Einsatz von Tablets zunimmt. Begründet wird dies damit, dass diese multifunktional einsetzbar sind. So lassen sich Anwesenheitslisten digital führen, Texte fürs Portfolio erstellen, Fotos anfertigen und an einen Fotoentwickler senden. Aber auch als Notfall-Telefon für Gruppenausflüge können Tablets genutzt werden. Wichtig ist, dass die verwendeten Geräte eine Zugriffsbeschränkung (Pin etc.) haben und es nur möglich ist, dienstlich autorisierte Anwendungen (Apps) zu nutzen bzw. zu installieren.

Der Ausdruck der erstellten Fotos erfolgt in den Einrichtungen durch

- Direktdruck in der Einrichtung
- Online-Übermittlung an einen Fotodienstleister
- Übertragen auf einen USB-Sticks bzw. Entnahme der Speicherkarte und anschließendem Ausdruck an einem öffentlichen Fotodrucker

Aus datenschutzrechtlicher Sicht ist der Direktdruck in der Einrichtung der sicherste Weg, da die Fotos die Einrichtung nicht verlassen und nicht auf weitere Datenträger übertragen werden.

Den Einrichtungen, die ihre Bilddateien an einen Fotodienstleister online übermitteln, haben wir folgenden Hinweis erteilt: Werden Fotos online übermittelt, muss sichergestellt sein, dass die Fotos nur auf Servern im EU-Wirtschaftsraum gespeichert und diese im Anschluss auch wieder gelöscht werden. Die Verbindung während der Übertragung der Bilddateien sollte selbstverständlich verschlüsselt sein.



Die Übertragung der Fotos auf einen unverschlüsselten USB-Stick oder die Entnahme der in der Regel unverschlüsselten Speicherkarte zum Entwickeln birgt Risiken, da ein Zugriff Dritter im Falle eines Verlusts möglich ist (vgl. Punkt 5.2.3 in diesem Tätigkeitsbericht).

Meldung Datenschutzvorfall

In den meisten Einrichtungen kannte zwar die Leitung den Ablauf, was im Fall einer Datenpanne oder möglichen Datenschutzverletzung zu unternehmen ist, dagegen war dies nicht immer allen Mitarbeitenden bekannt. Daher haben wir die Einrichtungen darauf hingewiesen, dass der Prozess, wie bei einer Datenpanne gehandelt werden soll, wer zu informieren ist und an wen im Fall einer Datenschutzverletzung eine Meldung zu erfolgen hat, allen Beschäftigten bekannt sein muss. Datenschutzverletzungen müssen ab Bekanntwerden unverzüglich, spätestens jedoch innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden.

Bereits im Tätigkeitsbericht 2021 haben wir unter Pkt. 4.1.3 ausführlich über verspätete Meldungen und die Rechtzeitigkeit von Meldungen berichtet.

Betroffenenrechte

Auskunftsersuchen bzw. Betroffenenanfragen hatten die überprüften Einrichtungen bisher noch nicht erreicht. Die Verantwortlichen wurden dahingehend sensibilisiert, dass auch für diese Betroffenenrechte ein Prozess etabliert oder bekannt sein sollte. Das Gesetz fordert, dass der Verantwortliche für derartige Auskünfte in jedem Fall eine Antwort erteilen muss und zwar unverzüglich, also ohne schuldhaftes Zögern, spätestens aber innerhalb eines Monats nach Eingang des Antrags auf Auskunftserteilung (§ 14 Abs. 3 S. 1 KDG, vgl. TB 2020, Pkt. 3.5).

Masernimpfung / Meldungen an das Gesundheitsamt

In einigen besuchten Einrichtungen herrschte noch Unsicherheit darüber, wie die Nachweise der seit dem 31.07.2022 verpflichtenden Masern-Impfung datenschutzkonform erbracht und aufbewahrt werden können. Bekannt war den Einrichtungen, dass Impfausweise nicht kopiert werden dürfen.



Zur datenschutzkonformen Erbringung der Nachweise haben wir uns umfassend in unserem letzten Tätigkeitsbericht (TB 2022, Pkt. 5.1) geäußert.

Kurz und knapp: Es genügt die Einsichtnahme und die Dokumentation!
Keine Kopie.

D.h. die Einrichtungen dürfen sich beispielsweise in der Kinderakte einen Vermerk machen, dass die Masernimmunität vorhanden ist. Auch ein separates Formular ist möglich.

Im Falle eines nicht erbrachten Nachweises sowie auch bei bestimmten Krankheiten (siehe IfSG) muss eine Meldung an das Gesundheitsamt erfolgen.

3.4.4 Webseiten-Check

In unserem Tätigkeitsbericht 2022 Punkt 7.4 hatten wir auf weitere Überprüfungen von Websites hingewiesen. Auch in diesem Berichtsjahr haben wir Websites proaktiv (anlasslos) überprüft. Schwerpunkte waren bekanntgewordene Abmahnungen bei externer Einbindung von Schriftarten (Fonts) ohne vorherige Einwilligung bzw. ohne Vorliegen eines Rechtfertigungsgrundes. Ein weiterer Aspekt waren rechtliche Anforderungen auf Grundlage des Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), speziell zum Thema der Speicherung von Informationen in der Endeinrichtung des Endnutzers (Cookies).

Bereits seit dem 1. Dezember 2021 ist das Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) in Kraft. Websites und Apps fallen unter den Begriff der Telemedien.

Vorgebeugt statt abgemahnt

Während der ersten Überprüfungen stellten wir einen erhöhten Beratungsbedarf zur rechtlichen und technischen Situation sowie den Verantwortlichkeiten einer Website fest, was wir zum Anlass nahmen, zielgerichteten Veranstaltungen zum Thema „Websites mit Fonts & Co im Selbsttest“ anzubieten.

Das Erstellen einer Website wird in der Regel an einen Fachmann übertragen. Dabei geht der spätere Betreiber/Verantwortliche davon aus, dass u.a.



alles ordnungsgemäß und weitestgehend rechtssicher übergeben und online geschaltet wird.

Ziel der Veranstaltung war ein Wissenstransfer, dass danach u.a. auch „Nicht-Techniker“ selbst in der Lage sind, mit bereits vorhandenen Standardmitteln wie dem Webbrowser, eine Website zu überprüfen. Es wurde zudem auch dahingehend sensibilisiert, dass der Betreiber einer Website der Verantwortliche bleibt – und nicht derjenige, der die Website mit vielen Raffinessen erstellt hat. Denn nicht immer ist das technisch Mögliche auch erforderlich.

Die Resonanz war groß, so dass wir die Veranstaltungsreihe über das Jahr verteilt an mehreren Terminen durchgeführt haben.

Häufige Auffälligkeiten:

- Schriftarten aus externen Quellen, nicht nur von Google oder Adobe
- Vorwiegend bei aktuellem Content - extern eingebetteter Inhalt, u.a. auch YouTube
- Ältere Webseiten mit alten externen Inhalten noch online
- Cookies werden sofort beim Aufruf der Webseite gesetzt
- Quercheck zur Datenschutzinformation war häufig nicht konform zur Website

Fazit:

Der Großteil der Websites war rechtlich bedenklich, Abmahnungen wären nicht unbegründet. An Hand eines Musters einer Beweissicherung wurde erläutert, wohin man beim Überprüfen der eigenen Website genauer schauen sollte.

First-Party Hosts

1. Testdomain XYY

Anfragen wurden an 1 First-Party hosts uebermittelt.

Drittanbieter-Hosts

1. f1-eu.readspeaker.com
2. docs.google.com
3. www.gstatic.com
4. apis.google.com
5. ssl.gstatic.com
6. content.googleapis.com
7. https

Anfragen wurden an 7 Drittanbieter-Hosts uebermittelt.



Die unerlaubte Weitergabe der Metadaten durch den Website-Betreiber stellt eine Verletzung des allgemeinen Persönlichkeitsrechts in Form des Informationellen Selbstbestimmungsrechts nach § 823 Absatz 1 BGB dar. Das Recht auf informationelle Selbstbestimmung beinhaltet das Recht des Einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Durch das vorgelagerte Laden, z.B. einer Schriftart aus externen Quellen, wäre eine freie Entscheidung mit Wahlmöglichkeit zur Datenübermittlung nicht gegeben.

3.5 Datenschutzvorfälle

3.5.1 Offener E-Mail Verteiler – Datenpanne mit Wiederholungsgarantie

Wir haben bereits mehrfach darüber berichtet, andere Aufsichtsbehörden ebenso, es gab schon Bußgelder und es fehlt auf keiner Datenschutzunterweisung – der offene E-Mail-Verteiler.

Offene E-Mail-Verteiler, die ohne Erforderlichkeit, Einwilligungserklärung oder einen anderen legitimierenden Grund verwendet werden, sind Datenschutzverstöße!

Trotz dieser Eindeutigkeit passiert es jedoch immer wieder, mal im kleinen und mal im großen Stil. Dabei macht es keinen Unterschied, ob "nur" wenige E-Mail-Adressen oder viele E-Mail-Adressen offengelegt worden sind. (Private) E-Mail-Adressen sind personenbezogene Daten i. S. v. § 4 Nr. 1 KDG. Dies trifft auch dann zu, wenn die Adresse nicht aus Vor- und Nachnamen besteht. Es genügt, wenn sie einer Person zugeordnet werden kann. Die datenschutzrechtliche Bewertung, dass es sich dabei regelmäßig um einen Datenschutzverstoß handelt, ist gleichbleibend.

Es folgt ein Best-Off ausgewählter Datenpannen aufgrund eines offenen E-Mail-Verteilers, die durch unsere Behörde im Berichtszeitraum beanstandet worden sind:

1) Infomail an Mitglieder

Innerhalb eines größeren Verbandes wurde an haupt- und ehrenamtliche Mitglieder eine E-Mail mit einer Terminankündigung zu einem Online-Dialog versendet. Die Haupt- und Ehrenamtlichen sind aktive, zum Teil aber auch ehemalige, Mitglieder dieses Verbandes. Auch werden private E-Mail-



Adressen für die Verbandsarbeit von den Mitgliedern genutzt. Die Info-mail an die aktiven und ehemaligen Mitglieder wurde mit einem offenen E-Mail-Verteiler versendet und stellt eine Verarbeitung (Offenlegung) i. S. v. § 4 Nr. 3 KDG dar. Eine Bedingung gem. § 6 Abs. 1 KDG, die das Versenden im offenen Verteiler legitimieren konnte, lag nicht vor.

Somit war der Versand dieser E-Mail mit offenem Verteiler eine unbefugte Offenlegung.

Dabei hatte die Verantwortliche mit einer Verfahrensbeschreibung Maßnahmen getroffen, um E-Mail-Adressen der aktiven und ehemaligen Mitglieder gegen unberechtigtes Verarbeiten zu schützen. Gemäß dieser Verfahrensbeschreibung dürfen personenbezogene Daten nur verarbeitet werden, wenn eine der Bedingungen gem. § 6 Abs. 1 KDG erfüllt ist. Im Weiteren wurde in der Verfahrensbeschreibung aufgeführt, dass bei E-Mails, die an mehr als eine Person versendet werden, immer die BCC-Funktion zu nutzen ist. Für offene E-Mail-Verteiler musste eine Freigabe eingeholt werden.

Der Mitarbeiter hat entgegen dieser Verfahrensbeschreibung personenbezogene Daten offengelegt, da die BCC-Funktion nicht genutzt worden ist. Da das Fehlverhalten jedoch dem Aufgaben- und Tätigkeitsbereich des Mitarbeitenden zuzuordnen ist, handelte es sich nicht um einen Mitarbeiterexzess, so dass gegenüber der Verantwortlichen eine Beanstandung ausgesprochen worden ist.

Die Verantwortliche hat im Nachgang den Datenschutzverstoß umfassend aufgearbeitet und das Verfahren „Versenden von E-Mails an einen großen Verteilerkreis“ optimiert, um derartige Vorfälle in Zukunft zu vermeiden. So sollen Infomails nur noch aus dem Datenbanksystem heraus versendet werden, weil dadurch alle E-Mail-Adressen automatisch in das BCC-Feld gesetzt werden.

2) Weiterleitung eines Informationsschreibens

Ein Vertreter eines Gremiums hat ein Informationsschreiben an die Mitglieder dieses Gremiums weitergeleitet. Die Mitglieder dieses Gremium, welches sich zu dieser Zeit noch konstituierte, waren sich nur namentlich bekannt. Weitere personenbezogene Daten u.a. auch die persönlichen und



privaten E-Mail-Adressen waren zu diesem Zeitpunkt noch nicht allen Mitgliedern bekannt. Die Weiterleitung des Informationsschreibens erfolgte nicht über die „BCC“-Funktion, sondern über einen offenen E-Mail-Verteiler („AN“-Feld), worüber sich ein Mitglied bei uns beschwerte.

Das Mitglied führte in seiner Beschwerde an uns aus, dass für die Weitergabe der privaten E-Mail-Adresse an alle Mitglieder des Gremiums trotz namentlicher Bekanntheit keine Einwilligung vorlag. Im Folgenden haben wir den Vertreter sowie auch die Verantwortliche zu diesem Vorfall angehört und eine Beanstandung gegenüber der Verantwortlichen ausgesprochen, die wir wie folgt begründet sahen:

Zum einen hat für die Verarbeitung (Offenlegung) i. S. v. § 4 Nr. 3 KDG keine Rechtmäßigkeit nach § 6 Abs. 1 KDG vorgelegen. Eine für diese Verarbeitung in Betracht kommende Einwilligungserklärung konnte uns nicht vorgelegt werden. Im Weiteren gab es für die Mitglieder des Gremiums keine Datenschutzinformation gem. §§ 15, 16 KDG, so dass diese zu Beginn der Datenerhebung in der Lage gewesen wären, bestimmen und einschätzen zu können, wer, was, wann über sie verarbeitet (offenlegt). Schlussendlich war es für die Erreichung des Zwecks, eine Informationsweiterleitung an die Mitglieder, nicht erforderlich einen offenen E-Mail-Verteiler zu verwenden.

Wie E-Mails korrekt zu versenden sind und was alles Beachtung finden muss, kann unter Punkt 7.3 in diesem Bericht nachgelesen werden.

3.5.2 Keine Auskunft unter dieser Nummer I

In § 17 KDG wird das Auskunftsrecht betroffener Personen geregelt. Nach Abs. 1 dieser Vorschrift hat eine betroffene Person das Recht, Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden.

Diese Regelung ist eine Kernvorschrift des KDG. Die betroffene Person soll erfahren, ob personenbezogene Daten über sie verarbeitet werden und ggf. um welche Daten es sich dabei handelt. Diese Kenntnis der Verarbeitung bildet die Basis dafür, dass die betroffene Person die Rechtmäßigkeit



der Verarbeitung überprüfen kann (Ehmann, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 15 Rn. 1). Damit stellt der Auskunftsanspruch ein zentrales Instrument zur Durchsetzung des Rechts auf informationelle Selbstbestimmung dar.

In § 17 KDG ist nicht geregelt, in welchem Zeitraum der Auskunftsanspruch zu erfolgen hat. Jedoch ist für die Vorschriften der §§ 17 bis 24 KDG in § 14 Abs. 3 KDG eine Antwortfrist quasi vor die Klammer gezogen. Danach muss der Verantwortliche unverzüglich, in jedem Fall aber innerhalb eines Monats, nach Eingang des Antrages die Auskunft zur Verfügung stellen. Der Begriff unverzüglich ist im Bürgerlichen Gesetzbuch § 121 Abs. 1 S. 1 BGB legal definiert und meint „ohne schuldhaftes Zögern“. Aufgrund dieser Vorschrift kann eine Auskunft, die einen Monat nach Eingang des Antrages erfolgt, bereits verspätet sein, wenn dem Verantwortlichen ein schuldhaftes Zögern nachgewiesen werden kann. Das „Ausreizen“ der Frist darf deshalb nicht die Regel sein, sondern ist komplizierteren Fällen vorbehalten.

Fristbeginn ist der Antragseingang. Dieser hat stattgefunden, sobald die Anfrage des Betroffenen derart in den Machtbereich des Verantwortlichen gelangt ist, dass dieser hiervon Kenntnis nehmen konnte. Eine tatsächliche Kenntnisnahme der Anfrage ist nicht erforderlich.

