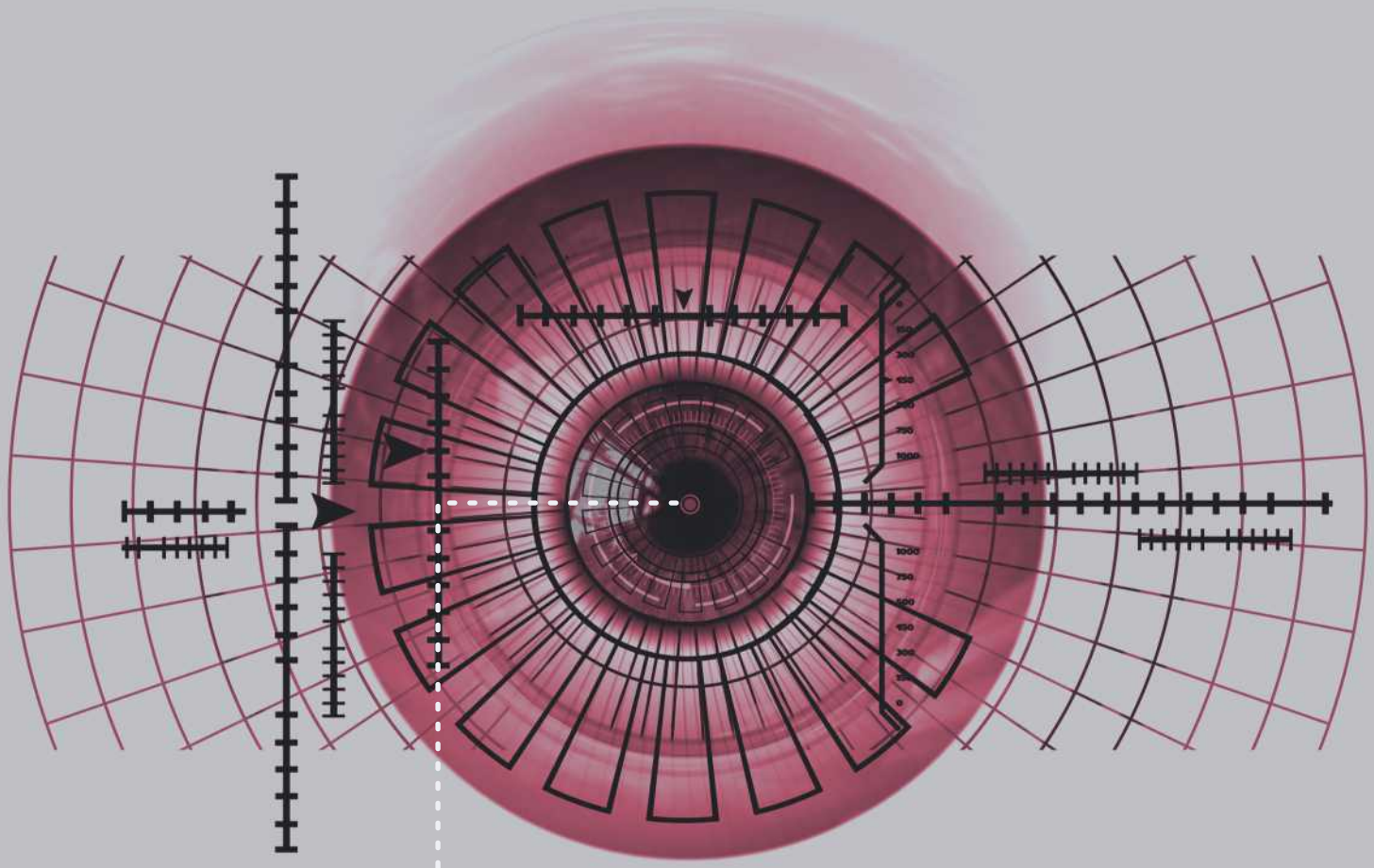


Tätigkeitsbericht 2025

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

Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, der wird am Ende beides verlieren.