In einem Fall hat ein ausländischer Staatsbürger ein Auskunftsersuchen an die Verwaltung eines Bistums gerichtet. Dieses wurde per Mail an die offizielle Mail-Adresse unter info@bistum.de gesandt. Die E-Mail war in mehreren Sprachen (französisch, deutsch, englisch) verfasst und an mehrere Empfänger versandt. Im Anhang enthielt sie eine png-Datei, in der ein Ausweisdokument zum Identitätsnachweis des Antragstellers gespeichert war. Aus diesen Gründen wurde die Mail vom Postsystem als Spam qualifiziert und in den entsprechenden Ordner verschoben. Dort eingegangene Spams werden nach ca. drei Monaten gelöscht, ohne dass eine persönliche Kontrolle seitens des Verantwortlichen durchgeführt wird.

Der Verantwortliche ist dem Auskunftsersuchen wohl wegen dieser Tatsachen nicht nachgekommen.

Auf dem Mailserver zugegangen ist eine E-Mail aber auch dann, wenn sie händisch oder automatisch in den Spam-Ordner verschoben worden ist.



Es ist Aufgabe des Verantwortlichen sicherzustellen, dass E-Mails, die ihm zugehen, auch bearbeitet werden. Umgedreht hat der Verantwortliche die Konsequenzen dafür zu tragen, dass er eingehende E-Mails ungelesen aussortiert oder aus anderen Gründen nicht zur Kenntnis nimmt.

Der Antragsteller konnte durch Vorlage einer Kopie der E-Mail-Anfrage, aus der das Sendedatum hervorgeht, glaubhaft machen, dass die E-Mail mit dem entsprechenden Inhalt an den Verantwortlichen gesendet worden ist. Der Verantwortliche hat eingeräumt, dass die entsprechende E-Mail bei ihm eingegangen sein kann und konnte deshalb den Zugang nicht substantiiert bestreiten.

Nachdem der Auskunftsanspruch mehr als sechs Monate unbeantwortet blieb, wendete sich der Betroffene an unsere Aufsicht.

Die Anforderungen an ein rechtmäßig gestelltes Auskunftsverlangen sind gering. So ist der Auskunftsanspruch regelmäßig nicht an eine bestimmte Form gebunden. Es ist nicht erforderlich, dass der Betroffene eine postalische Adresse für eine Rückmeldung angibt oder begründet, warum er eine entsprechende Auskunft verlangt. Ebenso wenig ist erforderlich, dass aus der Anfrage die Beziehung zum Verantwortlichen hervorgeht oder dass der Betroffene im Falle der Nichtbeantwortung noch einmal „nachhakt“. Soweit der Verantwortliche aber genau diese Punkte dafür ins Feld führte, um zu rechtfertigen, dass die Anfrage in den Spam-Ordner gelangt ist, konnte ihn das nicht exkulpieren. Der Verantwortliche muss sicherstellen, dass Betroffenenanfragen intern den richtigen Weg finden, um von den zuständigen Mitarbeitenden bearbeitet zu werden.

Es war in diesem Fall eine förmliche Beanstandung auszusprechen.

3.5.3 Keine Auskunft unter dieser Nummer II

In einem weiteren Fall bei demselben Verantwortlichen richtete sich ein Betroffener in der 20. Kalenderwoche (KW) 2022 mit einem Auskunftsersuchen nach § 17 KDG an den Generalvikar. Nachdem über ein Monat ohne Antwort vergangen war, wandte sich der Betroffene in der 25. KW erneut an den Generalvikar mit der Bitte um Beantwortung seines Auskunftsers-



suchens. Dieser lässt durch eine Mitarbeiterin nach zwei Wochen (27. KW) antworten, dass die Anfrage in Bearbeitung sei. Eine Auskunft werde spätestens in weiteren drei Wochen (30. KW) erteilt werden. Auch in der 30. KW passiert ... NICHTS!

Das bleibt auch weitere dreieinhalb Monate so, woraufhin der Betroffene in der inzwischen 43. KW erneut anfragt, wann er denn mit einer Antwort rechnen könne. Diese erneute Anfrage blieb einmal mehr unbeantwortet. Worauf der Betroffene in der 47. KW seine Frage nach dem Sachstand wiederholt und dabei auch auf die zwischenzeitliche Verfahrensdauer hinweist. Diesmal erhält der Betroffene sofort, nämlich noch am selben Tag eine Nachricht, in der ihm mitgeteilt wird, dass die Angelegenheit nunmehr dem betrieblichen Datenschutzbeauftragten übergeben worden sei. Welchen Informationswert diese Auskunft für den Betroffenen haben soll ist unklar, kann ihm doch egal sein wer sein Anliegen bearbeitet, wenn es doch nur irgendwer endlich einmal täte. Völlig überraschend meldete sich ohne zwischenzeitliche Erinnerung durch den Betroffenen in der 48. KW eine Mitarbeiterin des Verantwortlichen, um ihm die adventliche Botschaft zu übermitteln mit der Ankunft seiner Auskunft sei „in Kürze“ zu rechnen. Aber es geschah nur, was schon seit der 20. KW (s.o.) geschah, nämlich ... NICHTS!

Der Winter verging und das Frühlingsgras wuchs inzwischen über die Angelegenheit, als der Betroffene am Anfang des Sommers die Penetranz besaß, sich in der 26. KW (wohlgemerkt des Folgejahres 2023) erneut an den Generalvikar zu wenden. Der Betroffene fragte, langsam im Ton leichter Gereiztheit, an, ob er denn überhaupt noch mit einer Antwort rechnen könne. Bei einer solchen Impertinenz tat der Verantwortliche was er auch bislang schon tat ... NICHTS!

Daraufhin wandte sich der Betroffene offensichtlich vollends von Ungeduld getrieben, schon vor Ablauf eines weiteren Monats in der 27. KW, mit seinem Anliegen an den Ortsordinarius. Dieser ließ am selben Tag (!) durch einen Mitarbeiter mitteilen S. Exz. (Originalton) werde sich der Sache annehmen. Ob das geschehen ist, entzieht sich unserer Kenntnis, im Ergebnis passierte jedoch -wenig überraschend- ... NICHTS!



In der 34. KW wandte sich der Betroffene an unsere Behörde. Wir forderten den Verantwortlichen einen Tag später unter Hinweis auf den bisherigen Zeitablauf auf, zu dem Sachverhalt Stellung zu nehmen, was auch fristgemäß in der 37. KW geschah. Der Beanstandungsbescheid unserer Behörde erging in der 38. KW. Danach fand eine Einigung der Parteien statt.

Es handelte sich hier bei dem Verantwortlichen um eine kirchliche Stelle im Sinne von § 3 Abs. 1 KDG, die öffentlich-rechtlich verfasst ist. Gem. § 51 Abs. 6 KDG war deshalb die Verhängung eines Bußgeldes ausgeschlossen. Ein vergleichbar renitentes Verhalten eines nicht öffentlich-rechtlich verfassten Verantwortlichen hätte mit Sicherheit eine nicht unerhebliche Geldbuße nach sich gezogen.

Erschreckend in diesem Fall ist, dass die Bistumsleitung sich dem begründeten datenschutzrechtlichen Anspruch des Betroffenen verweigert hat. Wenn der Ortsordinarius als Gesetzgeber sich nicht an seine eigenen Gesetze hält, stellt sich schnell die Frage, ob dieses Gesetz mit der DS-GVO in Einklang steht, wie es Artikel 91 Abs. 2 DS-GVO verlangt.

3.5.4 Kostenzuschüsse für dienstliche Erreichbarkeit über private Geräte

Eine Ordnung zum Ersatz von Telefonkosten bei dienstlicher Nutzung privater Endgeräte hat für Irritationen bei den Beschäftigten gesorgt. Grund dafür war, dass man in einer Verwaltungseinheit eine einheitliche Regelung für alle Mitarbeitende einführen und damit jahrelang geduldete Individualvereinbarungen ablösen wollte. Die Kostenzuschüsse für die Nutzung privater Mobiltelefone waren wohl teilweise sehr hoch, was dadurch bedingt war, dass Mobilfunktarife vor einigen Jahren noch wesentlich preisintensiver waren als gegenwärtig.

Beim Blick in die Ordnung war jedoch klar, dass der zukünftig weitaus geringere Kostenzuschuss als der individuell vereinbarte an die Preisgabe und Veröffentlichung der Mobilfunknummer geknüpft sein sollte. Die Regelungen aus KDG und KDG-DVO waren in dieser Ordnung nur rudimentär enthalten.



So sollte der Zuschuss zu den Telefonkosten nur gewährt werden, wenn die private Telefonnummer des Mitarbeitenden in einer zentralen Datenbank sowie im Telefonverzeichnis der Verwaltungseinheit veröffentlicht wird. Dabei wäre eine Veröffentlichung der Mobilfunknummer nicht erforderlich, da der Mitarbeitende die dienstlichen Anrufe über eine Anrufweiterleitung auf seinem privaten Gerät empfangen konnte. Damit ist die private Rufnummer letztendlich unerheblich.

Für den Fall, dass die private Rufnummer veröffentlicht werden darf, sollte – so der Hinweis von uns – eine Auswahlmöglichkeit geschaffen werden. In diesem Zusammenhang haben wir auch darauf hingewiesen, dass es eine Widerrufsmöglichkeit geben muss.

Im Weiteren sollten Mitarbeitende den Dienstgeber sofort über den Verlust des privaten Mobiltelefons informieren, obwohl die Pflicht bestand, keine dienstlichen Daten auf dem Gerät zu speichern. Wenn keine dienstlichen Daten auf einem privaten Mobiltelefon oder einem anderen privaten technischen Endgerät vorhanden sind und diese in Folge eines Verlustes verloren gehen, so sind folgemäßig keine dienstlichen personenbezogenen Daten abhandengekommen. Deshalb kann in diesem Fall ein Datenschutzvorfall oder eine Datenschutzverletzung nach dem KDG ausgeschlossen werden. Eine Meldung an den Dienstgeber über den Verlust ist somit nicht erforderlich. Nur wenn der Mitarbeitende einer Veröffentlichung seiner privaten Rufnummer zugestimmt hatte und diese sich aufgrund des Verlustes ändert, sollte ein Hinweis an den Dienstgeber erfolgen.

Fazit: Um personenbezogene Daten und damit auch private Rufnummern von Mitarbeitenden zu verarbeiten bedarf es grundsätzlich einer Rechtmäßigkeit nach § 6 Abs. (1) KDG. Das Veröffentlichen in einem Telefonverzeichnis oder einer Datenbank ist im Sinne von § 4 Nr. 3 KDG eine Verarbeitung. Ein zu gewährender Kostenzuschuss ist jedoch keine Rechtsgrundlage für die Veröffentlichung der privaten Telefonnummer des Mitarbeitenden.

4 Datenschutzvorfälle im Gesundheitswesen

4.1 Dauerbrenner: Falsche versandte Patientenunterlagen

Auch in diesem Berichtszeitraum wurde uns mehrfach gemeldet, dass Entlassberichte, 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.



Unsere Prüfungen haben ergeben, dass in den meisten Fällen in den Einrichtungen entsprechende Datenschutzunterlagen vorhanden und die Verantwortlichen ihren Verpflichtungen gem. § 26 KDG nachgekommen waren. Die Verstöße wurden 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.

4.2 Beschwerden wegen fehlender oder verspäteter Erfüllung von Auskunftersuchen

In diesem Berichtszeitraum kam es vermehrt zu Beschwerden von Patienten, die angegeben hatten ihre Auskunftersuchen seien nicht oder erst verspätet erfüllt worden. Nicht alle Beschwerden waren berechtigt. Es wurden jedoch auch Beanstandungen ausgesprochen.



Damit der Einzelne nachvollziehen kann, ob und welche personenbezogenen Daten über ihn verarbeitet werden, sieht das Unionsrecht umfangreiche Informationsrechte vor. Gem. Art. 15 Abs. 1 DS-GVO kann Auskunft über die verarbeiteten personenbezogenen Daten und nach Art. 15 Abs. 3 DS-GVO zudem noch eine Kopie hiervon verlangt werden (Art. 15 DS-GVO entspricht § 17 KDGD). Darüber hinaus ist das Recht auf Auskunft auch durch Art. 8 Abs. 2, S. 2 Grundrechtecharta (GRC) und in Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) im europäischen Primärrecht abgesichert.

Kurzum: Das Auskunftsrecht ist ein zentraler Bestandteil im Datenschutz. Von daher bedarf es auch keiner Begründung zur Ausübung dieses Rechts, wie der Europäische Gerichtshof (EuGH)³¹ erst jüngst erneut betonte. Der Anspruch ist zudem unverzüglich, spätestens aber binnen Monatsfrist zu erfüllen. Nur ausnahmsweise darf aufgrund besonderer und dem Anspruchsteller binnen Monatsfrist mitgeteilter Umstände eine Beantwortung binnen drei Monaten erfolgen (Art. 12 Abs. 3 DS-GVO/ § 14 Abs. 3 KDGD).

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

4.3 Plastischer Chirurg nutzt Fotos von Patientin für Schulungszwecke

Unsere Dienststelle erreichte die Beschwerde einer Patientin einer Klinik, die in ihrer Einrichtung eine Fachabteilung für Plastische, Ästhetische und Rekonstruktive Mikrochirurgie betreibt. Darüber hinaus bietet die Klinik das gesamte Spektrum der ästhetischen Chirurgie, insbesondere komplexe Straffungsoperationen nach Gewichtsreduktion.

Eine Patientin hatte sich in einer Sprechstunde dieser Fachabteilung im Hinblick auf eine solche Behandlung beraten lassen. Im Rahmen der Beratung wurde ein Behandlungsplan erstellt, den die Patientin bei der

³¹ EuGH, Urteil vom 26.10.2023 -Az.: C-307/22



Krankenkasse einreichen sollte. In diesem Zusammenhang wurden von der Patientin Fotos angefertigt, die den gesamten Körper der Patientin, welche nur mit Slip und BH bekleidet war, abbildeten.

Zwischen den Parteien war unstreitig vereinbart, dass die Fotos ausschließlich für die Vorlage bei der Krankenkasse zur Dokumentation des Kostenübernahmeersuchens Verwendung finden sollten. Ein leitender Mitarbeiter der Fachabteilung verwendete die erstellten Fotos, auf denen die Patientin in der beschriebenen Weise abgebildet war, im Rahmen eines Vortrages bei einem Treffen einer Selbsthilfegruppe Adipositas. Bei diesem Treffen war die Patientin dann selbst anwesend.

Die Verantwortliche hat ausgeführt, das Gesicht der Patientin sei unkenntlich gewesen. Die Patientin hatte dem nicht widersprochen. Das Nutzen der Fotos im Rahmen des Vortrages stellt einen Datenschutzverstoß dar, der von unserer Behörde beanstandet wurde.

Fotos stellen personenbezogene Daten i.S. d. § 4 Nr. 1 KDG dar. Ein Arzt, der selbst Aufnahmen vom Körper eines Patienten macht, wird zwar rechtlich zum Urheber dieser Bilder und erwirbt damit umfassende Rechte daran. Dies hat aber nicht zur Folge, dass diese beliebig verwendet werden dürfen. Die Rechte des Urhebers werden durch die Rechte des Patienten am eigenen Bild eingeschränkt. Das Recht am eigenen Bild geht zurück auf das allgemeine Persönlichkeitsrecht gem. Art. 2 Abs. 1 GG i. V. m. § 22 Kunsturhebergesetz (KUG). § 22 KUG sieht vor, dass Bildnisse nur mit Einwilligung der Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. Die Patientin hätte mithin eine Einwilligung zur Nutzung ihrer Bilder zu Vortragszwecken erteilen müssen, was nicht erfolgt war. Die Rechtsprechung sieht ein schutzwürdiges Interesse des Abgebildeten immer dann als gegeben an, wenn er in einer für Dritte erkennbaren Weise wiedergegeben wird. Das ist der Fall, wenn Fotos vom äußeren Erscheinungsbild des Patienten gemacht werden. Selbst wenn Teile des Gesichts unkenntlich gemacht werden, ist bei solchen Bildern stets die schriftliche Einwilligung des Patienten einzuholen. Nach einer Entscheidung des OLG Düsseldorf genügt es, dass die Erkennbarkeit für einen mehr oder wenigen Bekanntenkreis besteht.³² Für das OLG Zweibrücken ist es ausreichend,

³² OLG Düsseldorf, Urteil vom 09.02.2010 - I 20 U 151/19



dass sich die Erkennbarkeit aus sonstigen Merkmalen ergibt.³³ Da im vorliegenden Fall zwar das Gesicht der Patientin unkenntlich gemacht worden ist, eine Identifizierung jedoch anhand der Frisur, ihres körperlichen Erscheinungsbildes und des Umstandes, dass die Petentin selbst Teilnehmerin der Vortrages bei der Selbsthilfegruppe war, liegt ein personenbezogenes Datum vor.