Benjamin Franklin

10. Tätigkeitsbericht des Diözesandatenschutzbeauftragten

für

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

Berichtszeitraum 01.01.2025 bis 31.12.2025

Inhaltsverzeichnis

Inhaltsverzeichnis

Zehn Jahre KDSA-Ost 5

Erosion des Datenschutzes 8

1. Entwicklung des Datenschutzes 11

1.1 Entwicklung des Datenschutzes in Europa 11

1.1.1 EuGH: Auskunftsersuchen nach der DS-GVO – Schadensersatzanspruch 11

1.1.2 EuGH stärkt Datenschutz: Pseudonymisierung allein reicht nicht immer 13

1.1.3 Automatisierte Entscheidungsfindung - Algorithmus muss nachvollziehbar sein 15

1.1.4 Höflichkeitsfloskeln und Datenschutz 15

1.2 Entwicklung des Datenschutzes in Deutschland 16

1.2.1 Einsichtsrecht statt Kopie: LAG München konkretisiert Auskunftsanspruch bei Compliance-Untersuchungen 16

1.2.2 Datenschutzverletzung im Bewerbungsverfahren – abgelehnter Jurist fordert Schadensersatz 18

1.2.3 Wann sind E-Mails Ende-zu-Ende zu verschlüsseln? 21

2. Datenschutz allgemein 23

2.1 Grundlegendes zum Auskunftsersuchen 23

2.2 Zulässigkeit von Videoüberwachung in Kirchlichen Einrichtungen 27

2.3 Verpflichtungserklärung zum Datengeheimnis – oft zu kurz und nicht vollumfänglich 31

2.4 Veröffentlichen von Informationen auf Instagram 34

2.5 Benennung der zuständigen Aufsicht in den Datenschutzinformationen 37

2.6 Nachweis des E-Mail-Empfangs 38

2.7 Keine Kopien von Personalausweisen zulassen! 40

2.8 Klimaschutz durch Datenschutz: Datensparsamkeit als Beitrag zur Energiewende 41

3 Datenschutzaufsicht 44

3.1 Prüfaktionen 44

3.1.1 Datenschutzüberprüfung – Schule 44

3.1.2 Datenschutzüberprüfung von Mitarbeitervertretungen 46

3.2 Datenschutzvorfälle – Auskunftsersuchen 51

3.2.1 Wann ist ein Auskunftsanspruch erfüllt? 51
3.2.2 Auskunftsersuchen ignoriert – Bußgeld kassiert I 53
3.3 Datenschutzvorfälle - Videoüberwachung 54
3.3.1 Videoüberwachung von Bereichen in Krankenhäusern 54
3.3.2 Videoüberwachung im Eingangsbereich einer Einrichtung und des davor befindlichen Straßenraumes 57
3.3.3 Videoüberwachung im Jugendraum 59
3.4 Datenschutzvorfälle - Offene E- Mailverteiler 60
4 Datenschutz im Gesundheitswesen 61
4.1 Neuregelung zum Datenschutz im Krankenhausgesetzes Berlin 61
4.2 Datenschutzvorfälle im Gesundheitswesen 63
4.2.1 Klassischer Fall: Verlust physischer Dokumente 63
4.2.2 Falsch versandte Patientenunterlagen 64
4.2.3 Auskunftsersuchen ignoriert – Bußgeld kassiert II 65
4.2.4 Cyberangriffe und Ransomware 66
4.2.5 Neugierige Mitarbeiter 67
4.2.6 Kostenvoranschlag per E-Mail 69
5 Datenschutz in Kita und Schule 70
5.1 Fotos im Kindergarten– Risiken minimieren – TOMs etablieren 70
5.2 Datenschutzvorfälle 72
5.2.1 Einbruchdiebstahl in Kita mit gravierenden Folgen 72
5.2.2 Schusselige Lehrer oder wie können analoge Unterlagen besser transportiert werden? 74
6 Datenschutz im Beschäftigungsverhältnis 76
6.1 Zum Auskunftsersuchen 76
6.1.1 Kann ein Arbeitnehmer auf einen Auskunftsanspruch verzichten? 76
6.1.2 Wo haben Sie sich beworben? - Annahmeverzugslohn und Auskunftspflicht des Arbeitnehmers 78
6.2 Krankenstand / Arbeitsunfähigkeit 81
6.2.1 Zwischen Datenschutz und Informationspflicht - Krankmeldungen mit der eAU 81
6.2.2 Umgang mit Gesundheitsdaten – Entgeltfortzahlung 83
6.2.3 Mitteilung über den Krankenstand kann teuer werden 85
6.3 Dürfen Regelungen einer Betriebs- oder Dienstvereinbarung das Schutzniveau des Datenschutzes unterschreiten? 86

6.4 Elektronische Entgeltabrechnungen: BAG erlaubt rein digitale Bereitstellung 88
6.5 Darf der Arbeitgeber die Freigabe von Outlook-Kalendern verpflichtend anordnen? .. 90
6.6 Weiterleitung dienstlicher E-Mails an private Accounts 92
6.7 Vorlage erweiterter Führungszeugnisse bei Sozialhilfeträgern 94
6.8 Datenschutzvorfälle 96
6.8.1 Falscher Drucker für Personaldaten 96
6.8.2 Vervielfältigen von Personalunterlagen durch die MAV 97
7 Technische Datenschutzprüfungen 99
7.1 IT-Labore für technische Überprüfungen 100
7.2 Technische Überprüfungen – anlasslos 101
7.2.1 Websites 101
7.2.2 E-Mail 102
7.3 E-Mail-Kommunikation 102
7.3.1 Die unsichtbare Spam-Welle – Warum wir plötzlich fremde Autoresponder erhalten? 102
7.3.2 Ein „Bcc“ Missverständnis auf den Punkt gebracht 105
7.4 E-Mail - Serienbrief mit Outlook und Word 108
7.5 E-Mail-Verschlüsselung mit S/MIME nicht ohne Tücken 111
7.5.1 Schwierigkeiten bei der Langzeitarchivierung von E-Mails mit S/MIME 111
7.5.2 Risiken der Zertifikatsverwaltung 112
7.5.3 Technische Herausforderungen 113
Die Kirchliche Datenschutzaufsicht Ost 115
KDSA Ost als Dienststelle 115
Organigramm 115
Unsere Aufgaben und Befugnisse 115
Öffentlichkeitsarbeit 116
Auszug aus unseren Veranstaltungen 2025 117
Anhang 119
Auskunftsersuchen gem. § 17 KDG / Art. 15 DS-GVO Handlungsleitfaden 119
Prozessregelung für das Erstellen und Verarbeiten von Fotos 121
Supportende von Windows 10 und weiteren Microsoft Produkten 122
Abkürzungen 124

Zehn Jahre KDSA-Ost

Die kirchliche Datenschutzaufsicht der ostdeutschen Bistümer wurde zum 01.01.2016 durch den Erzbischof von Berlin und die Bischöfe der Diözesen Erfurt, Dresden-Meißen, Görlitz und Magdeburg errichtet.

Damit wurde auch ein neues Kapitel im kirchlichen Datenschutz aufgeschlagen.

Den Grundstein für die Einführung selbständiger Datenschutzaufsichtsbehörden legte der Europäische Gerichtshof (EuGH).

Im Jahr 2010 entschied dieses Gericht in einem Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland, dass die Datenschutzaufsicht „jeglicher äußeren Einflussnahme entzogen sein" müsse, „die ihre Entscheidungen steuern könnte". Damit hat der EuGH 2010 klargestellt, dass jedes Risiko einer Einflussnahme auf die objektive und unabhängige Entscheidung der Datenschutzaufsichtsbehörden vermieden werden muss.

Die nord- und ostdeutschen Bistümer hatten das Urteil umgesetzt, indem sie einen Diözesandatenschutzbeauftragten eingesetzt hatten, der in Hannover residierte und für den Bereich von Göttingen bis Flensburg und von der holländischen bis zur polnischen Grenze zuständig war. Die Zuteilung eines solchen Gebietes an einen einzelnen Mitarbeiter ließ erkennen, wie man sich seinerzeit eine Datenschutzaufsicht vorstellte. Der Kollege tat, was er tun konnte. Er verfasste umfangreiche Arbeitshilfen und Stellungnahmen zu datenschutzrechtlichen Themen und er wachte. Er wachte wie § 17 Abs. 1 S. 1 der Kirchlichen Datenschutzordnung (KDO) es vorsah, über die Einhaltung der Vorschriften über den Datenschutz. In diesem Zusammenhang bezeichnete er sich selber einmal als „Kettenhund". Er wacht und wenn etwas passiert wird er aktiv.

Mit in Kraft treten der Datenschutzgrundverordnung im Jahr 2016 war klar, dass diese Verfahrensweise den neuen Anforderungen des Datenschutzes nicht mehr genügt.

Auf dem angesprochenen Gebiet entstanden zwei Kirchliche Datenschutzaufsichten, die KDSA Nord und die KDSA Ost, von denen in jeder vier Mitarbeitende beschäftigt sind. Die Zuständigkeit der KDSA Ost erstreckt sich seitdem über das Gebiet der fünf Ostdeutschen Bundesländer mit Ausnahme des mecklenburgischen Teils von Mecklenburg-Vorpommern.

Die Schaffung unabhängiger Aufsichten, die dem Weisungsrecht kirchlicher Autoritäten entzogen sind, war Neuland für die Kirchen. Umso mehr

trifft das zu, nachdem nach in Kraft treten des Kirchlichen Datenschutzgesetzes (KDG) die Aufsichten berechtigt sind, selbst einem Bischof Weisungen zu erteilen, gegen die er sich nur auf gerichtlichem Wege wehren kann.

Das spricht für ein großes Vertrauen gegenüber den Aufsichten und insbesondere gegenüber deren LeiterInnen.

Tatsächlich ist es in den zehn Jahren des Bestehens dieser Behörde noch nicht einmal passiert, dass von Seiten eines Bischofs, Generalvikars oder anderen Verantwortlichen versucht worden ist, die Unabhängigkeit der Aufsichten infrage zu stellen oder Einfluss auf unsere Tätigkeit auszuüben.

Mit den Kolleginnen und Kollegen der staatlichen Aufsichten, also den Landesdatenschutzbeauftragten, gibt es regelmäßige Erfahrungsaustausche. Bei den ersten Treffen wurde uns mit großer Skepsis begegnet.

Teilweise schien es eine Verärgerung darüber zu geben, dass den Kirchen die Möglichkeit eingeräumt wurde, ihre Aufgaben selber zu regeln. Insbesondere der deutlich geringere Strafrahmen des KDG im Verhältnis zur DSGVO nährte die Befürchtung, die Kirchen beriefen sich auf ihre Eigenständigkeit nur, um einen „Datenschutz light“ zu praktizieren.

Die Kirchen wurden mit Vereinen gleichgesetzt und man traute den kirchlichen Diözesandatenschutzbeauftragten keine wirkliche Unabhängigkeit zu.

Diese Befindlichkeiten sind inzwischen, zumindest im Bereich unserer Aufsicht, einer vertrauensvollen Zusammenarbeit gewichen.

Die Höhe des Bußgeldrahmens, der deutlich unter den staatlichen Grenzen liegt, gibt dennoch immer wieder Anlass zu Diskussionen.

Betrachtet man den Bußgeldrahmen des KDG jedoch als Obergrenze bzw. Kappungsgrenze, bestehen kaum Unterschiede zwischen der Höhe der verhängten Bußgelder. Die Konferenz der katholischen Datenschutzaufsichten hat sich auf diese Betrachtung festgelegt.

Im Bereich von Kirche und Caritas werden selten leistungsfähige Großunternehmen anzutreffen sein, denen gegenüber aufgrund ihrer Leistungsfähigkeit Bußgelder im sechsstelligen Bereich zu rechtfertigen wären. Solche werden auch im staatlichen Bereich nur selten ausgesprochen. Bei vergleichbar großen Einrichtungen, wie Altenheimen und Krankenhäusern, gibt es praktisch keinen Unterschied bei der tatsächlich verhängten Bußgeldhöhe.

Die nunmehr nach der Evaluation des KDG beschlossene Erhöhung des Bußgeldrahmens dürfte daher kaum praktische Auswirkungen haben.

Besonderheiten unserer Aufsichten

§ 3 Abs. 1 KDG bestimmt den organisatorischen Anwendungsbereich des Gesetzes. Unter Hinzuziehung von Schematismus, Caritas Organigrammen oder Verzeichnissen und anderen Übersichten aus dem kirchlichen Bereich kennen wir die Verantwortlichen, für die wir zuständig sind, nahezu abschließend. Das erleichtert uns als Aufsicht die Arbeit, weil wir uns für unsere Angebote von Überprüfung, Beratung und Schulung direkt an die Verantwortlichen wenden können.

Das unterscheidet uns von staatlichen Aufsichten, die keine Möglichkeit haben, die in ihren Zuständigkeitsbereich fallenden Verantwortlichen flächendeckend zu ermitteln. Das gibt uns die Chance proaktiv zu agieren.

So führen wir seit einigen Jahren sogenannte anlasslose Prüfungen bei Verantwortlichen in unserem Zuständigkeitsbereich durch.

Solche Prüfungen erfolgen an zwei Tagen an einem bestimmten Standort. Bei der Auswahl der Einrichtungen wird Wert daraufgelegt, dass sowohl größere Einrichtungen als auch kleinere Einrichtungen nach einem zuvor ausgearbeiteten Prüfungsschema überprüft werden.

Am Abend laden wir zu einer offenen Sprechstunde ein, zu der Haupt- und Ehrenamtliche aber auch alle interessierten Personen eingeladen sind. Im Rahmen dieser Präsenzveranstaltung besteht die Möglichkeit Fragen zum Datenschutz mit der Aufsicht zu diskutieren oder zu klären.

Die Ergebnisse unserer Prüfungen werden mit den Verantwortlichen besprochen und in einem Protokoll festgehalten.

Ziel dieser Aktionen ist es in den jeweiligen Einrichtungen eine Sensibilisierung zum Thema Datenschutz zu erreichen.

Fehler oder Defizite werden aufgezeigt und Lösungen besprochen. Die Datenschutzaufsicht soll so als Unterstützer in datenschutzrechtlichen Fragen wahrgenommen werden. Dies gilt sowohl für den Verantwortlichen, als auch für deren Datenschutzbeauftragte.

Weiterhin sollen durch den persönlichen Kontakt Hemmschwellen zur Aufsicht abgebaut werden. Dadurch soll Verantwortlichen und Datenschutzbeauftragten der „kurze Dienstweg“ zur Aufsicht nahegebracht werden.

Das gleiche Ziel verfolgen wir auch mit unseren Videosprechstunden, die wir regelmäßig anbieten und die allen Interessierten offenstehen.

Die Datenschutzmeldungen, die bei uns eingehen, kommen zu ca. 80% von Verantwortlichen bzw. ihren betrieblichen Datenschutzbeauftragten selber. Eine Quote, die im staatlichen Bereich bei weitem nicht erreicht wird.

Wesentlich zu diesem Ergebnis beigetragen hat sicher auch unser Aufruf „Melden macht frei!"

Wer bei der Bundeswehr gewesen ist, kennt diesen Spruch. Dort hat das Melden dazu geführt, dass man die Verantwortung an den Vorgesetzten übertragen hat.

So ist unser Aufruf nicht zu verstehen. Der Verantwortliche bleibt weiterhin verantwortlich und kann durch eine Meldung nicht die Verantwortung auf die Aufsicht abzuschieben.

Wir sehen uns aber als Aufsicht verpflichtet, diejenigen, die melden dann nicht allein zu lassen. Wir sehen vielmehr durch die Meldung eine gegenseitige Verpflichtung begründet.

Uns wird Vertrauen entgegengebracht, weil man durch die Meldung Hilfe bekommt. Die Freiheit, die man durch die Meldung erlangt, besteht darin, Unterstützung für eine Lösung zu bekommen.

Durch die aufgezeigten Angebote und das dargestellte Selbstverständnis der Aufsicht konnten wir durch unsere Tätigkeit in den letzten zehn Jahren die Wahrnehmung unserer Aufsicht verändern. Wir sehen uns heute nicht mehr als der eingangs erwähnte, vielleicht beißende „Kettenhund", sondern eher als begleitender Assistenzhund, der vor dem Eintritt von Übeln bewahrt.

Auch in den kommenden Jahren wollen wir mit aufsichtlicher Autorität und partnerschaftlicher Unterstützung für einen praxisnahen Datenschutz eintreten, der gleichermaßen die Arbeit der Verantwortlichen, wie die Persönlichkeitsrechte Betroffener berücksichtigt.

Erosion des Datenschutzes

Politisch wird Datenschutz wieder vermehrt als Hindernis für wirtschaftliche Innovation gesehen. So stellt die vom Bundespräsidenten eingesetzte Kommission „Initiative für einen handlungsfähigen Staat" in ihrem Abschlussbericht fest: „Ein überzogener Datenschutz aber ist für viele

inzwischen zum Ärgernis geworden. Die Datenschutzgrundverordnung der EU (DS-GVO) wird in Deutschland strenger angewendet als in anderen EU-Staaten."[1] Einen Beleg für diese Behauptung bleiben die Verfasser im Bericht schuldig.