Da der Zweck für die Anfertigung und weiteren Verwendung der Fotos (Dokumentation für den Kostenübernahmeantrag) zwischen den Parteien klar vereinbart war, stellt die Verwendung der Fotos in einem Vortrag eine unerlaubte Zweckänderung dar. Eine Einwilligung zur Nutzung der Fotos in einem Vortrag war nicht erteilt. Eine andere Bedingung des § 6 Abs. 1 KDG war auch nicht erfüllt. Die Veröffentlichung war mithin rechtswidrig. Der Datenschutzverstoß wurde durch unsere Behörde geahndet.

4.4 Verlorene Unterlagen

1. Unserer Dienststelle wurde gemeldet, dass eine Spaziergängerin neben einem Radweg an einer viel befahrenen Straße Dokumente gefunden hat, aus denen sich Stationsbelegungen eines Krankenhauses ergaben. Aus den Belegungsplänen ergaben sich die Namen der Patienten, das Alter, zum Teil deren Verweildauer nach BGB bzw. Psychisch-Kranken-Gesetz (PsychKG) sowie teilweise auch Angaben zu auffälligen Verhaltensweisen. Allein die Unterbringung nach BGB-Vorschriften lassen Rückschlüsse auf die gesundheitliche Gefährdung/Beeinträchtigung der Personen zu. Gleiches gilt für eine Unterbringung gem. PsychKG.

Der Verantwortliche hat angegeben, dass es sich bei diesen Belegungslisten um Übergabelisten zum Schichtwechsel handelt. Auch wenn in der betroffenen Einrichtung Regelungen zum Umgang mit diesen Listen bestehen und es untersagt ist, diese Listen außerhalb des Stationsgebäudes mitzuführen, wurde der Vorfall zum Anlass genommen, den Verstoß zu be-
anstanden, um den Verantwortlichen nachhaltig zur Einhaltung des Datenschutzes anzuhalten.

2. Gemeldet wurde uns ein weiterer Fall. Einer Mitarbeiterin einer Suchtberatung ist auf dem Heimweg nach Dienstschluss eine Tasche mit

³³ OLG Zweibrücken, Urteil vom 07.06.2010 -4 W 53710



Unterlagen von 6 Klienten einer Haftanstalt verloren gegangen. Die Unterlagen enthielten den Namen, das Geburtsdatum, das Geschlecht, die Staatsangehörigkeit, den Aufenthaltsort (JVA), die Aktenzeichen und die Art der Straftaten sowie die Dauer der Unterbringung.

Angegeben worden ist, dass zum Aufgabenspektrum der Mitarbeiter Suchtberatung neben der Beratung vor Ort auch die Beratung von inhaftierten Klienten gehört. Die Mitarbeiter nehmen zu diesen Terminen, welche in den Haftanstalten wahrgenommen werden, die jeweiligen Akten mit. Da die betroffene Mitarbeiterin in unmittelbarer Nähe zur Justizvollzugsanstalt wohnt, in der sie Termine wahrzunehmen hatte, hat diese die Unterlagen am Vortag mit nach Hause genommen, um nicht am nächsten Tag zunächst in die Dienststelle fahren zu müssen, um die Unterlagen abzuholen. Dies wäre mit einem hohen Zeitaufwand verbunden gewesen. Da diese Verfahrensweise mit der Einrichtungsleitung und der Datenschutzkoordinatorin abgestimmt war, alle Mitarbeiter zum Datenschutz eingewiesen und geschult sind und eine Verpflichtungserklärung gem. § 5 KDG unterzeichnet haben, haben wir es bei der Feststellung einer Datenschutzverletzung belassen und keine Sanktionen verhängt.

4.5 Videoüberwachung

Im Rahmen einer anlasslos durchgeführten Datenschutzüberprüfung wurde im Jahr 2020 in einer Klinik festgestellt, dass die Ein- und Ausgänge überwacht werden und insgesamt 14 Kameras vorhanden waren. Mit der Klinikleitung wurde die Erforderlichkeit der Kameraüberwachung erörtert.

Im Ergebnis konnte nur teilweise Einigkeit über die Erforderlichkeit von einzelnen Kameras erzielt werden.

Hinsichtlich der weiteren Kameras konnte kein Konsens gefunden werden, was im Ergebnis dazu führte, dass mit einem Beanstandungsbescheid im Jahr 2021 festgestellt worden ist, dass die Videoüberwachung mit 3 Kameras unzulässig ist.

Der Verantwortlichen wurde die Auflage erteilt, diese Kameras abzuschalten. Gegen diesen Bescheid wurde Rechtsmittel eingelegt. Das Verfahren wurde vor dem Interdiözesanen Datenschutzgericht geführt. In der mündlichen Verhandlung hat das Gericht ausgeführt, dass es der Auffassung ist, eine



der Kameras dürfte nach derzeitigem Stand der Sachverhaltsaufklärung nicht erforderlich sein, da die überwachte Tür durch eine Schließanlage gesichert ist. Dieser Einschätzung ist der, die Verantwortliche vertretende, Prozessvertreter nicht entgegengetreten.

Die Erforderlichkeit der beiden weiteren Kameras wurde vom Gericht ebenfalls nicht gesehen. Der Verantwortlichen wurde empfohlen, die Notwendigkeit der Überwachung mit diesen beiden Kameras zu überprüfen.

Die Parteien schlossen in der mündlichen Verhandlung einen Vergleich. Die Verantwortliche verpflichtete sich den Betrieb der beiden streitigen Kameras zu evaluieren und der Datenschutzaufsicht bis zum 31.07.2023 das Ergebnis der Überprüfung mitzuteilen. Bezüglich dieser beiden Kameras wurde vereinbart, dass der Bescheid insoweit aufgehoben wird. Bezüglich der weiteren Kamera wurde der Bescheid vom 04.10.2021 unstreitig bestandskräftig.

Mit Schreiben vom 31.07.2023 hat die Verantwortliche unserer Datenschutzaufsicht mitgeteilt, dass eine Evaluation des Betriebes der Kameras erfolgt ist und diese zwischenzeitlich außer Betrieb genommen worden sind. An einem Donnerstag Anfang September wurde im Rahmen einer unangekündigten Kontrolle festgestellt, dass alle 3 Kameras weiterhin in Betrieb waren. Seitens der hinzugezogenen Datenschutzkoordinatorin wurde versucht, das mit technischen Schwierigkeiten zu entschuldigen.

Am darauffolgenden Montag hat die Verantwortliche der Datenschutzaufsicht per E-Mail Screenshots des Monitors am Empfang (vorher/nachher) übersandt. Auf den Aufnahmen ist erkennbar, dass die Kameras am Tag nach der Kontrolle (um 13:25 Uhr) ausgeschaltet sind.

Der Verantwortlichen wurde dieser Sachverhalt mitgeteilt und Gelegenheit zur Stellungnahme gegeben. Die Verantwortlichen hat dann unstreitig gestellt, dass der Betrieb der einen Kamera spätestens seit 18.01.2023 (mündliche Verhandlung) und der Betrieb der beiden anderen Kameras seit dem 31.07.2023 unzulässig war und dass diese nunmehr abgeschaltet sind.

Da ein Verstoß gegen § 52 KDG vorliegt, wurde dieser Verstoß sanktioniert und ein Bußgeld im fünfstelligen Bereich festgesetzt. Das Bußgeld wurde vom Verantwortlichen akzeptiert und bezahlt.



5 Datenschutz in Kita und Schule

5.1 Verarbeitungstätigkeiten in Kindertagesstätten

5.1.1 Ein Verzeichnis für Verarbeitungstätigkeiten – nicht nur lästiges Übel

Bereits in den letzten Jahren sowie auch in diesem Berichtsjahr wurden bzw. sind Kindertagesstätten durch unsere Dienststelle überprüft worden. Dabei wurden unserer Dienststelle auch die Verzeichnisse für Verarbeitungstätigkeiten – das Herzstück eines jeden Datenschutzkonzeptes – vorgelegt. In einigen Einrichtungen waren diese Verzeichnisse nicht vorhanden oder fehlerhaft. Ursächlich dafür ist eine große Unsicherheit bezüglich ihrer Erstellung und der zu enthaltenden Angaben. Auch ist den Einrichtungen nicht immer klar, für welche Verfahren ein Verzeichnis zu erstellen ist.

Dabei hat es einen enormen Vorteil einen Überblick aller Verarbeitungsvorgänge zu haben, bei denen personenbezogene Daten verarbeitet werden. So bringt ein ordentlich geführtes Verzeichnis Struktur in die Datenschutzdokumentation und hilft dabei die Vorgaben, die sich aus dem Datenschutzrecht ergeben, einzuhalten. Es lässt sich beispielsweise schnell erkennen, welches personenbezogene Datum an welcher Stelle verarbeitet wird und an welche Stellen diese Daten übermittelt werden.

Verarbeitungstätigkeiten, die regelmäßig in einer Kindertagesstätte anfallen, sind u.a.:

- Anmeldung eines Kindes / Wartelisten etc.
- Aufnahme und Abschluss eines Betreuungsvertrages
- Führen / Anlegen einer Kinderakte (Stammdaten)
- Anwesenheitslisten
- Anlegen von Notfalllisten (Telefonnummern der Eltern) und/oder Abhollisten



- Gruppen- und Geburtstagslisten
- Portfolioarbeit
- Entwicklungsdokumentation, Bildungsbeobachtung etc.
- Anfertigen und Ausdrucken von Fotos
- Unfallmeldungen, Meldungen ans Gesundheitsamt
- Kita-Apps
- Mitarbeiterlisten
- Mitarbeiterverträge
- Dienstpläne
- Arbeitszeiterfassung

(Diese Liste ist nicht vollständig)

5.1.2 Inhalt eines Verarbeitungsverzeichnisses in Kindertageseinrichtungen

Jede einzelne Verarbeitungstätigkeit muss durch den Verantwortlichen dokumentiert werden. Der Inhalt dieser Dokumentation ist in § 31 Abs. 1 KDG beschrieben. Folgende Angaben müssen dabei enthalten sein:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie des betrieblichen Datenschutzbeauftragten, sofern ein solcher zu benennen ist;

Anzugeben sind hierbei die Anschrift und die elektronischen und telefonischen Kontaktdaten der Verantwortlichen sowie des betrieblichen Datenschutzbeauftragten. Bei dem Verantwortlichen ist die Person gemeint, die allein oder mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Im Bereich der von Kindertagesstätten können dies die Leitungen der Einrichtung sein und nicht zwingend der Pfarrer der Trägerpfarre oder die Geschäftsführung des Trägervereins. Je



nach Entscheidungskompetenz der Leitung kann es sich auch um gemeinsame Verantwortliche handeln.

b) die Zwecke der Verarbeitung;

Für jede Verarbeitung personenbezogener Daten muss ein eindeutiger und aussagekräftiger Zweck angegeben werden. Der Zweck der Verarbeitung sollte die Verarbeitungstätigkeit näher beschreiben.

Ziel den Zweck genauer zu beschreiben ist, dass sich der Verantwortliche mit der Datenverarbeitung auseinandersetzt. Ein weiterer wichtiger Punkt ist die Einhaltung des gesetzlichen Erlaubnistatbestandes. Im Datenschutzrecht dürfen Daten nur verarbeitet werden, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat. Die Verarbeitung ist im maßgebenden KDG nur erlaubt, wenn eine Bedingung aus § 6 Abs. 1 erfüllt ist. Daher kann es auch sinnvoll sein, die Rechtsgrundlage beim Zweck der Verarbeitung zu benennen oder ggf. separat im Verzeichnis aufzuführen.

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

Für jede Verarbeitungstätigkeit ist die Kategorie der Personen zu nennen, die von der Verarbeitung betroffen ist. In einer Kindertagesstätte sind das vor allem die zu betreuenden Kinder, aber auch die Erziehungsberechtigten und Mitarbeitenden.

Im Weiteren sind auch die Kategorien der personenbezogenen Daten zu beschreiben, die in der jeweiligen Verarbeitungstätigkeit verarbeitet werden.

In Kindertageseinrichtungen fallen regelmäßig (nicht ausschließlich) folgende Datenkategorien an:

- Anschrift und Kontaktdaten (Telefon, E-Mail) der Erziehungsberechtigten, Bankverbindung
- Geburtsdatum des Kindes
- Ggf. Staatsangehörigkeit und Konfession
- Angaben zum Sorgerecht
- Fotos, Videos, Tonaufzeichnungen



- Gesundheitsdaten (z. B. Allergien, Impfungen, Behinderungen, Krankheiten)
- Entwicklungsdaten
- Anschriften und Kontaktdaten von Mitarbeitenden
- Ggf. Informationen zum Arbeitsverhältnis (z. B. Umfang, Befristung, Arbeitszeit)
- Urlaub, Krankheit und Fortbildung von Mitarbeitenden

d) gegebenenfalls die Verwendung von Profiling;

Durch die Verwendung von Profiling-Methoden kann ein genaues Profil über Verhaltensweisen einzelner Personen erstellt werden. In die Privatsphäre dieser Personen wird dadurch in besonderem Umfang eingegriffen.³⁴ Nach unserer Ansicht gibt es für Profiling in Kindertagesstätten keinen Anlass. Im Gegenteil, die Einrichtung soll dem Kind Schutz bieten. Jedes Kind soll sich frei entfalten und entwickeln können.

e) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

In einigen Verarbeitungstätigkeiten werden die personenbezogenen Daten an weitere (externe) Empfänger übermittelt. Diese müssen an dieser Stelle beschrieben werden. Empfänger der Daten können im Kita-Bereich beispielsweise das Jugend- und Gesundheitsamt, die Kommune zur Kostenabrechnung, der Essensanbieter, aber auch IT-Dienstleister oder Kita-App-Betreiber, mit denen ein Auftragsverarbeitungsvertrag besteht, sein. Dadurch kann es auch im Kita-Bereich möglich sein, dass ein Empfänger personenbezogener Daten in einem Drittland ansässig ist (siehe nächster Punkt).

f) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationalen Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation und der dort getroffenen geeigneten Garantien;

³⁴ Johanna Werperts, in: Sydow, Kirchliches Datenschutzrecht, 1. Auflage 2021, § 31 Rn. 9



Der Drittlandtransfer wird nur zutreffen, wenn etwaige IT-Dienstleister, Software, Apps oder Videokonferenztools eingesetzt werden. Für die Übermittlungen personenbezogener Daten an Kommunen, Träger oder Ämter ist dieser Punkt nichtzutreffend.

Beachtet werden aber muss im Gegensatz zu den Bestimmungen aus der DS-GVO, dass auf jeden Fall geeignete Garantien für die Datenübermittlung erbracht werden müssen, unabhängig davon ob bereits Angemessenheitsbeschlüsse bestehen.

g) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

An dieser Stelle ist abschließend für jede Verarbeitungstätigkeit die Löschfrist (Aufbewahrungszeit) zu nennen. Es gibt Verarbeitungstätigkeiten, wie z.B. das Anlegen eines Portfolios, zu denen keine gesetzlichen Aufbewahrungspflichten bestehen, weil der Zweck, zu dem diese angefertigt worden sind, mit Beendigung der Betreuungszeit entfällt. Dagegen gibt es etliche Verfahren, für deren Datenspeicherung gesetzliche Aufbewahrungsfristen maßgebend sind. Die Löschfristen können sich auch aus den Nachweis- oder Rechenschaftspflichten gegenüber der Jugendhilfe, dem Träger, der Kommune oder der Unfallkasse ergeben. Es genügt auch kein allgemeiner Verweis auf die Aufbewahrungsfrist, sondern es sind genaue Angaben zur Speicherdauer zu machen (in Jahren).

h) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 26 dieses Gesetzes.