Auch im Koalitionsvertrag 2025 wird der Datenschutz den Interessen der Wirtschaft angepasst. „Im Interesse der Wirtschaft streben wir eine Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesdatenschutzbeauftragten an. Sie soll dann Bundesbeauftragte für Datennutzung, Datenschutz und Informationsfreiheit sein."[2] Datenschutz wird im Koalitionsvertrag offensichtlich als Hindernis für eine wirtschaftliche Entwicklung betrachtet. Dabei weckt auch die Wortwahl Zweifel an einem effektiven Datenschutz, wenn eine Umbenennung der Bundesbeauftragten für Datenschutz erfolgen soll, indem Datennutzung dem Titel hinzugefügt wird. Die Zentralisierung hätte für die Regierung den Vorteil, dass Datenschutz durch Druck auf eine einzige Stelle beeinflusst werden könnte, während bislang 17 Datenschutzbehörden existieren.

Bei staatlichen Leistungen soll zudem das Einwilligungsprinzip abgeschafft werden. Bürger würden dann, wie bei der Elektronischen Patientenakte, nicht mehr gefragt werden, ob der Staat ihre Daten nutzen darf, sondern müssten einer Nutzung aktiv widersprechen.

Bundeswirtschaftsministerin Katherina Reiche hat nach Medienberichten bei einem Treffen in den USA ihre Unterstützung signalisiert, das Gesetz für digitale Dienste und den Digital Markets Act (DMA) zu relativieren – also ausgerechnet jene Regulierung, die die Marktmacht großer US-Techkonzerne begrenzen soll. Im Gegenzug sollen die USA Zugeständnisse bei angedrohten Stahlzöllen machen.[3] Hier werden die Persönlichkeitsrechte aller Bürger zur Handelsware für die Interessen eines Teils der Industrie und deren Profitinteresse.

Das Narrativ, Datenschutz behindere die Wirtschaft, wird maßgeblich von dieser selbst in den Vordergrund gespielt. Am Beispiel von „Cookies" wird dies offenkundig. Die Anwender sind von Cookie-Bannern genervt. Es ist aber keineswegs für jede Webseite erforderlich, diese Banner zu verwen-

1 https://www.ghst.de/fileadmin/images/01_Bilddatenbank_Website/Demokratie_staerken/Initiative_f%C3%BCr_einen_handlungsf%C3%A4higen_Staat/Abschlussbericht/Abschlussbericht_neu.pdf S. 100 ff
2 Koalitionsvertrag Rn. 2253, 2254
3 https://www.zeit.de/digital/datenschutz/2025-12/datenschutz-ueberwachung-bundesregierung-widerstand-palantir-ccc/seite-2

den. Soweit keine einwilligungsbedürftigen Verarbeitungen vorgenommen werden, ist nach der DS-GVO auch keine Einwilligung nötig.

Hier wird deutlich, dass einige den Datenschutz kritisieren, weil er ihren Gewinninteressen im Wege steht.

Andererseits haben aber Beraterfirmen ein nachhaltiges Interesse daran, bestehende Datenschutzregelungen zu verkomplizieren, um ihre Beratungsleistungen zu verkaufen.

Auch Forderungen aus der Politik nach immer neuen Registern, z. B. für psychisch kranke (Gewalttäter),[4] für Menschen mit geändertem Geschlechtseintrag,[5] lässt eine Erosion des Datenschutzes vermuten. Weil aus einzelnen Gruppen einzelne Straftäter hervorgegangen sind, sollen diese Gruppen insgesamt unter Generalverdacht gestellt werden.

Die Aufgabe von Freiheit und Persönlichkeitsrechten, um vermeintliche Sicherheit zu gewinnen, gilt auch für das ursprünglich geplante Gesetz zur digitalen Chatkontrolle. Behörden hätten nach diesem Gesetz Anbieter von Kommunikationsdiensten, wie z. B. WhatsApp, zur Überwachung privater Kommunikation verpflichten können. Dabei hätten sogenannte „Aufdeckungsanordnungen" gegen Anbieter von interpersonellen Kommunikationsdiensten verhängt werden können, mit denen sie z.B. von Messenger-Dienste verlangen können, die Kommunikation all ihrer Nutzenden zu überwachen. Dafür reicht aus, dass die Behörde ein erhebliches Risiko festgestellt hat, dass der betroffene Dienst für die Verbreitung sexueller Gewaltdarstellungen genutzt wird. „Sollte jemals eine autokratische Partei wie die AfD die Macht übernehmen oder die parlamentarische Mehrheit, brauchte sie keine Gesetze mehr zu ändern, um derartige Kontrollinstrumente dann konsequent gegen die andere Seite zu verwenden."[6]

Die Kirchen müssen dafür sorgen, dass ihre Mitglieder geschützt werden. Da die AfD die Kirchen zu ihren Gegnern erklärt hat und diejenigen richten will, die über die AfD richten[7], besteht eine konkrete Gefahr der Benachteiligung von Kirchenmitgliedern im Falle einer Regierungsübernahme. Ein sparsamer Umgang mit personenbezogenen Daten ist deshalb nochmal einzufordern (das betrifft u. a. die Veröffentlichung von Bildern oder die Offenlegung von E-Mail-Verteilern).

4 https://www.zdfheute.de/politik/deutschland/linnemann-register-psychisch-kranke-gewalttaeter-cdu-kommentar-100.html
5 https://www.mdr.de/nachrichten/deutschland/politik/trans-personen-meldedaten-verordnung-innenministerium-selbstbestimmungsgesetz-102.html
6 Wolfgang Kubicki, in: https://www.fdp.de/chatkontrolle-ist-frontalangriff-auf-die-buergerrechte
7 Hans-Thomas Tillschneider, MdL, stellvertretender Landesvorsitzender der AfD Sachsen-Anhalt 2017, Rede beim Bundesparteitag der AfD in Hannover 2017

1 Entwicklung des Datenschutzes

1.1 Entwicklung des Datenschutzes in Europa

1.1.1 EuGH: Auskunftsersuchen nach der DS-GVO Schadensersatzanspruch

Die DS-GVO gewährt verschiedene Rechte zum Schutz personenbezogener Daten, wozu auch das Auskunftsrecht nach Art. 15 DS-GVO zählt. Doch was, wenn dieses Recht zum Geschäftsmodell wird, um Schadensersatzansprüche zu provozieren? Aktuell hat darüber das Amtsgericht Arnsberg (AG Arnsberg) zu entscheiden. Das Gericht hat mit Beschluss vom 31.07.2024 dem Europäischen Gerichtshof (EuGH) verschiedene Fragen zur Vorabentscheidung vorgelegt. Zum Verfahren hatten wir bereits in unserem Tätigkeitsbericht 2024 unter Punkt 1.2.2 berichtet.

Im vorliegenden Fall abonnierte der Betroffene online einen Newsletter und forderte im Anschluss Auskunft über die von der Betreiberin verarbeiteten Daten gemäß Art. 15 DS-GVO. Mit der Empfangsbestätigung erklärte diese die Anfrage innerhalb eines Monats beantworten zu wollen. Dem Auskunftsbegehren gab die Betreiberin allerdings nicht statt. Sie vertrat die Auffassung, es handele sich um eine rechtsmissbräuchliche Anfrage, da das Begehren des Betroffenen darauf abziele, Verstöße zu provozieren und darauf basierend Schadensersatzansprüche geltend zu machen. Hierbei handle es sich um ein Geschäftsmodell, was auch zahlreiche Berichte und Blogbeiträge bestätigen würden. Ein solches Verhalten untergrabe den Schutzzwecke der DS-GVO, so die Betreiberin.

Der Betroffene hielt dem entgegen, dass das Auskunftsrecht bedingungsfeindlich sei und etwaige Motive unerheblich seien. Als der Betroffene infolge der Auskunftsverweigerung Schadensersatz i. H. v. 1.000, - € verlangte, erhob die Betreiberin hiergegen Klage.

Inzwischen liegen die Schlussanträge des Generalanwaltes beim EuGH vor.

Der Generalanwalt Maciej Szpunar hat am 18.09.2025 seine Schlussanträge vorgelegt – und setzt klare Grenzen für missbräuchliche Geltendmachung von Betroffenenrechten.

Dieser schlägt vor, Art. 12 Abs. 5 Satz 2 DS-GVO so auszulegen, dass auch ein einmaliger Auskunftsantrag schon als „exzessiv“ und somit rechtsmissbräuchlich eingestuft werden kann, wenn anhand der Umstände des Einzelfalls eine Missbrauchsabsicht nachweisbar sei. Dies sei der Fall, wenn die betreffende Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt habe, gerade um diesen Auskunftsantrag stellen zu können und anschließend Schadensersatz zu verlangen.

Zugleich betont der Generalanwalt: Die bloße Tatsache, dass jemand oft Schadensersatz verlangt, reicht nicht aus – maßgeblich bleibt eine Einzelfallprüfung, u.a. nach Gegenstand des Auskunftsersuchens und zeitlichem Abstand zur Einwilligung.

Insofern könnte dem Kläger möglicherweise zum Verhängnis werden, dass er den Auskunftsantrag nur wenige Tage nach der Newsletterbestellung einreichte.

Die Entscheidung des Gerichtshofs bleibt abzuwarten.

Der Fall steht nicht isoliert:

Das Bundesarbeitsgericht (BAG)[8] hat im Juni 2025 zwei Verfahren zu Auskunft und immateriellem Schaden nach Art. 82 DS-GVO bis zur EuGH-Klärung ausgesetzt. Das unterstreicht die erhebliche Praxisrelevanz – insbesondere die Frage, ob bereits „Kontrollverlust“ oder „Ungewissheit“ über die Datenverarbeitung als Schaden genügt.

Fazit:

Wenn das Gericht der Ansicht des Generalanwaltes folgt, bleibt es für Verantwortliche ein Vabanquespiel in solchen Fällen eine Auskunft wegen Missbräuchlichkeit des Antrages abzulehnen, da die Beweislast für missbräuchliches Vorgehen von Auskunftsersuchenden beim Verantwortlichen liegt.

Verantwortliche müssen entscheiden, ob es für sie einfacher ist die erwünschte Auskunft zu erteilen oder sie unter dem Hinweis auf missbräuchliches Verhalten zu verweigern und sich so einem möglicherweise Jahre dauernden Rechtsstreit auszusetzen.

8 BAG, Beschluss vom 24.06.2025 -8 AZR 308/24 (A); BAG, Beschluss vom 24.06.2025 - 8 AZR 4/25 (A)

1.1.2 EuGH stärkt Datenschutz: Pseudonymisierung allein reicht nicht immer

In einem Urteil vom 04.09.2025 hat der Europäische Gerichtshof (EuGH)[9] klargestellt: Pseudonymisierte Daten gelten auch dann als personenbezogene Daten, wenn sie an Dritte weitergegeben werden.

Für Unternehmen bedeutet dies, dass die Pseudonymisierung sie nicht automatisch von den Informationspflichten oder anderen Anforderungen der DS-GVO befreit.

Worum ging es im Rechtsstreit?

Eine EU-Behörde hatte Stellungnahmen von Betroffenen pseudonymisiert und anschließend an ein Beratungsunternehmen weitergegeben. Die Betroffenen wurden darüber jedoch nicht informiert. Der EU-Datenschutzbeauftragte sah darin einen Verstoß gegen die DS-GVO. Nun bekam er vom EuGH Recht.

Der Europäische Gerichtshof (EuGH) stellte klar, dass maßgeblich die Sicht des ursprünglichen Verantwortlichen sei.

Kernaussage des Urteils

- **Pseudonymisierung bedeutet nicht gleich Anonymisierung**
  Auch wenn Namen oder direkte Identifikatoren entfernt sind, können die Daten noch einen Personenbezug haben.
- **Die Sicht des Datenverantwortlichen ist entscheidend**
  Maßgeblich ist nicht, ob der Empfänger die Daten einer Person zuordnen kann, sondern ob der ursprüngliche Verantwortliche dies könnte.
- **Informationspflicht bleibt bestehen**
  Betroffene müssen über eine geplante Weitergabe ihrer Daten informiert werden. Dies gilt sogar dann, wenn der Empfänger die Daten faktisch nicht mehr einer Person zuordnen kann.

Was bedeutet das in der Praxis?

- **1. Keine „Abkürzungen“ durch Pseudonymisierung**
  Auch pseudonymisierte Daten sind in der Regel personenbezogen und unterliegen den Pflichten der DS-GVO.

9 EuGH, Urteil vom 04.09.2025 -C-413/23 P

- **2. Informationspflichten einhalten**
  Betroffene sind rechtzeitig (also vor einer Weitergabe) zu informieren. Ein Hinweis „die Daten sind ja pseudonymisiert" reicht nicht.
- **3. Dokumentation und Prozesse prüfen**
  Unternehmen sollten sicherstellen, dass sie Informationspflichten klar geregelt haben und dies auch nachweisen können.

Fazit:

Der EuGH hat die Verantwortung für den Schutz personenbezogener Daten eindeutig dem Datenverarbeiter zugerechnet. Unternehmen sind auch bei pseudonymisierten Daten dazu verpflichtet, die Anforderungen der DS-GVO einzuhalten.

Nur wenn sauber dokumentiert, transparent informiert und technische Maßnahmen mit organisatorischen Pflichten kombiniert werden, können rechtliche Risiken gesenkt werden.

Siehe dazu auch unsere Ausführungen im Bericht 2023 zur Entscheidung des EuGH vom 26.04.2023.[10]

1.1.3 Automatisierte Entscheidungsfindung - Algorithmus muss nachvollziehbar sein

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 27.02.2025[11] mal wieder die Verbraucherrechte gestärkt. So müssen Unternehmen, die Bonitätsbewertungen durchführen, ihre Verfahren zur automatisierten Entscheidungsfindung (auch Profiling) im Rahmen von Auskunftsersuchen so offenlegen, dass diese von den betroffenen Personen nachvollzogen werden können.