Die technischen und organisatorischen Maßnahmen sollen die einzelnen Verarbeitungsvorgänge absichern bzw. sicherer machen, damit es zu keinem Verlust, unbefugter Offenlegung oder weiterer Datenschutzverletzungen kommt. Hierbei kann im Allgemeinen auf eine Anlage verwiesen werden, in der alle diese Maßnahmen und ihr Schutzzweck erfasst sind.

Effektive Maßnahmen im Bereich der Kindertageseinrichtungen können sein:

- das Verschließen des Büros der Leitung
- Verschließbare Schränke für sensible Unterlagen



- Regelmäßiges Löschen von Fotos, wenn diese auf technischen Endgeräten gespeichert sind
- Verschlüsselte Datenübertragung für notwendige Empfänger nutzen
- BCC-Funktion für Elterninformationen
- Begrenzte Zutrittsmöglichkeit für die Sorgeberechtigten und Besucher

Im Anhang von diesem Bericht ist ein Muster der Verarbeitungstätigkeit Aufnahmevertrag enthalten.

5.2 Datenschutzvorfälle

5.2.1 Enkeltrick in der Kita

Der Enkeltrick gehört zu den häufigsten Betrugsmaschen. Kriminelle geben sich dabei als Enkel bzw. Angehöriger aus, kontaktieren die Betroffenen per Telefon, E-Mail, SMS oder WhatsApp und bitten unter irgendeinem ominösen Umstand um Geld. Dabei werden der oder die Täter immer einfallsreicher. So wurde in einer Kindertagesstätte in unserem Zuständigkeitsgebiet das E-Mail-Postfach der Leitung gehackt und an die Mailadressen der Eltern im Namen der Leitung eine E-Mail versendet. Die E-Mail enthielt eine Geldforderung, da sich die Kita-Leitung angeblich in der Türkei befinde und aufgrund eines Diebstahls dringend Geld benötige.

Der Datenschutzvorfall wurde unserer Dienststelle gemeldet, da durch den Hackerangriff die E-Mailadressen der Eltern sowie deren Namen und Kommunikationsinhalte unbefugt offengelegt worden sind. Die Kita-Leitung hat damit richtig eingeschätzt, dass ein Verlust der Kontrolle über die eigenen Daten, Identitätsdiebstahl und -betrug als Folgen des Datenschutzvorfalls eintreten können. Auch finanzielle Verluste können die Folge sein, falls auf die Geldforderungen der Täter eingegangen wird.

Im Weiteren ist eine Information an alle Sorgeberechtigten erfolgt, der IT-Service wurde hinzugezogen und der Fall wurde polizeilich zur Anzeige gebracht. Glücklicherweise ist niemand auf die Geldforderung eingegangen.



In diesem Zusammenhang möchten wir darauf hinweisen, dass ein E-Mail-Postfach kein sicherer und damit geeigneter Ablageort von personenbezogenen Daten ist. Personenbezogene Daten sind in diesem Fall nicht nur die Namen und die dazugehörigen E-Mail-Adressen, sondern auch Adressen und Telefonnummern, die zusammen als Kontakt im Adressbuch gespeichert werden können. Zudem können in den Kommunikationsinhalten auch personenbezogene Daten, u.U. auch personenbezogene Daten besonderer Kategorie enthalten sein.

5.2.2 Zugriff auf Kinderakten

In einer Einrichtung hat sich eine Hauswirtschaftskraft unberechtigter Weise Zugriff zu zwei Kinderakten verschafft. Hintergrund war, dass sich genau in diesen Kinderakten Gesprächsprotokolle der Kitaleitung mit einem Sorgeberechtigten der Kinder befanden. Das Gespräch wurde am Vortag geführt. Glücklicherweise ist es "nur" bei einer kurzen Einsichtnahme geblieben, da die Hauswirtschafterin von einem Mitarbeitenden dabei er tappt wurde.

Kinderakten können neben personenbezogene Daten gem. § 4 Nr. 1 KDG (Adresse, Geburtsdatum) auch personenbezogene Daten besonderer Kategorie gem. § 4 Nr. 2 KDG (Gesprächsprotokolle, Meldungen an Gesundheits- oder Jugendämter, Zuziehen weiterer Hilfen) enthalten. In diesem Fall enthielten die Akten Gesprächsprotokolle, aus denen das Hinzuziehen weiterer Hilfen resultierte. Deren missbräuchliche Verarbeitung kann die Betroffenen in ihrer gesellschaftlichen Stellung beeinträchtigen. Sie sind daher als besonders schutzwürdig anzusehen. Nach § 7 Abs. 1 lit. f) KDG müssen personenbezogene Daten in einer Weise verarbeitet und somit auch aufbewahrt werden, die eine angemessene Sicherheit dieser Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung.

Ursächlich für diesen unbefugten Zugriff war, dass das Büro, in dem die Kinderakten aufbewahrt worden sind, nicht verschlossen war. Die Einrichtung hat nach diesem Vorfall sofort reagiert. Das Büro wird sobald es nicht



besetzt ist verschlossen. Den Schlüssel hat die Einrichtungsleitung und im Vertretungsfall die Vertretung.

Aufgrund der zeitnahen und sachgemäßen Umsetzung sicherheitserhöhender Maßnahmen zur Aufbewahrung der Kinderakten haben wir zwar einen Datenschutzvorfall festgestellt, aber von weiteren Auflagen oder Sanktionen abgesehen.

5.2.3 Speichermedien auf Abwegen

Speicherkarten für Fotokameras aber auch USB-Sticks überzeugen durch ihre Eigenschaft, dass relativ große Datenmengen auf einem kleinen Gerät gespeichert und ohne große technische Kenntnisse übertragen und weiterverarbeitet werden können. Ein Vorteil ist auch, dass diese kleinen Geräte bzw. Medien sehr platzsparend sind. Doch genau das wird ihnen immer wieder zum Verhängnis. Sie gehen verloren.

Sind auf diesen Medien im Fall eines Verlustes unverschlüsselt personenbezogene Daten, wie zum Beispiel Fotos oder Teilnehmerlisten, gespeichert, werten wir diesen Verlust als Datenschutzverletzung. Denn in einem solchen Fall handelt es sich um eine unbefugte Offenlegung, da Dritten eine Kenntnisnahme eingeräumt wird, auch dann, wenn die Kenntnisnahme lediglich möglich ist.

Auch im Berichtsjahr 2023 haben wir mehrere Beanstandungen gegenüber Einrichtungen aussprechen müssen, denen derartige Medien abhandengekommen waren.

6 Datenschutz im Beschäftigungsverhältnis

6.1 Im Interessenkonflikt – Betriebsratsvorsitzender als Datenschutzbeauftragter

Das Bundesarbeitsgericht³⁵ (BAG) hat sich in seinem Urteil vom 06.06.2023 erneut mit der Frage beschäftigt, ob ein Betriebsratsvorsitzender gleichzei-

³⁵ BAG, Urteil vom 06.06.2023 -9 AZR 383/19



tig auch das Amt des Datenschutzbeauftragten ausführen kann. Der EuGH hat am 09.02.2023³⁶ zu dieser Frage bereits eine Entscheidung getroffen. Der EuGH hat mit Klarheit festgestellt, dass die nationalen Vorschriften § 38 Abs. 2 i. V. m. § 6 Abs. 4 Satz 1 BDSG grundsätzlich mit Unionsrecht und speziell mit der DS-GVO vereinbar sind. Nach Ansicht des EuGHs muss jedoch in jedem Einzelfall geprüft werden, ob durch die Abberufung des Datenschutzbeauftragten die Verwirklichung der Ziele der DS-GVO gefährdet ist. Liegt ein Interessenkonflikt vor, so dürfte nach Ansicht des EuGHs eine Abberufung zulässig sein.

Im nunmehr entschiedenen Fall hat das BAG einen Interessenkonflikt bejaht. Die vorhergehenden Instanzen, u.a. das Landesarbeitsgericht (LAG) Sachsen³⁷ und das Arbeitsgericht Dresden hatten festgestellt, dass die Stellung als Betriebsratsvorsitzender einer Bestellung zum betrieblichen Datenschutzbeauftragten nicht entgegensteht. Begründet wurde dies mit den Regelungen aus § 38 Abs. 2 BDSG i. V. m. § 6 Abs. 4 Satz 1 BDSG, so dass ein betrieblicher Datenschutzbeauftragter nur aus wichtigem Grund i.S.v. § 626 BGB abberufen werden kann.

Zur Begründung führt das BAG an, dass personenbezogene Daten dem Betriebsrat nur zu Zwecken zur Verfügung gestellt werden dürften, die das Betriebsverfassungsgesetz ausdrücklich vorsehe. Der Betriebsrat entscheide durch Gremiumsbeschluss darüber, unter welchen konkreten Umständen er welche personenbezogenen Daten vom Arbeitgeber fordere und auf welcher Weise er diese anschließend verarbeite. In diesem Rahmen lege er die Zwecke und Mittel der Verarbeitung personenbezogener Daten fest. Aus diesem Grund könne der Betriebsratsvorsitzende die Einhaltung des Datenschutzes nicht hinreichend unabhängig überwachen.

Damit setzt sich das BAG in Widerspruch zur Entscheidung des Gesetzgebers. In § 79a BetrVG ist ausdrücklich festgelegt, dass der Betriebsrat Teil des Verantwortlichen und gerade nicht eigener Verantwortlicher ist.

Das Urteil findet aber im Bereich des kirchlichen Datenschutzes keine Anwendung. § 36 Abs. 7 KDg legt abschließend fest, welche Beschäftigten

³⁶ EuGH, Urteil vom 09.02.2023 -C-453/21

³⁷ LAG Sachsen, Urteil vom 23.08.2019 - 1 O 80/19



von der Benennung zum betrieblichen Datenschutzbeauftragten ausgenommen sind.

6.2 Offboarding – Löschung personalisierter E-Mail-Konten von Beschäftigten

Was müssen Arbeitgeber bei der Löschung personalisierter E-Mail-Konten von Beschäftigten beachten?

Diese Frage wurde uns im Berichtszeitraum von einer Verantwortlichen gestellt. Verfügen Beschäftigte über ein dienstliches personalisiertes E-Mail-Konto, stellt sich für den Arbeitgeber als Verantwortlichem bei deren Ausscheiden stets die Frage, wie mit dem E-Mail-Konto zu verfahren ist. Idealerweise wird der Umgang mit dienstlichen E-Mail-Konten im Vorhinein in einer Verfahrensbeschreibung geregelt. Handelt es sich um E-Mail-Adressen, die durch den Namen der beschäftigten Person gekennzeichnet sind, hat der Verantwortliche für deren unverzügliche Deaktivierung nach dessen Ausscheiden Sorge zu tragen.

Grundsätzlich steht es dem Arbeitgeber frei, die private Nutzung eines dienstlichen E-Mail-Postfachs zu zulassen oder zu untersagen. Bei personalisierten Postfächern besteht aber stets die Möglichkeit, dass die oder der Beschäftigte E-Mails mit privaten Inhalten erhält, auch wenn das Konto von den Beschäftigten ausschließlich dienstlich genutzt wird bzw. werden darf. Solche E-Mails dürfen in jedem Fall nicht weiter inhaltlich zur Kenntnis genommen werden, sobald ihr privater Charakter deutlich wird. Dienstliche E-Mails kann sich ein Arbeitgeber zwar von den Beschäftigten vorlegen lassen, jedoch überschreitet eine automatisierte Weiterleitung in der Regel die Grenze der Erforderlichkeit für betriebliche Zwecke. Bei einem Ausscheiden einer oder eines Beschäftigten sollte daher ein personalisiertes E-Mail-Postfach umgehend mit dem Ausscheiden deaktiviert werden, damit dort keine weiteren E-Mails eingehen können.

Was ist zu tun?

Arbeitgeber sollten klare, schriftliche Vorgaben machen, wie bei einem Ausscheiden aus dem Betrieb mit dem E-Mail-Postfach und archivierten E-Mails der betroffenen Person zu verfahren ist. Ein personalisiertes Postfach ist mit dem Ausscheiden aus dem Betrieb zu deaktivieren, private E-Mails



sind zu löschen. Den Beschäftigten ist schon vorab die Möglichkeit zu geben, private E-Mails zu löschen. Private E-Mails sollten zudem in einem separaten Ordner gespeichert werden.

6.3 Anspruch auf Entfernung einer Abmahnung aus einer Personalakte

Datenschutzrechtliche Fragestellungen gewinnen im Rahmen arbeitsrechtlicher Auseinandersetzungen in der Praxis weiter an Bedeutung. Gestritten wird vor allem um die Reichweite und Grenzen des Auskunftsanspruchs nach Art. 15 DS-GVO (vgl. Ausführungen zu Entscheidungen des EuGHs unter Punkt 1. in unserem Tätigkeitsbericht).

Die Entwicklungen rund um andere im Datenschutzrecht verankerte Betroffenenrechte sollten dabei jedoch nicht aus dem Blickfeld geraten. Diskutiert wird in der Rechtsprechung im Zusammenhang mit dem Entfernungsanspruch einer Abmahnung aus der Personalakte die Anwendbarkeit der DS-GVO auf in Papierform geführte Personalakten.

Das LAG Baden-Württemberg³⁸ bejaht in einer aktuellen Entscheidung – abweichend zu anderen Arbeitsgerichten – die Anwendbarkeit der DS-GVO auf in Papierform geführte Personalakten und daraus folgend einen Anspruch auf Entfernung einer Abmahnung aus der Personalakte nach Beendigung des Arbeitsverhältnisses. Die Entscheidung geht über das Abmahnungsrecht hinaus und hat Auswirkungen auf den generellen Umgang mit den in Personalakten enthaltenen Daten.

Das ist passiert

Ein Arbeitnehmer arbeitete für mehrere Jahre in einem Fitnessstudio. In diesem Zusammenhang erhielt er eine Abmahnung mit dem Vorwurf, Arbeitszeiten unrichtig angegeben zu haben. Als er sein Arbeitsverhältnis beendete, forderte er den Arbeitgeber auf, die Anschuldigung des Arbeitszeitbetrugs zurückzunehmen - also die Abmahnung- aus seiner Personalakte zu entfernen. Außerdem forderte er Auskunft über personenbezogene Daten und Übermittlung der Personalakte. Nachdem sich der Arbeitgeber weigerte, erhob er Klage vor dem Arbeitsgericht. Neben der Entfernung der Abmahnung aus der Personalakte forderte der Kläger u.a. auch Schadensersatz wegen der unterbliebenen Auskunftserteilung in Höhe von 5.000 €.

³⁸ LAG Baden-Württemberg, Urteil vom 28.07.2023 – 9 Sa 73/21



Die Argumentation des Gerichtes zum Anspruch auf Entfernung der Abmahnung

Das Gericht gab dem Kläger insoweit Recht, als dass er einen Anspruch auf Löschung der Abmahnung hatte. So habe sich der Zweck der Abmahnung, nämlich die Warnung des Arbeitnehmers vor einer möglichen Kündigung erledigt, nachdem das Arbeitsverhältnis bereits erloschen ist. Auch diene eine solche Abmahnung nicht mehr zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Die nicht mehr erforderliche Abmahnung sei daher nach Art. 17 Abs. 1 DS-GVO zu löschen, da es keine gesetzlichen Aufbewahrungsfristen für Abmahnungen gebe. Damit wird die von unserer Behörde vertretende Rechtsauffassung bestätigt.³⁹

Zur bisherigen Rechtslage

Das BAG leitete den Anspruch auf Entfernung einer Abmahnung aus einer Personalakte bislang aus §§ 242, 1004 BGB analog ab. Differenziert wurde danach, ob ein Entfernungsanspruch des Arbeitnehmers während des bestehenden Arbeitsverhältnisses oder nach dessen Beendigung geltend gemacht wurde und ob die Abmahnung rechtmäßig oder rechtswidrig war.

Nach Ansicht des BAGs haben Arbeitnehmer nach Beendigung des Arbeitsverhältnisses regelmäßig keinen zivilrechtlich begründeten Anspruch mehr auf Beseitigung - selbst einer zu Unrecht erteilten Abmahnung- aus der Personalakte. Begründet wurde diese Ansicht damit, dass kein berechtigtes Interesse auf Entfernung besteht, da die Abmahnung nach Beendigung des Arbeitsverhältnisses grundsätzlich weder das berufliche Fortkommen bei dem bisherigen Arbeitgeber behindere noch sonstige arbeitsrechtlichen Nachteile drohten.