Der Verantwortliche muss der betroffenen Person die Verfahren und Grundsätze, die er bei der automatisierten Verarbeitung seiner personenbezogenen Daten anwendet, präzise, transparent und leicht verständlich darlegen, d.h. die bei einer Auskunftei begehrte Auskunft sowie der Algorithmus zur Berechnung des Bonitäts-Scores muss für den Verbraucher nachvollziehbar sein.

Auch hier legt der EUGH das Recht auf Auskunft weit aus, indem er der Formulierung aus Art. 15 Abs. 1 lit. h) DS-GVO „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswir-

10 KDSA, TB 2023, Pkt. 1.1.5 Personenbeziehbarkeit pseudonymer Daten
11 EuGH, Urteil vom 27.02.2025 - C-203-22

kungen einer derartigen Verarbeitung für die betroffene Person“ so interpretiert, dass die betroffene Person die Entscheidung der Auskunftei nachvollziehen kann und prüfen kann, ob die verarbeitetet Daten sowie deren Ergebnis korrekt sind.

1.1.4 Höflichkeitsfloskeln und Datenschutz

Die Anrede „sehr geehrte Frau ..., sehr geehrter Herr ...“ in Geschäftsbriefen ist derzeit wohl noch die Regel in der geschäftlichen Kommunikation. Auch beim Ausfüllen von Online-Formularen werden Anwender regelmäßig verpflichtet, sich für eine dieser beiden Anreden zu entscheiden. Da es sich dabei häufig um Pflichtfelder handelt, kommen Kunden nicht umhin, eine der vorgegebenen Optionen zu wählen.

Ob solche Vorgehensweisen mit dem Datenschutzrecht zu vereinbaren sind, hatte der Europäische Gerichtshof (EuGH) zu entscheiden.

Das Gericht wurde angefragt, ob durch die Angaben „Herr“ oder „Frau“ die allgemeine Verkehrssitte in der privaten, geschäftlichen und behördlichen Kommunikation berücksichtigt werden und als erforderlich angesehen werden kann, ohne dass der Grundsatz der Datenminimierung dem entgegenstünde.

Der EuGH[12] stellte zunächst fest, dass die Anrede, die einer männlichen oder weiblichen Geschlechtsidentität entspricht, als „personenbezogenes Datum“ einzustufen ist. Weiterhin führt das Gericht aus, dass für die Verarbeitung personenbezogener Daten die Grundsätze des Art. 5 Abs. 1 DS-GVO (entspricht § 7 Abs. 1 KDG) beachtet und eine der Bedingungen des Art. 6 Abs. 1 DS-GVO (entspricht § 6 Abs. 1 KDG) gegeben sein muss. Die Liste der Fälle, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann, ist erschöpfend und abschließend und die Rechtfertigungsgründe seien eng auszulegen. Die in diesem Zusammenhang dargestellten Ausnahmen und Einschränkungen hinsichtlich des Grundsatzes des Schutzes personenbezogener Daten müssen sich auf das unbedingt Notwendige beschränken. Dementsprechend hat der Verantwortliche dieser Verarbeitung nachzuweisen, inwiefern der Hauptgegenstand des Vertrags ohne die Verarbeitung der in Rede stehenden personenbezogenen Daten nicht erfüllt werden könnte.

12 EuGH, Urteil vom 09.01.2025 - C-394/23d

Eine Kommunikation zwischen Diensteanbieter und Kunden kann die Beachtung der allgemeinen Verkehrssitte erfordern und insbesondere Höflichkeitsformeln enthalten, um den Respekt des betreffenden Unternehmens gegenüber seinem Kunden zum Ausdruck zu bringen und dadurch das Markenimage dieses Unternehmens zu schützen. Eine solche Kommunikation muss jedoch nicht notwendigerweise anhand der Geschlechtsidentität des betreffenden Kunden personalisiert werden.

In der Regel wird die Verarbeitung personenbezogener Daten hinsichtlich der Anrede der Kunden, die darauf abzielt, die geschäftliche Kommunikation aufgrund ihrer Geschlechtsidentität zu personalisieren, weder objektiv unerlässlich noch wesentlich für die ordnungsgemäße Erfüllung eines Vertrags sein und daher nicht als für die Erfüllung dieses Vertrags erforderlich angesehen werden können.

Anregungen für die Praxis:

- Verantwortliche sollten Kunden / Klienten / Patienten (männlich/weiblich/divers) die freie Wahl lassen, ob sie überhaupt eine Anrede wünschen und wenn ja, ob die Anrede als männlich, weiblich oder divers ausgestaltet sein soll.
- Generelle Verwendung völlig geschlechtsneutraler Höflichkeitsformeln.

1.2 Entwicklung des Datenschutzes in Deutschland

1.2.1 Einsichtsrecht statt Kopie: LAG München konkretisiert Auskunftsanspruch bei Compliance-Untersuchungen

Worum ging es?

Eine leitende Angestellte („Klägerin“), die sich in Elternzeit befindet, verlangte von ihrem Arbeitgeber („Beklagte“) die Herausgabe einer Kopie oder zumindest die Einsicht in einen Compliance-Abschlussbericht. Dieser Bericht wurde nach einer internen Untersuchung wegen ihres Führungsstils

erstellt, der als „einschüchternd“ und „respektlos“ beschrieben wurde. Der Arbeitgeber stützte seine Kündigungsbemühungen und andere Maßnahmen gegen die Klägerin auf diesen Bericht.

Das Arbeitsgericht München (1. Instanz) gab der Klägerin im Hauptantrag recht. Danach musste die Beklagte eine Kopie des Berichts herausgeben. Das Landesarbeitsgericht (LAG) München (2. Instanz) änderte das Urteil ab und entschied, dass die Beklagte keine Kopie zur Verfügung stellen, aber der Klägerin Einsicht in den Bericht gewähren muss.

Die Begründung des LAG München[13]

1. Hat die Klägerin Anspruch auf eine Kopie des Berichts nach der DS-GVO?

Die Klägerin berief sich auf Art. 15 Abs. 3 DS-GVO, der Betroffenen das Recht auf eine Kopie ihrer personenbezogenen Daten gibt.

Das LAG hat den Anspruch auf eine vollständige Kopie des Berichts verneint.

- Das Gericht stellte klar, dass die DS-GVO nur einen Anspruch auf eine Kopie der *personenbezogenen Daten* selbst gibt, nicht aber auf eine Kopie des *gesamten Dokuments* (des Berichts).
- Der Bericht enthält viel mehr als nur Daten über die Klägerin: Er umfasst auch die Aussagen der Zeugen, Zusammenfassungen, Bewertungen der Ermittler und rechtliche Schlussfolgerungen. All das sind keine reinen personenbezogenen Daten der Klägerin.
- Einen Grund dafür, dass der gesamte Bericht zur Verständlichkeit der Daten nötig sei, sah das Gericht nicht. Nach Ansicht des Gerichts möchte die Klägerin im Grunde die Prozessstrategie und die internen Bewertungen der Beklagten ausforschen, was über den eigentlichen Zweck des datenschutzrechtlichen Auskunftsanspruchs hinausgeht.