Zur aktuellen Diskussion

Seit in Krafttreten der DS-GVO ist die Diskussion neu entfacht. Arbeitnehmer stützen den Entfernungsanspruch nunmehr zunehmend auf den Löschungsanspruch aus Art. 17 DS-GVO (§ 19 KDG). Danach sind personenbezogene Daten insbesondere dann unverzüglich zu löschen, wenn deren

³⁹ 7. Tätigkeitsbericht 2022, Punkt 6.6, KDSA



Speicherung für die Zwecke, für die sie erhoben oder verarbeitet wurden, nicht mehr notwendig ist. Mit Beendigung des Arbeitsverhältnisses haben sich die Zwecke einer Abmahnung, insbesondere deren Rüge- und Warnfunktion, grundsätzlich erledigt.

Damit wäre eine Abmahnung mit dem Beendigungsdatum aus der Personalakte zu entfernen. Voraussetzung ist jedoch, dass in Papierform geführte Personalakten dem Regelungsbereich der Vorschrift unterfallen. In der Rechtsprechung ist diese Frage umstritten. Anknüpfungspunkt ist Art. 2 Abs. 1 DS-GVO, der den Anwendungsbereich der Verordnung im Fall nicht-automatisierter Verarbeitung nur dann für eröffnet erklärt, wenn personenbezogene Daten in einem „Dateisystem“ gespeichert werden oder gespeichert werden sollen.

Nach der Ansicht des LAG Baden-Württemberg erfüllen in Papierform geführte Personalakten klar die Anforderungen an ein datenschutzrechtliches „Dateisystem“, da Personalakten in der Regel eine einheitliche äußere Gestaltung nach den Kriterien Name, Vorname, Personalnummer aufweisen. Daher stellen Sie eine strukturierte Sammlung personenbezogener Daten dar und unterfallen somit dem Begriff des datenschutzrechtlichen „Dateisystems“. Damit eine Datensammlung vorliegt bedarf es keiner Mindestanzahl von Akten. Ausreichend seien daher zwei strukturierte Vorgänge, wenn später weitere Vorgänge hinzukommen könnten, so das LAG.

Anders als das LAG Baden-Württemberg hielt kürzlich jedoch noch das LAG Sachsen⁴⁰ in Anschluss an eine Entscheidung des LAG Niedersachsen⁴¹ den Lösungsanspruch aus Art. 17 DS-GVO auf in Papierform geführte Personalakten für nicht anwendbar. Für Personalakten gelte rechtlich der Grundsatz der Vollständigkeit und nicht der Grundsatz der Datensparsamkeit. Die Anwendung datenschutzrechtlicher Grundsätze in Bezug auf Papierakten sei daher zweifelhaft und im Ergebnis wegen der weitreichenden Folgen des damit einhergehenden Rechtsschutzes abzulehnen.

Schadenersatz wegen der nichterteilten Auskunft

Das LAG entschied ferner, dass der Kläger einen Anspruch auf Zahlung einer Entschädigung i. H. v. 2.500 € wegen der z.T. erheblich verspäteten und

⁴⁰ LAG Sachsen, Urteil vom 31.03.2023 – 4 Sa 117/21

⁴¹ LAG Niedersachsen, Urteil vom 4.05.2021 – 11 Sa 1180/20



z.T. gar nicht vorgenommenen Erfüllung der Verpflichtung zur Auskunftserteilung nach Art. 15 Abs. 1 DS-GVO habe. Dem Kläger stehe ein Anspruch auf Auskunftserteilung nach Art. 15 Abs. 1 Satz 1 DS-GVO ohne weiteres zu, da der geltend gemachte Anspruch hinreichend bestimmt war, um ein Tätigwerden der Beklagten im Sinne einer Auskunftserteilung zu veranlassen. In Abwägung dieser Gesamtumstände sah das LAG eine Entschädigung von 2.500 € als angemessen an.

Die Revision gegen das Urteil des LAG Baden-Württemberg ist inzwischen beim BAG unter dem Aktenzeichen 8 AZR 215/23 anhängig. Aufgrund der Bedeutung des Rechts auf Vergessenwerden (Art. 17 DS-GVO/ § 19 KDG) ist eine höchstrichterliche Klärung des Anwendungsbereichs der DS-GVO wünschenswert.

Folgen für die Praxis

Die Nichtbeachtung datenschutzrechtlicher Betroffenenrechte kann im Einzelfall zu drastischen Rechtsfolgen führen. Ratsam ist bis zur höchstrichterlichen Klärung eines datenschutzrechtlichen Löschananspruches personenbezogener Daten in Papierakten zur Vermeidung von Sanktionen den Datenbestand in Personalakten zu prüfen und ein Löschkonzept zu etablieren, um sicherzustellen, dass sowohl im laufenden Arbeitsverhältnis als auch bei Beendigung des Arbeitsverhältnisses nur solche Dokumente in der Personalakte des jeweiligen Arbeitnehmers enthalten sind, welche rechtlich noch aufbewahrt werden dürfen.

Es dürfte mittlerweile bekannt sein, dass Arbeitnehmer einen Auskunftsanspruch nach Art. 15 DS-GVO (§ 17 KDG) im Hinblick auf ihre personenbezogenen Daten haben. Dieser Auskunftsanspruch muss zwingend erfüllt werden, um Schadensersatzansprüche zu vermeiden, wie die besprochene Entscheidung zeigt.

6.4 Zeitwertkonten – Musterberechnung

Eine Einrichtung möchte Zeitwertkonten für ihre Beschäftigten einführen.

In diesem Zusammenhang wurde uns von einem Petenten mitgeteilt, dass die Geschäftsführung dieser Einrichtung personenbezogene Daten von



Beschäftigten an eine Versicherungsgesellschaft weitergegeben und diese Gesellschaft für die Beschäftigten Muster- bzw. Beispielsrechnungen für die jeweiligen Beschäftigten erstellt habe. Dabei seien u. a. folgende Daten von der Weitergabe betroffen gewesen: Name, Vorname, Geburtsdatum, Anschrift, Bruttoentgelt, Kinderfreibetrag, Steuerklasse. Eine Zustimmung der Mitarbeitenden zu dieser Übertragung sei weder erfragt, noch von diesen erteilt worden.

Im Rahmen der Prüfung stellte sich heraus, dass Geschäftsführung und Mitarbeitervertretung übereingekommen sind, Zeitwertkonten einzuführen. Eine entsprechende Dienstvereinbarung wurde geschlossen. Um den Beschäftigten deutlich zu machen, welche Möglichkeiten ihnen durch diese Konten eröffnet werden, beauftragte die Einrichtungsleitung das Versicherungsunternehmen Beispielsrechnungen individuell für einzelne Beschäftigte zu erstellen. Dafür wurde mit dem Versicherungsunternehmen ein Auftragsverarbeitungsvertrag abgeschlossen. Auftragsverarbeiter ist gem. § 4 Nr. 10 KDG eine natürliche oder juristische Person, ... die allein oder gemeinsam mit anderen personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Verantwortliche bestimmt dabei weiterhin Zweck und Mittel der Verarbeitung. Der Auftragsverarbeiter verarbeitet die ihm übertragenen personenbezogenen Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen. Nach Erreichung des Zwecks werden die personenbezogenen Daten dem Verantwortlichen vom Auftragsverarbeiter zurückgegeben.

Es handelt sich insoweit bei dem Auftragsverarbeiter nicht um einen Dritten i. S. v. § 4 Nr. 12 KDG.

Die Einrichtung ist berechtigt die personenbezogenen Daten zu verarbeiten, also auch an den Versicherer zu übermitteln, wenn dies im Rahmen einer Auftragsverarbeitung gem. § 29 KDG erfolgt.

Durch die Verarbeitung der personenbezogenen Daten durch das Versicherungsunternehmen als Auftragsverarbeiter ist eine Verletzung des Schutzes personenbezogener Daten, die eine Verletzung der Rechte und Freiheiten einer natürlichen Person darstellt, nicht verbunden. Über den Auftragsverarbeitungsvertrag ist sichergestellt, dass das Versicherungs-



unternehmen die erlangten Daten nicht für eigene kommerzielle Zwecke missbraucht. Ein Datenschutzverstoß konnte nicht festgestellt werden.

7 Technischer Datenschutz

7.1 E-Mail-Postfach gehackt - was können Sie jetzt tun

Trotz Sicherheitsvorkehrungen und sicherer Passwörter kommt es immer mal wieder vor, dass sich Kriminelle Zugriff zu E-Mail-Accounts verschaffen, z.B. durch Account-Phishing.

Sie versenden anschließend Nachrichten über den E-Mail-Account im Namen des Absenders und bitten -wie so oft- um Geldzuwendungen, weil der angebliche Absender beispielsweise in eine Notsituation geraten ist oder versenden weitere Phishing-Mails oder Schadsoftware.

In einem weiteren Verlauf tragen sich die Kriminellen mit einer E-Mail-Adresse zur Weiterleitung von eingehenden Nachrichten ein und ändern die Zugangsdaten (Passwort), so dass der eigentliche Inhaber des E-Mail-Accounts keinen Zugriff mehr auf sein Postfach hat.

Die Geschädigten (Opfer) erfahren meistens erst viel später davon, z.B. wenn sie von Empfängern, die Nachrichten mit bedenklichen Inhalten empfangen haben, angesprochen werden oder wenn ihnen der Zugang zum E-Mail-Postfach aufgrund der Passwortänderung nicht mehr möglich ist.

Kommt für die E-Mail-Kommunikation eine Software zum Einsatz, die man üblicherweise ohne zusätzliche Eingabe der E-Mail-Accountdaten (Login/Passwort) nutzt, wie z. B. Microsoft Outlook, so kann ein typisches Verdachtsmoment für eine Kompromittierung des E-Mail-Accounts sein, dass z.B. kein Empfang neuer Nachrichten möglich ist.

Was kann man tun, falls eine Kompromittierung auffällig wird?

- Ändern des Passworts, solange ein Zugriff zum Postfach noch möglich ist. Ist dieses nicht der Fall, wenden Sie sich zeitnah an die



zuständige IT-Abteilung bzw. einen Administrator des E-Mail-Postfachs, ggf. auch an den Provider.

- Informieren Sie ggf. weitere Personen nach einer Meldekette für IT-Sicherheitsvorfälle.

Weitere mögliche Schritte:

- Löschen Sie nicht vorschnell den Account, sondern sperren Sie den betroffene E-Mail-Account für eine Untersuchung und Beweissicherung.
- Informieren Sie ggf. die zuständige Behörde/Polizei über diesen Vorfall und sprechen Sie den weiteren Verlauf ab, damit z.B. wichtige Daten für Analysezwecke nicht vorzeitig vernichtet werden.

Führen Sie einen Viren-Scan auf allen Geräten durch, von denen Sie Zugriff auf das E-Mail-Postfach hatten (z.B. Laptop, Smartphone...).

- Richten Sie ein neues E-Mail-Postfach mit neuer E-Mail-Adresse ein.
- Informieren Sie alle Kontakte über die neue E-Mail-Adresse mit dem Hinweis, dass es ab dem jetzigen Zeitpunkt keine Nachrichten mehr von der alten E-Mail-Adresse geben wird.
- Ggf. können die aktiven Empfänger die alte E-Mail-Adresse als „Junk-/Spam-Absender“ in ihrem E-Mail-Programm markieren.
- Prüfen Sie zusammen mit Ihren betrieblichen Datenschutzbeauftragten, ob Sie eine Meldung nach § 33 KDG auslösen müssen.
- Prüfen Sie Dienste oder Logins, die mit dem E-Mail-Account verknüpft waren und vergeben Sie auch hierfür neue Zugangsdaten. Grundsätzlich sollten immer unterschiedliche Passwörter für unterschiedliche Dienste/Logins genutzt werden.
- Wenn es noch möglich ist, durchsuchen Sie Ihre E-Mails nach Zugangsdaten oder weiteren Informationen, die die Kriminellen abgefangen haben könnten, z.B. im Rahmen von Passwort-Rücksetzfunktionen.

Empfehlung:

Das E-Mailpostfach (unabhängig vom Anbieter) ist kein zentraler und geeigneter Langzeitspeicher und kein Archiv für Kommunikationsdaten.



Information, die aufgrund von Aufbewahrungsfristen oder Rechenschaftspflichten aufbewahrt werden müssen, sind außerhalb des E-Mail-Postfachs, beispielsweise in einem Dokumentenarchiv zu sichern.

Ebenso sollten auch keine Zugangsdaten im E-Mailpostfach aufbewahrt werden.

Identitätsdaten wie z.B. auch E-Mail-Accounts werden durch Kriminelle zur weiteren Nutzung in Identity Leak Datenbanken eingetragen und zugänglich gemacht. Das Hasso-Plattner-Institute in Potsdam (HPI) stellt eine Abfrage zur Verfügung, wo man selbst überprüfen kann, ob eine E-Mail-Adresse bereits in globalen Datenbanken bekannt geworden ist.

Links:

Link: HPI Identity Leak Checker

<https://sec.hpi.uni-potsdam.de/ilc/search>

Phishing - (k)eine schöne Bescherung

<https://www.kdsa-ost.de/aktuelles/phishing-k-eine-schoene-bescherung.html>

7.2 QR-Codes – Bequemlichkeit mit Tücken?

Quick-Response-Codes (QR-Codes) haben in den letzten Jahren ihren Weg in die verschiedensten Bereiche unseres Alltags gefunden – von der Speisekarte im Restaurant über das Bezahlen von Produkten und Dienstleistungen on- und offline bis hin zum einfacheren Zugriff auf Websites. Die Vorteile von QR-Codes sind sowohl aus Unternehmenssicht als auch aus Verbrauchersicht unumstritten. Dennoch sind sie auch mit Risiken verbunden. Nutzer sollten sich der Risiken bewusst sein und sehr genau hinschauen, bevor sie ihren nächsten QR-Code scannen.

Hier ein Beispiel: Für den Super Bowl 2022 entwickelte die Krypto-Plattform Coinbase eine besonders raffinierte Werbeanzeige, bei der ein QR-Code auf einem Bildschirm herumsprang. User, die den Code scannten, wurden zum App-Download weitergeleitet und erhielten 15 US-Dollar in Bitcoin. Mit einem Anstieg an App-Installationen um 309 Prozent in der ersten Woche brachte die Werbeanzeige Coinbase zweifellos den erhofften Erfolg.

Funktion von QR-Codes

Während ein Barcode (auch Strichcode genannt) in der Regel nur kurze alphanumerische Zeichenfolgen darstellen kann, kann ein QR-Code größere Datenmengen enthalten. Es gibt zwei Arten von QR-Codes – statische und dynamische – die sich darin unterscheiden, ob die Information direkt im Code enthalten ist (transparent) oder auf Grund einer anpassbaren Umleitung erzeugt wird. Ein häufiger Anwendungsfall ist eine hinterlegte URL, die auf eine Webseite verweist, auf der sich der entsprechende Inhalt befindet, aber auch u.U. einen Download einer Datei auslösen könnte.

Statische QR-Codes werden verwendet, wenn sich die Informationen nicht ändern. Ist der Code erst einmal erzeugt, lassen sich die enthaltenen Daten nicht mehr aktualisieren (statisch). Diese Art von QR-Code wird oft zu einfachen Zwecken, wie dem Teilen von Website-Links, Kontaktdaten oder WLAN-Passwörtern u. ä. genutzt. Die Lebenszeit des statischen Codes ist, solange die enthaltenen Daten gültig sind, nicht begrenzt.



Einer der Vorteile von statischen QR-Codes mit Inhaltsdaten ist, dass die darin enthaltenen Informationen auch offline, also ohne eine Internetverbindung ausgelesen werden können. Ein weiterer Vorteil zeigt sich in der Transparenz, da die Information oder ein Link zum Ziel direkt abgelesen werden kann.

Ein einmal angefertigter statischer QR-Code lässt nicht mehr ändern und kann auch nicht zu einem dynamischen QR-Code umgewandelt/geändert werden.