2. Hat die Klägerin Anspruch auf Einsicht in den Bericht als Teil ihrer Personalakte?

Als leitende Angestellte hat die Klägerin nach dem Sprecherausschussgesetz (§ 26 Abs. 2 SprAuG, analog zum Betriebsverfassungsgesetz) ein Recht auf Einsicht in ihre Personalakte.

13 LAG München, Urteil vom 12.06.2025 - 2 SLa 70/25

- Das Gericht ordnet den Compliance-Bericht als Bestandteil der materiellen Personalakte der Klägerin ein, da er sich unmittelbar auf ihr Arbeitsverhältnis und Verhalten bezieht.
- Der Arbeitgeber darf keine „Geheimakten" über den Arbeitnehmer führen. Der Inhalt der Personalakte kann daher auch kein gegenüber dem Arbeitnehmer geschütztes Geschäftsgeheimnis sein, so das Gericht.
- Das HinSchG ist hier laut Gericht nicht anwendbar, da die Vorwürfe (schlechter Führungsstil) keine „Katalogtaten" (wie Straftaten oder bußgeldbewehrte Verstöße) im Sinne des Gesetzes sind.
- Der Arbeitgeber kann die Einsicht nicht verweigern, um Hinweisgeber zu schützen. Er muss aber sicherstellen, dass die Identität der Hinweisgeber und Zeugen, denen Vertraulichkeit zugesichert wurde, etwa durch Schwärzung entsprechender Passagen unkenntlich gemacht wird. Versäumt der Arbeitgeber diese Anonymisierung, kann er die Einsicht trotzdem nicht verweigern.

Fazit:

Das Urteil des LAG München bringt eine sachgerechte Differenzierung zwischen Datenschutz und Unternehmensinteressen. Arbeitgeber müssen den Zugang zu personenbezogenen Daten ermöglichen, sind aber nicht verpflichtet, vollständige Compliance-Berichte herauszugeben. Für Arbeitnehmer eröffnet das Urteil dennoch eine effektive Möglichkeit, über das Einsichtsrecht Transparenz zu erlangen und ihre Rechte zu wahren.

Das LAG ließ die Revision zum Bundesarbeitsgericht (BAG) zu, soweit es um den Anspruch auf Überlassung einer Kopie ging. Das Verfahren vor dem BAG wird zeigen, ob diese Auslegung des Art. 15 DS-GVO Bestand haben wird.

1.2.2 Datenschutzverletzung im Bewerbungsverfahren – abgelehnter Jurist fordert Schadensersatz

Die Recherche von Bewerbern im Internet (sog. Background Checks) ist in vielen Unternehmen gelebte Praxis. Oft werden dabei frei verfügbare Informationen herangezogen, um die Eignung eines Kandidaten besser einschätzen zu können. Doch aktuelle Entscheidungen zeigen deutlich:

Eine solche Recherche birgt erhebliche rechtliche Risiken, insbesondere, wenn sie ohne transparente Information gegenüber dem Bewerber erfolgt. Wer als Arbeitgeber versäumt, die Informationspflichten der DS-GVO (KDG) zu beachten, sieht sich schnell immateriellen Schadensersatzforderungen ausgesetzt.

Das Verfahren: Ein Klick zu viel?

Ein Rechtsanwalt bewarb sich auf eine Stelle in der Rechtsabteilung der Universität Düsseldorf. Er wurde vom Personalleiter der Hochschule „gegoogelt", da diesem der Name des Bewerbers bekannt vorkam. In einem öffentlich zugänglichen Wikipedia-Eintrag stieß er dabei auf Hinweise zu einem nicht rechtskräftigen Strafurteil wegen versuchten Betruges. Der Anwalt soll Bewerbungen vorgetäuscht haben, um Entschädigungszahlungen nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) zu beanspruchen. Diese Information führte zur Ablehnung des Bewerbers. Er wurde von der Universität nicht darüber informiert, dass sie personenbezogene Daten über ihn aus öffentlich zugänglichen Quellen erhoben hatte. Er klagte vor dem Landesarbeitsgericht Düsseldorf (LAG) erfolgreich auf Schadensersatz.

Das LAG[14] sprach dem Kläger 1.000, - € Schmerzensgeld wegen Verstoßes gegen die DS-GVO zu. Die allgemeine Internetrecherche über den Bewerber sei als erforderlich i. S. v. Art. 6 Abs. 1 lit. b) DS-GVO anzusehen, da sie notwendig gewesen sei, um die Eignung des Bewerbers beurteilen zu können, so dass es sich um öffentlich zugängliche Informationen handelt. Das LAG meint, Bewerber dürfen im Rahmen eines Einstellungsverfahrens „gegoogelt" werden. Offen gelassen hat das LAG jedoch, ob dies auch für anlasslose Recherchen gilt. Im vorliegenden Fall war einem Mitglied der Auswahlkommission der Name des Bewerbers bekannt vorgekommen.

Die Recherchen im Internet – insbesondere über Google – ist bei der Personalauswahl nicht unüblich und mithin ein nicht außer Acht zulassendes Spannungsfeld. Bei der Recherche handelt es sich um eine Verarbeitung personenbezogener Daten. Das LAG wies in seiner Entscheidung darauf hin, dass gemäß Art. 14 Abs. 1 lit. d) DS-GVO Arbeitgeber verpflichtet sind, betroffene Personen über die Quelle und Kategorie dieser Daten zu informie-

14 LAG Düsseldorf, Urteil vom 10.04.2024 - 12 Sa 1007/23

ren, unbeschadet der Tatsache, dass sie öffentlich zugänglich sind. Nach Ansicht des LAG führt ein Verstoß gegen die Informationspflicht nicht zu einem Beweisverwertungsverbot. Diese Feststellung führt dazu, dass Beweise in Verfahren vor Gerichten genutzt werden können, auch wenn sie aufgrund eines Verstoßes gegen Art. 13 bzw. 14 DS-GVO gewonnen worden sind. Dies dürfte für Arbeitgeber relevant sein.

Kontrollverlust allein genügt nicht!

Nach der Rechtsprechung des BGH kann ein bloßer „Kontrollverlust" über personenbezogene Daten einen ersatzfähigen immateriellen Schaden für Betroffene begründen. Wie das BAG nun feststellte, braucht es aber mehr als bloßes Unwohlsein oder hypothetische Risiken.

Betroffene müssen darlegen können, dass sie tatsächlich einen Schaden erlitten haben – sei es durch Rufschädigung, diskriminierende Entscheidungen oder die konkrete Nutzung der Daten durch Dritte. Eine rein subjektive Sorge genügt nicht. Auch das BAG[15] hat darauf abgestellt, dass eine gewisse Erheblichkeitsschwelle überschritten werden muss, um Ersatzansprüche zu begründen.