Dynamische QR-Codes bieten hingegen mehr Flexibilität, ohne das Aussehen des Codes an sich zu ändern. Diese Codes enthalten eine einzigartige URL (meistens Kurz-Link), die zu einem Server führt (Ziel1), wo eine Weiterleitung zum eigentlichen Ziel (Ziel2) eingerichtet ist. Wird ein dynamischer QR-Code gescannt, wird der Benutzer nicht ohne Umweg zum eigentlichen Ziel (Ziel2) geleitet, sondern ruft zuerst das „Ziel1“ auf und erst im zweiten Schritt wird er zu dem eigentlichen „Ziel2“ weitergeleitet. Die Dynamik ist in einer technisch gestalteten flexiblen Weiterleitung zu sehen.





Diese Art macht dynamische QR-Codes zur idealen Lösung, wenn die enthaltenen Ziel-Informationen sich regelmäßig ändern und aktualisierbar sein sollen, wie z. B. bei Veranstaltungsdaten, Speisekarten in Restaurants mit z.B. Saisonkarte, Sonderangeboten oder messbaren Kampagnen.

Allerdings gilt auch hier, dass sich der Inhalt des QR-Codes nicht mehr ändern lässt. Was sich ändern lässt, ist die Weiterleitung zu „Ziel2“. Auch bei dieser Art des Codes ist die Lebenszeit vom erreichbaren Kurz-Link (URL) abhängig.

Gefahrenpotenzial mit QR-Codes

Es gibt die unterschiedlichsten Bedrohungen und Betrugsmaschen, bei denen QR-Codes von Kriminellen ausgenutzt werden. Was u.a. auf eine bequeme und scheinbar sorglose Bedienung zurückzuführen ist und sich in der Masse gut verbreiten lässt, bietet einfallsreichen Cyberkriminellen entscheidendes Verwendungspotential. Hinzu kommt, dass der Code wie ein Bild projiziert ist und somit für Sicherheitsprogramme quasi unter dem Radar übertragen werden kann.

Beispiel bekannter und verbreiteter Bedrohungen:

Phishing mit QR-Code (Quishing) – eine Betrugsmasche entstanden aus der Wortkombination „QR“ und „Phishing“. Dabei handelt es sich um einen QR-Code-basierten Phishing-Angriff, bei dem ein QR-Code dazu benutzt wird, um ein Opfer auf eine präparierte Webseite zu locken und anschließend an persönliche bzw. vertrauliche Daten zu gelangen oder den Benutzer zum Herunterladen von Dokumenten, z.B. mit integriertem Schadcode, zu verleiten.

Eine weiter verbreitete Betrugsmasche zielt auf das Quick-Response-Code-Login (QRL) ab und nennt sich **QRLJacking**. QRL wird häufig als eine Alternative zu passwortbasierten Authentifizierungsverfahren verwendet. Statt der manuellen Eingabe von Benutzername und Passwort (Bequemlichkeit) scannt der Benutzer einen angezeigten QR-Code. Damit erfolgt eine automatisierte Anmeldung am entsprechenden System/Portal, falls der Vorgang nicht durch eine zusätzliche Authentifizierungsmaßnahme (Mehrfaktor) verhindert wird.





Marketing mit QR-Codes machts möglich – Kriminelle können legitime QR-Codes an öffentlichen Orten, Restaurants, Postern etc. durch andere Codes ersetzen, die den Nutzer auf betrügerische Webseiten umleiten.

7.2.1 Vorsichtsmaßnahmen

QR-Code-Scans grundsätzlich zu vermeiden erscheint etwas unrealistisch. Nutzer können jedoch proaktive Maßnahmen ergreifen, um verbundenen Risiken zu mindern.

- **Überprüfung des Urhebers des QR-Codes:** Scannen Sie keine QR-Codes fremder Quellen, vor allem wenn diese attraktiven Angebote oder Rabatte anpreisen.
- **Vermeidung von Anmeldungen per QR-Code:** Sie sollten es möglichst vermeiden, sich mit einem QR-Code bei einer unbekanntenen Anwendung oder einem Dienst anzumelden.
- **Vorsicht bei der Eingabe persönlicher Daten:** Werden Sie nach dem Scan-Vorgang auf eine Webseite weitergeleitet, die Sie zur Eingabe persönlicher Daten auffordert, prüfen Sie, ob Sie überhaupt dorthin wollten.
- **Vertrauenswürdigen QR-Code-Scanner verwenden:** Die meisten Smartphones verfügen über eine vorinstallierte Scanner-App. Wenn Sie eine Drittanbieter-App herunterladen, überprüfen Sie ihre Vertrauenswürdigkeit.
- **Das Ziel des QR-Codes überprüfen:** Falls die Scanner-App die Möglichkeit bietet, überprüfen Sie den enthaltenen Link, wohin der QR-Code Inhalt Sie verweist.
- **Mehr-Faktor-Authentifizierung (MFA) aktivieren, wo es angeboten wird:** Sollten einige Daten in die Hände von Cyberkriminellen geraten, schützt in dem Fall die zusätzliche MFA, damit diese nicht an persönliche Daten gelangen, sich an Web-Portale anmelden oder Transaktionen auslösen. Die MFA wird nicht nur bei Banken, sondern u.a. bei vielen E-Mail-Providern angeboten.
- **Physischer QR-Code Check,** wo es möglich ist: In Einrichtungen, Restaurants, Museum etc. vor dem Scannen physisch prüfen, ob es sich um einen Original-Code handelt und nicht um einen zusätzlich überklebten QR-Code.

**Fazit:**

Cyberangriffe nehmen in rasantem Tempo zu und die Gefahr von QR-Code Betrugsmaschinen ist nicht zu unterschätzen, zumal sich die Codes in einer breiten Masse etabliert haben.

Da diese Betrugsmaschine zur Manipulation höchst effektiv ist, sollten Nutzer sich den damit verbundenen Risiken bewusst werden. Wo es möglich ist, sollte unbedingt eine Mehrfaktor-Authentifizierung eingestellt werden.

7.3 Das A-B-C beim E-Mailversand

Bereits in unserem Tätigkeitsbericht für das Jahr 2022 haben wir unter Punkt 3.1 auf den Umgang mit E-Mail-Adressen in Verbindung mit dem Versenden von Nachrichten hingewiesen. Trotzdem gab es im aktuellen Berichtsjahr zahlreiche Datenpannen im Zusammenhang mit dem Versenden von Nachrichten an mehrere Empfänger u.a. in Form offener E-Mail-Verteiler. Damit gemeint ist, dass alle Empfänger der Nachricht alle weiteren Empfänger (E-Mail-Adressen) sehen können. Entweder stehen in so einem Fall die E-Mail-Adressen (Empfänger) im „AN“ Feld (an @Empfänger...) oder im „CC“ Feld (zusätzlich an @Copy-Empfänger...). Die Einträge in diesen beiden Feldern werden im Klartext an alle dort enthaltenen E-Mail-Empfänger übermittelt.

Ich habe Post und jetzt auch die Adressen: Je nachdem um was für einen Inhalt es sich handelt, den damit alle Empfänger erhalten, kann sich daraus eine meldepflichtige Datenpanne ergeben. Folgendes ist zu beachten:

- Persönliche E-Mail-Adressen sind personenbezogene Daten (außer typische E-Mail-Adressen von Funktions-/Bereichspostfächern, wie z.B. „info@“, „personal@“, „rechnung@“, „einkauf@“ etc...).
- Der Inhalt einer Nachricht könnte Informationen enthalten, die nicht für jeden Empfänger bestimmt sind. Die Informationen müssen daher nicht unbedingt datenschutzrelevant sein. Eine Bekanntgabe könnte u.U. auch gegen andere betriebliche oder gesetzliche Vorschriften verstoßen.

Im Verlauf einer weiteren Bearbeitung der uns gemeldeten Datenpannen und Beschwerden zeigten sich folgende häufige Ursachen auf:



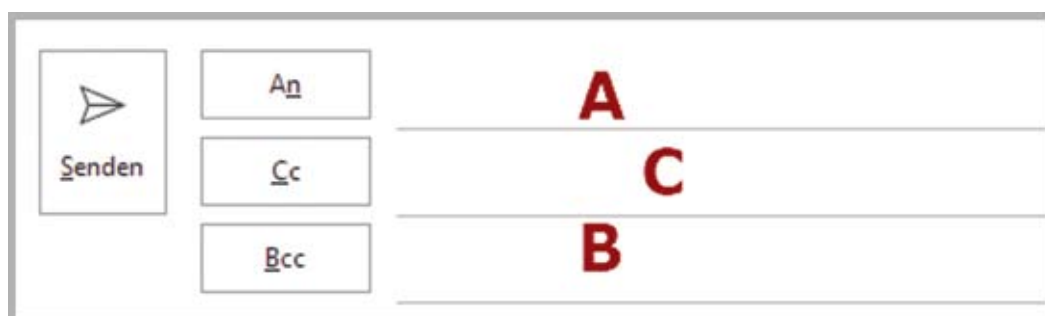
- Eine interne Richtlinie für die betriebliche E-Mail-Kommunikation war nicht vorhanden oder ist nicht bekannt. Hier spielt nicht nur der Datenschutz eine Rolle, sondern wie zuvor genannt auch betriebliche Richtlinien/Vorgaben.
- Das E-Mail-Programm zeigte nur die Eingabefelder „AN“ und „CC“ an. Das „BCC“-Feld war nicht aktiviert.
- Die E-Mail wurde versehentlich an Unbeteiligte oder offenen Verteiler versendet.

Merke:

- CC (Carbon Copy): Wenn ein Empfänger in „CC“ gesetzt wird, erhält diese Person eine Kopie der E-Mail. Alle anderen Empfänger können sehen, wer in „CC“ gesetzt wurde.
- BCC (Blind Carbon Copy): Wenn ein Empfänger in „BCC“ gesetzt wird, erhält diese Person ebenfalls eine Kopie der E-Mail, aber die anderen Empfänger können nicht sehen, dass diese Person eine Kopie erhalten hat. Es ist damit u.a. eine diskretere Art Empfänger einzubeziehen, ohne dass die anderen Empfänger etwas davon wissen.

7.3.1 Das A-B-C mit Outlook

Die meisten werden es bereits kennen, Microsoft Outlook (Outlook), welches sich im betrieblichen Umfeld als ein gängiges E-Mail-Programm etabliert hat. Microsoft Outlook findet man in der Praxis in den verschiedensten Versionen vor. Outlook bietet für den Anwender unzählige Konfigurationsmöglichkeiten, die kaum zu überblicken sind. Das geht von allgemeinen Programmeinstellungen bis hin zu speziellen Applikationen für E-Mail, Kalender, Kontakte, Sprache u.v.m. Zusätzlich gibt es Einstellmög-





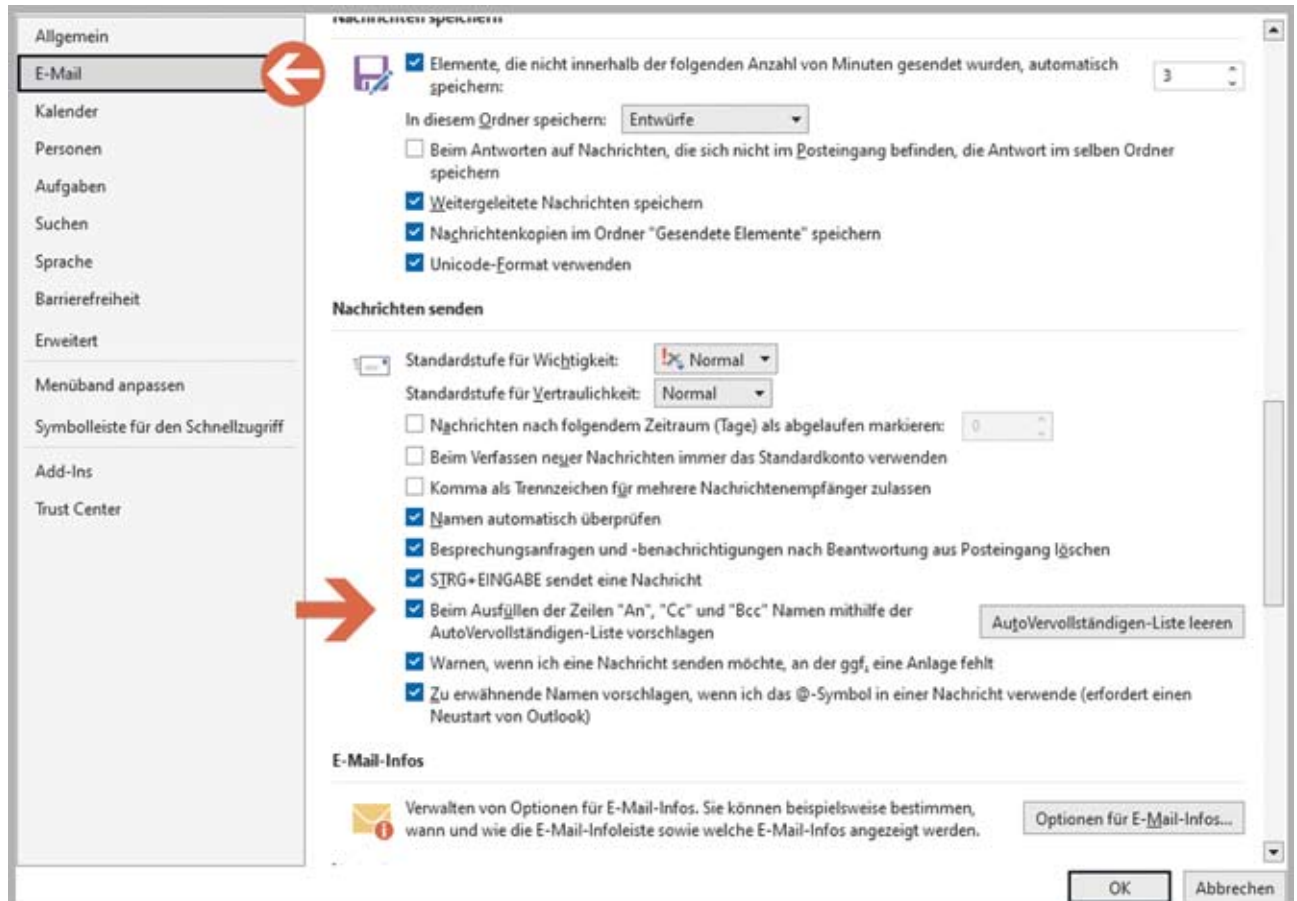
lichkeiten beim Verfassen einer Nachricht (Neue E-Mail), die dementsprechend nur in diesem Kontext gelten.

Im weiteren Verlauf bezieht sich die Beschreibung auf eine Microsoft Outlook Offline Version und die Option „Bcc“ für den E-Mailversand, die in der Regel standardmäßig nicht angezeigt wird. **Grundlegenden Programm-einstellungen findet man im Menü unter „Datei“ und „Optionen“.**

Zuvor noch zwei Tipps für die Outlook-Optionen (Einstellungen), durch die u.a. unbeabsichtigte Datenpannen vermieden werden können.

Das könnte eine Falle werden – z.B. bei Namensgleichheit!

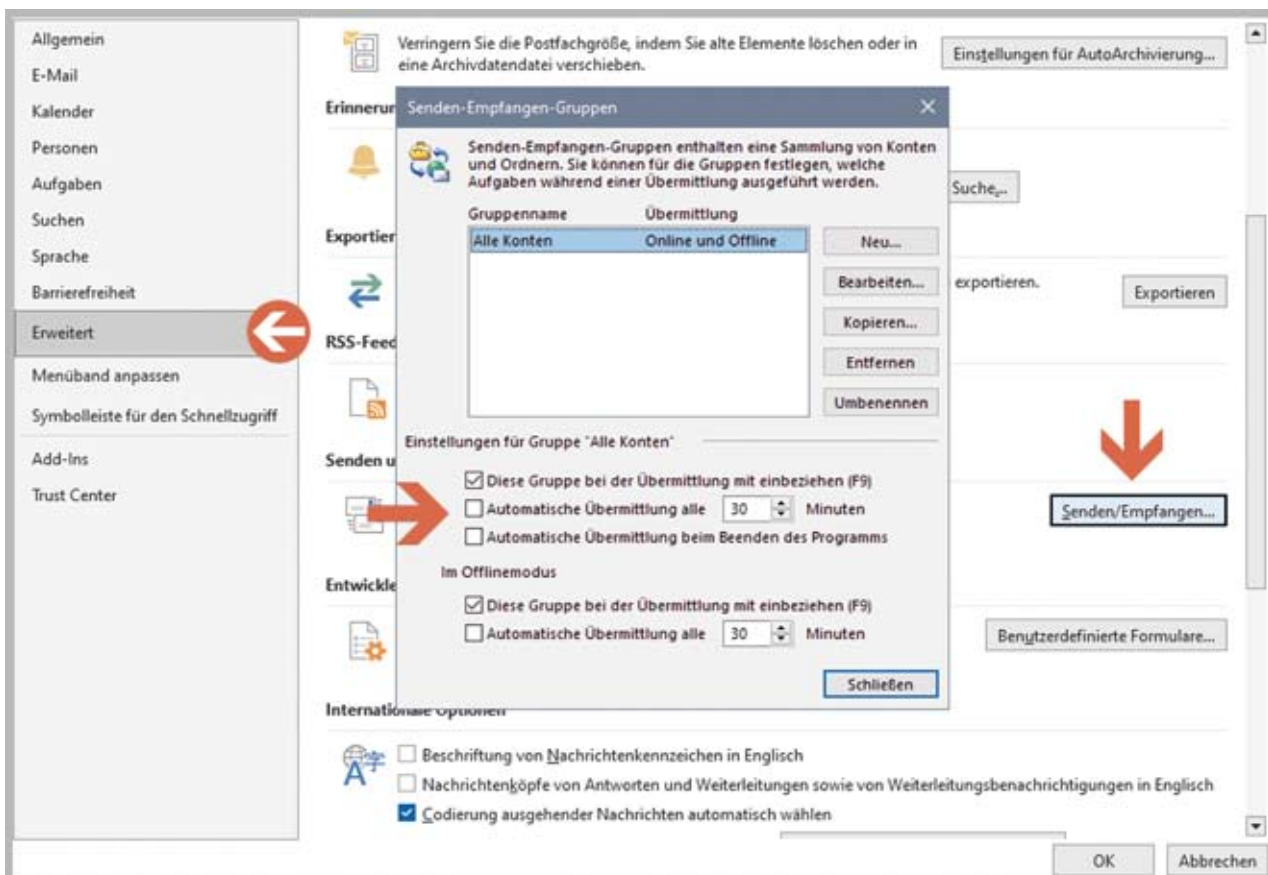
In der Praxis kommt es schon mal vor, dass beim Versuch einen Empfänger einzugeben, Vorschläge erscheinen. Diese Vorschläge hat sich das Programm im Laufe einer E-Mail-Kommunikation in Form einer Historie gemerkt. Sobald ein Empfänger eingetippt wird, erscheint ein Empfänger (durch Autovervollständigung), der so anfängt, wie der, der gerade eingetippt wurde.



Bei ähnlichen Namen kann es passieren, dass Nachrichten ausversehen an einen falschen Empfänger gesendet werden. Falls eine automatische Vervollständigung von Empfängern nicht gewünscht ist, kann sie hier deaktiviert werden. Optional kann die Historie (Liste) bei Bedarf hier geleert werden.

E-Mail-Programme sind in der Regel so eingerichtet, dass nach dem Betätigen der Sende-Taste die Nachricht sofort versendet wird (typischer Weise unwiederbringlich).

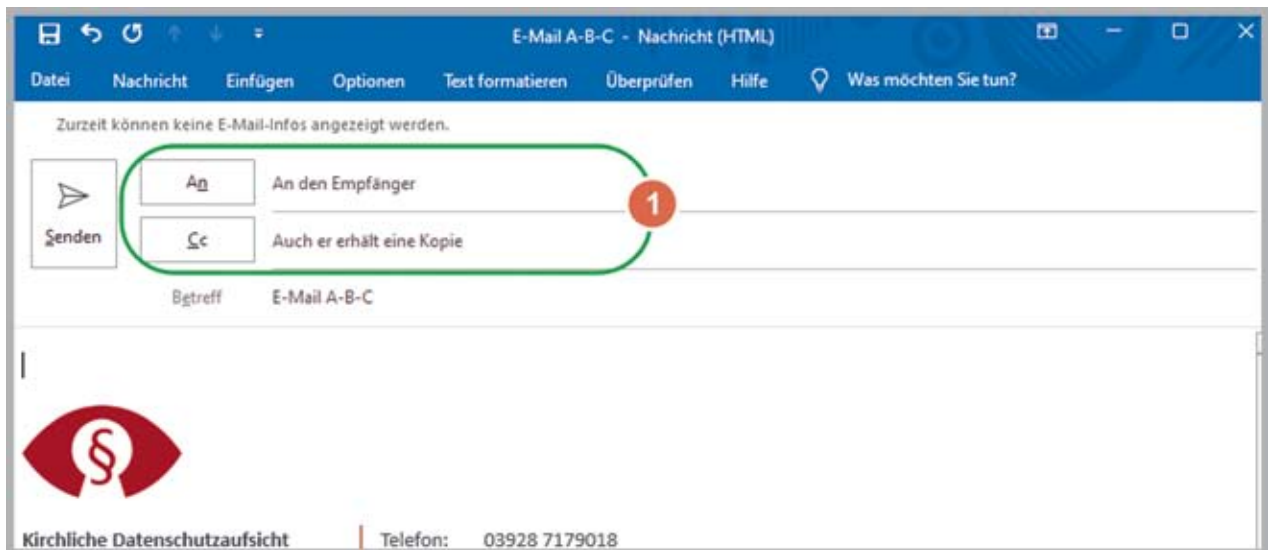
In den Outlook-Optionen unter „Erweitert“ lässt sich der Ablauf anpassen, z. B. wenn nicht sofort versendet werden soll. In der Abbildung ist die Einstellung so gewählt, dass erst durch eine manuelle Aktion (per F9-Taste) Nachrichten versendet werden.



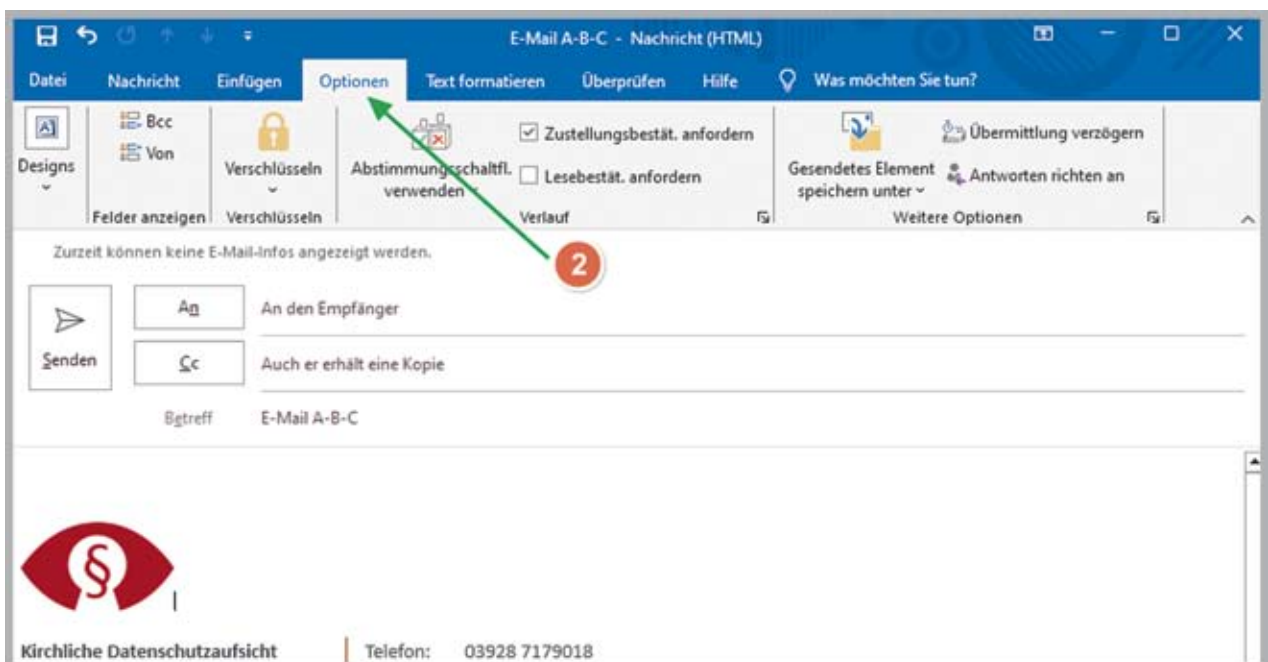


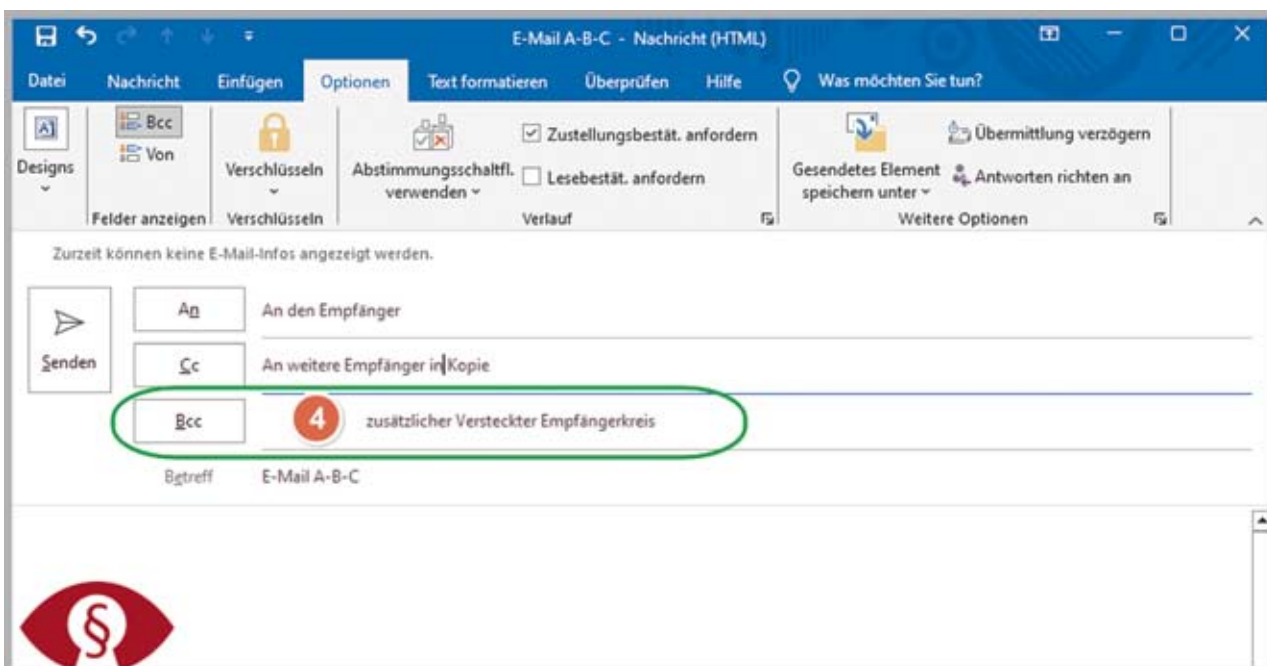
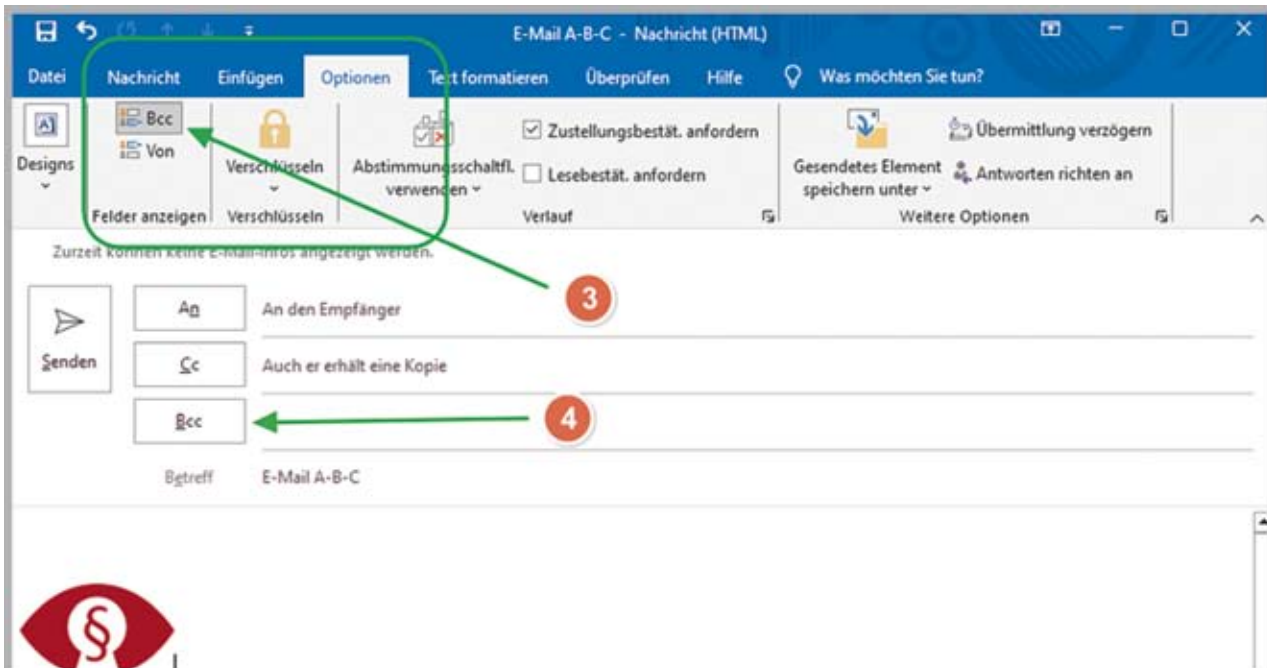
Einrichtung der „A-B-C“ Felder

Die Einstellungen sind im Menü einer Nachricht zu finden. Dafür wird eine neue Nachricht erstellt (entweder „Neue E-Mail“ oder „Strg+N“), wodurch sich ein weiteres **Fenster (1)** öffnet. In diesem Fenster und dem Menü unter dem Punkt **„Optionen“ (2)** sind die gewünschten Einstellungen zu fin-



den, womit zusätzliche Felder für Empfänger oder Absender (Von) aktiviert oder deaktiviert (3) (4) werden können.

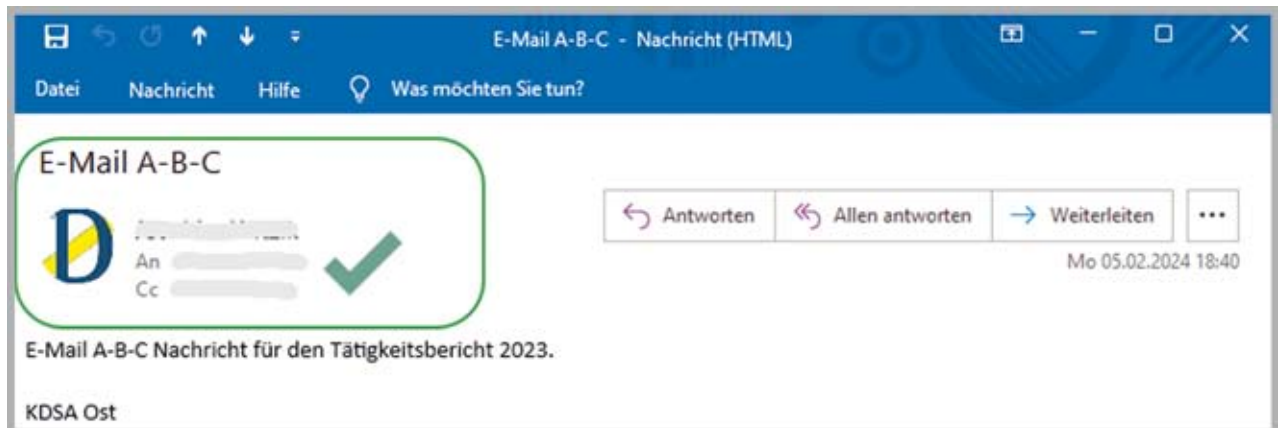




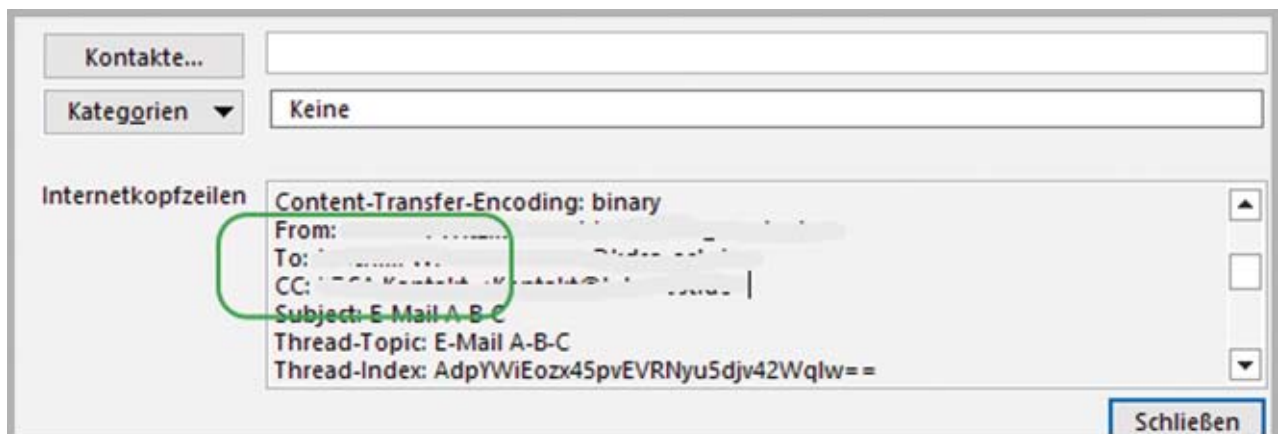
7.3.2 Wie sieht es bei den Empfängern aus?

Nun kann die Einstellung getestet werden, indem eine Testnachricht an unterschiedliche Adressaten in den Feldern „An-Bcc-Cc“ verschickt wird.

Die Empfänger können nur Empfänger in den Feldern „An“ und „Cc“ sehen und nicht zusätzliche „geheime“ Empfänger, die im Feld „Bcc“ eingetragen wurden.



Ein Blick in die E-Mail-Kopfdaten (auch Metadaten genannt) zeigt, dass hier die zusätzlich (geheimen) Empfänger auch nicht vorhanden (nicht sichtbar) sind.

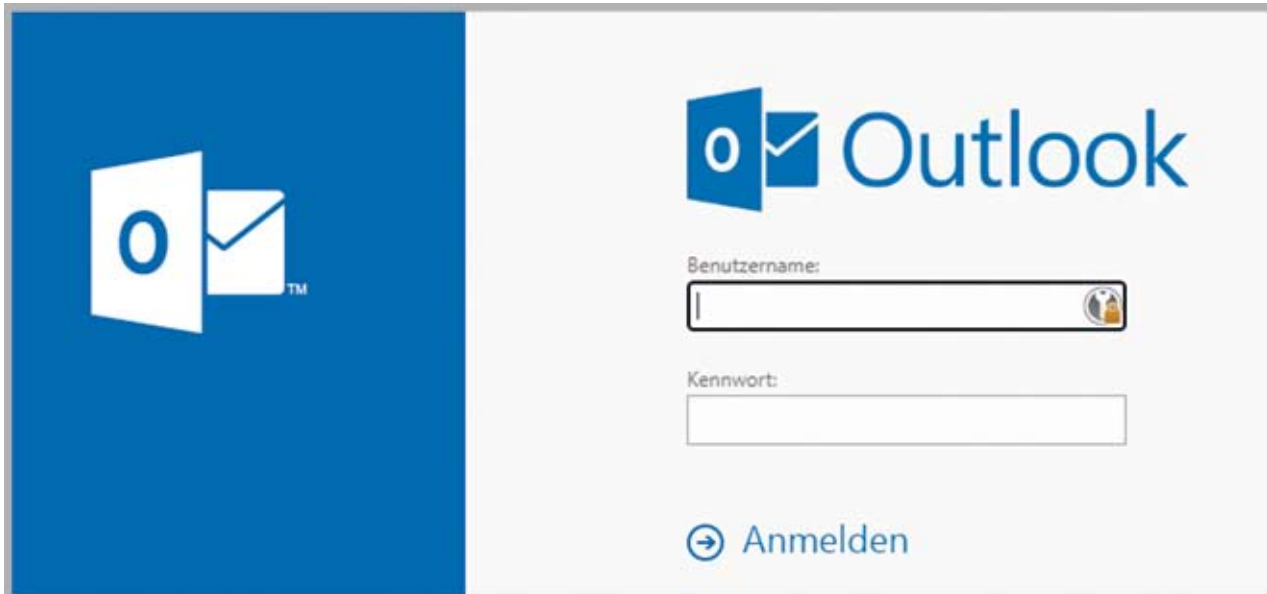


7.4 Phishing/Cyber-Attacke – Ausbreitung gestoppt

Anfang Dezember wurde uns eine E-Mail mit dem Hinweis zugestellt, in unserem Postfach finden wir die bereits angeforderte Rechnung als PDF. Schnell war klar, dass es sich hierbei um eine Phishing-Mail handelte. In der Nachricht selbst war weder ein Schadcode enthalten noch wurde ein Schadcode durch den enthaltenen Link nachgeladen. Die E-Mail war also „sauber“. Beim Betätigen des Links zur angeblichen Rechnung wurde auf eine Outlook-Web-Access Website (Exchange OWA) geleitet.

Wir haben auf unserer Website im Artikel „Phishing – (k)eine schöne Bescherung“ berichtet⁴².

⁴² <https://www.kdsa-ost.de/aktuelles/phishing-k-eine-schoene-bescherung.html>



Was als nicht unbedingt typisch bei so einer Nachricht erschien, war der Absender. Dieser stammte aus vertrauenswürdiger Quelle – was sich u.a. auch in den Kopfdaten der Nachricht zeigte. Zeitnah wurde versucht, den Absender zu kontaktieren, was sich zu diesem Zeitpunkt als erfolglos erwies. Später konnte uns der Absender bestätigen, dass sein Postfach kompromittiert war, womit die Phishing-Mails versendet worden sind.

Durch die interessante Gestaltung und die Verwendung der Exchange OWA-Website wurde die E-Mail in unserem Cyberlabor analysiert und netzforensisch untersucht.

Erschreckendes Ergebnis:

Durch die Analyse der extra dafür verwendeten OWA-Website konnte die Funktion und damit auch der Verkehrsweg nachvollzogen werden. Die Phishing-Kampagne zielte überwiegend auf den deutschsprachigen Raum ab. Ziel der Kriminellen ist die Abfischung von E-Mail-Account-Daten, was bei vielen Einrichtungen u.a. auch Benutzer-Account-Daten in der betrieblichen Infrastruktur sein können.

Der analysierte Verkehrsweg der Daten führte (natürlicher Weise) ins Ausland. Und zwar nicht auf ein System der Kriminellen, was zu einfach wäre, sondern auf ein System einer vertrauten Einrichtung/Institution, welches von den Kriminellen benutzt wurde. Wahrscheinlich handelt es sich um ein gehacktes System, das für solche Zwecke verwendet wird.



Im Rahmen weiterer Analysen konnten wir auf einige „abgefischte“ Daten sehen.

Daraufhin wurde das Landeskriminalamt (LKA) informiert und Strafanzeige gestellt. Das LKA informierte die Absender der Phishing-Mails aus Deutschland.

KDSA informiert Betroffene – allerdings schwierig

Ist so eine Maschinerie erst einmal angelaufen, so ist sie kaum noch zu stoppen, zumal sich die Verkehrswege der Daten nicht im europäischen Raum befinden.

Betroffene, die wir ermitteln konnten, haben wir versucht zeitnah zu informieren, was sich jedoch als nicht so einfach erwies. In diesem Fall ist es ziemlich ungeschickt, den Betroffenen über sein abgefishetes E-Mail-Postfach zu informieren. Demzufolge war für eine zeitnahe Information das Telefon das Mittel der Wahl.

Fast alle Anrufe wurde sofort abgewimmelt. Da brachte auch der Hinweis nicht viel, dass wir die letzten Zeichen des Kennworts nennen können. Wahrscheinlich waren die Personen am Telefon von Enkeltrick-Maschen sensibilisiert.

Nicht aufgegeben

Die Maschinerie hielt und hält nicht an - immer weitere Einrichtungen, Betriebe, Institutionen, Labore etc. (laut Internetdomain) fielen der Phishing-Attacke zum Opfer u.a. auch kirchliche Einrichtungen.

Daraufhin wurden Ansprechpartner anhand der Internetdomain ermittelt und diese per E-Mail informiert. Zusätzlich wurde eine Notfallrufnummer für weitere Informationen bekannt gegeben.

Betroffene E-Mail-Adressen kamen u.a. aus den folgenden Bereichen:

- Kindertagesstätte
- Caritas
- Forschungsinstitute
- Institut in Österreich





- Stadtverwaltung (zur Erinnerung, der Fall aus dem Landkreis Anhalt Bitterfeld)
- Ingenieurbüros

Schadensbegrenzung

Ganz stoppen lässt sich so eine Maschinerie wahrscheinlich nicht, aber durch das schnelle Handeln haben wir ein Teil dazu beigetragen, die Ausbreitung zumindest einzuschränken.

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.



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

Organisation/Dienststelle der KDSA Ost



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, dass 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 gemeinsame 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.

Video-Sprechstunde



Veranstaltungen



Auszug aus unseren Veranstaltungen 2023

Datenschutz – Quo vadis 5 Jahre KDG

Anlässlich des 5. Jahrestages lädt die KDSA Ost zum Dialog/Erfahrungsaustausch



DSGVO und KDG feiern ihren fünften Geburtstag

Ein Beschäftigtendatenschutzgesetz gibt es noch immer nicht, obwohl die ersten Gesetzesinitiativen dazu bereits vor über 30 Jahren beraten worden sind.



TOMtalk?! Hackerangriff, Datenverlust - wie vorbereitet?

Ransomware vs. Daten weg! Wir laden ein zum Dialog/Informations-Austausch - wie sind wir auf so ein Ereignis vorbereitet, gibt es organisatorische Abläufe/Maßnahmen oder ist man bereits betroffen?

Websites mit Fonts & Co im Selbsttest

Veranstaltung zu Websites mit Fonts und Co – eine praxisbezogene Online-Veranstaltung für Website Betreiber, Datenschutzbeauftragte, Interessenten und „Nicht-Techniker“ (keine besonderen Vorkenntnisse erforderlich).

Datenschutz im Pfarrbüro und Spenderdaten

Dialog/Informations-Austausch zu Fragen rund um das Thema Datenschutz im Pfarrbüro stellen.

Heute schon ein Foto gemacht?

Eigene Fotos verbreiten - dafür ist jeder selbst verantwortlich. Doch wie sieht es mit Bildern/Videos aus, die andere über jemanden verbreiten, in der Regel sogar an einen gänzlich unbekanntem Personenkreis.

Unsere regelmäßigen und sehr in Anspruch genommene Videosprechstunden

Nachgefragt?!

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



Anhang

Muster Verarbeitungsverzeichnis Aufnahmevertrag

Muster Verarbeitungsverzeichnis Aufnahmevertrag

Angaben nach § 31 Abs. 1 KDG	
Angaben zum Verantwortlichen	
Name	Kita St. XY
Kontakt	Name (Kita Leitung)
Adresse	Kirchstraße 1, 12345 Kinderhausen
Telefon	01234-56789
E-Mail:	E-Mail@IhreDomain
Angaben zum Datenschutzbeauftragten	
Name	Name oder Firma (Dienstleister)
Adresse	Datenstraße 1, 12349 Sicherheitshausen
Telefon	01239-56789
E-Mail	E-Mail@Dienstleister
Verarbeitungstätigkeit: Aufnahmevertrag	
Verantwortliche Abteilung / Ansprechpartner	Leitungsperson
Zweck der Verarbeitung	Erfassung der Kinderdaten zur Erfüllung der gesetzlichen Pflichten; Erfassung der Kinderdaten zur ordnungsgemäßen Durchführung des Betreuungsvertrages
ggf. Nennung der Rechtsgrundlage (Rechtmäßigkeit nach § 6 Abs. 1 KDG)	Betreuungsvertrag
Beschreibung betroffene Person bzw. Personengruppe	betreutes Kind; Erziehungsberechtigte
Beschreibung personenbezogene Daten bzw. Datenkategorien	Name, Vorname, Anschrift, Telefonnummer, E-Mail-Adresse, ggf. Staatsangehörigkeit, ggf. Konfession, Sorgerecht, ggf. Geschwisterkinder und Betreuungszeit, Gesundheitsdaten (z.B. Impfstatus), Bankverbindung etc.
ggf. die Verwendung von Profiling	wird nicht angewendet
Empfänger, gegenüber die Daten offengelegt werden	Leitung der Einrichtung; ggf. Träger oder Kommune
Datenübermittlung an ein Drittland	nein
Frist für die Löschung:	6 Jahre nach Ende der Betreuungszeit
Datum der Erstellung	01.06.20xy
Datum der letzten Änderung	30.11.20xy
Name und Unterschrift	



Microsoft Versionsinformationen

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

Microsoft Windows 10

Version	Startdatum	Enddatum
Version 22H2	18. Okt. 2022	14. Okt. 2025
Version 21H2	16. Nov. 2021	11. Juni 2024
Version 21H1	18. Mai 2021	13. Dez. 2022

Microsoft Windows 11

Version	Startdatum	Enddatum
Version 23H2	31. Okt. 2023	10. Nov. 2026
Version 22H2	20. Sept. 2022	14. Okt. 2025
Version 21H2	04. Okt. 2021	08. Okt. 2024

Exchange Server

Edition/Produkt	Startdatum	MSS-Ende	EOL
Exchange Server 2019	22.10.2018	09.01.2024	14.10.2025
Exchange Server 2016	01.10.2015	13.10.2020	14.10.2025
Exchange Server 2013	09.01.2013	10.04.2018	11.04.2023

Quelle: Microsoft



Abkürzungen

AEUV	Vertrags über die Arbeitsweise der Europäischen Union
ADV-Vertrag	Auftragsverarbeitungsvertrag
AG	Amtsgericht
ArbG	Arbeitsgericht
ArbZG	Arbeitszeitgesetz
AU	Arbeitsunfähigkeit
AVR	Richtlinien für Arbeitsverträge in den Einrichtungen des Deutschen Caritasverbandes
BAG	Bundesarbeitsgericht
BetrVG	Betriebsverfassungsgesetz
BDSG	Bundesdatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Bundesbeauftragte für Datenschutz und Informationssicherheit
BGB	Bürgerliches Gesetzbuch
BT.-Drs	Bundestag-Drucksache
BVerfG	Bundesverfassungsgericht
BZRG	Bundeszentralregistergesetz
Can.	Codex Jurix Canonici
CIC	Codex Iuris Canonici (lateinisch für Kodex des kanonischen Rechtes)
DDSB	Diözesandatenschutzbeauftragten
DiGA	Digitale Gesundheitsanwendung
DSK	Datenschutzkonferenz
DSK-DBK	Datenschutzgericht der Deutschen Bischofskonferenz
DS-GVO	Datenschutz-Grundverordnung
DVO	Kirchliche Dienstvertragsordnung
ePA	elektronische Patientenakte
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof



FDZ	Forschungsdatenzentrum
GG	Grundgesetz
GrCH	Grundrechtecharta
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HTML	Hypertext Markup Language (Auszeichnungssprache für Webseiten)
http	Hypertext Transfer Protokoll (unverschlüsselt)
https	Hypertext Transfer Protokoll Secure (verschlüsselt)
HK-SozDatenschutzR	Handkommentar Sozialdatenschutzrecht
IDSG	Interdiözesane Datenschutzgericht
IfSG	Infektionsschutzgesetz
KI	Künstliche Intelligenz
LAG	Landesarbeitsgericht
LG	Landgericht
KDG	Kirchliches Datenschutzgesetz
KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz
KUG	Kunsturhebergesetz
MAV	Mitarbeitervertretung
NJW	Neue Juristische Wochenzeitung
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PsychKG	Psychisch-Kranken-Gesetze
RiLi	Richtlinie
SEU	Schuleingangsuntersuchungen
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
VDD	Verbandes der Diözesen Deutschlands
VG	Verwaltungsgericht
VVT	Verzeichnis von Verarbeitungstätigkeiten
VwVfG	Verwaltungsverfahrensgesetz





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