Das LAG bejahte den Eintritt eines Schadens im vorliegenden Fall. Durch die fehlende Mitteilung sei der Bewerber zum bloßen Objekt der Datenverarbeitung geworden und habe einen erheblichen Kontrollverlust mit negativen Auswirkungen auf die Auswahlentscheidung im Bewerbungsprozess erlitten. Für das LAG war der Inhalt der Datenverarbeitung bei der Beurteilung des Schadens relevant. Der Bericht über die strafrechtliche Verurteilung stellt im Zusammenhang mit dem Bewerbungsverfahren eine negative Tatsache dar, zumal diese auch unrichtig wiedergegeben war. Bei der Höhe des Schadens wurde das negative Ausmaß der „gegoogelten" Information berücksichtigt. Das BAG hat die Entscheidung des LAG bestätigt.[16]

Fazit:

Die Entscheidung des BAG hat Signalwirkung. Sowohl das LAG Düsseldorf als auch das BAG halten Internetrecherchen im Bewerbungsverfahren

15 BAG, Urteil vom 20.06.2024 - 8 AZR 124/23
16 BAG, Urteil vom 05.06.2025 - 8 AZR 117/24

grundsätzlich für zulässig, setzen aber eine transparente Information nach Art. 14 DS-GVO voraus. Das LAG sprach wegen des Kontrollverlusts 1.000, - € zu, das BAG bestätigte diesen Betrag, präzisierte die Anforderungen an Kausalität und Schadensdarlegung und wies weitergehende Ansprüche mangels Nachweises der Bestqualifikation ab. Das BAG betont erneut, dass der Schadensersatz nach Art. 82 DS-GVO keine strafende, sondern ausschließlich eine ausgleichende Funktion hat. Wer Online-Recherchen vornimmt, muss dies dokumentieren und transparent machen.

1.2.3 Wann sind E-Mails Ende-zu-Ende zu verschlüsseln?

Personenbezogene Daten müssen durch eine Behörde nicht zwingend Ende-zu-Ende verschlüsselt werden, da eine Transportverschlüsselung (TLS) gemäß der DS-GVO zumeist ausreicht. Dies hat das OVG Nordrhein-Westfalen[17] entschieden.

Liegt kein besonders hohes Risiko vor, welches eine weitergehende Verschlüsselung erforderlich macht, reiche in den meisten Fällen eine TLS-Verschlüsselung (Transport Layer Security) aus, so das Gericht. TLS ist ein Protokoll, das entwickelt wurde, um die Sicherheit von Daten, die über Netzwerke übertragen werden, zu gewährleisten. Es sorgt dafür, dass Daten im Internet nicht im Klartext übertragen werden, somit Datenschutz und Datensicherheit während der Kommunikation über das Internet gewährleistet bleiben.

Der Kläger habe kein besonderes Risiko nachweisen können, was eine weitergehende Verschlüsselung erforderlich gemacht hätte. Damit bleibt es bei der generellen Regelung der DS-GVO, wonach angemessene Sicherheitsmaßnahmen getroffen werden müssen, aber keine spezifische Verschlüsselung zwingend vorgeschrieben ist, so das Gericht.

Nach Ansicht des OLG Schleswig-Holstein[18] ist eine differenzierte, einzelfallbasierte Risikoeinschätzung entscheidend. Für besonders kritische und sensible Inhalte wird auch weiterhin eine Ende-zu-Ende-Verschlüsselung erforderlich sein.

17 OVG Nordrhein-Westfalen, Beschluss vom 20.02.2025 -16 B 288/23
18 OLG Schleswig-Holstein, Urteil vom 18.12.2024 - 12 U 9/24

Mit Urteil vom 18.12.2024 hat der 12. Senat des OLG eine Entscheidung zur E-Mail-Verschlüsselung beim Rechnungsversand getroffen. Das rechtskräftige Urteil stärkt die Position der Rechnungsempfänger und definiert neue Standards für die DS-GVO-konforme Kommunikation.

Im zugrundeliegenden Fall wurde eine unverschlüsselte Rechnung eines Unternehmens durch einen sogenannten „Man-in-the-Middle"-Angriff abgefangen. Der Angreifer änderte die Bankverbindung in der Rechnung und leitete sie an den eigentlichen, privaten Empfänger weiter. Die Rechnungsempfängerin überwies den geschuldeten Betrag (ca. 15.000, - €) dadurch auf das Konto eines unbekannten Dritten.

Der Unternehmer forderte weiterhin die Zahlung vom Empfänger, da er der Meinung war, eine Erfüllung der Zahlungsverpflichtung sei nicht eingetreten.

Das OLG stellte in seiner Entscheidung mehrere wichtige Punkte klar:

- Die Überweisung auf das Konto des unbekannten Dritten hat nicht zur Erfüllung der werkvertraglichen Zahlungsverpflichtung geführt.
- Der Rechnungsempfängerin steht jedoch ein Schadenersatzanspruch in Höhe der fehlgeleiteten Überweisung aus Art. 82 DS-GVO zu, welcher dem Rechnungssteller entgegengehalten werden kann.
- Eine reine Transportschlüsselung (SMTP, TLS 1.2, 1.3) ist bei E-Mails mit hohem finanziellem Risiko nicht ausreichend. Eine Ende-zu-Ende-Verschlüsselung (*PGP, S/MIME*) wäre hier erforderlich gewesen.
- Durch die fehlende Ende-zu-Ende-Verschlüsselung war die Vertraulichkeit, Integrität und Authentizität der Nachricht nicht gewährleistet.
- Das Verschulden des Rechnungsstellers wird gesetzlich vermutet – eine Entlastung gelang in diesem Fall nicht. Dies begründet einen Schadenersatzanspruch aus Art. 82 DS-GVO.

Anregungen für die Praxis:

1. Überprüfung interner Verschlüsselungsrichtlinien für den E-Mail-Verkehr.

2. Implementierung von Ende-zu-Ende-Verschlüsselung (PGP, S/MIME) für sensible Inhalte, insbesondere:

- E-Mails mit besonderen personenbezogenen Daten (§ 11 KDG)
- Mitteilungen mit Berufsgeheimnissen (z. B. medizinisches Personal, Rechtsanwälte)
- Mitteilungen mit hohem finanziellem Risiko (hohe Rechnungen)

3. Alternative Lösungen in Betracht ziehen:

- Nutzung von Rechnungsportalen mit entsprechenden Verschlüsselungstechniken
- Klassischer Postversand als analoge Option

Hinweis: In unserem Tätigkeitbericht 2020 hatten wir uns bereits mit dem unterschiedlichen Verständnis von Verschlüsselungsmechanismen auseinandergesetzt.[19]

2 Datenschutz allgemein

2.1 Grundlegendes zum Auskunftsersuchen

Grundsatz

Bereits im letzten Jahr haben wir aufgrund mehrfacher Beschwerden Seminare zum Thema „Auskunftsrecht" angeboten. Die Zunahme von Beschwerden setzt sich dennoch in diesem Jahr fort. Dies nehmen wir zum Anlass das Thema an dieser Stelle nochmals darzustellen.

§ 17 Abs. 1 KDG „Die betroffene Person hat das Recht, von dem Verantwortlichen eine Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten …"

Diese Vorschrift gewährt einen doppelten Anspruch. Der Verantwortliche hat Betroffenen zunächst mitzuteilen, ob personenbezogene Daten von

19 KDSA, TB 2020, Pkt. 7.2 Unterschiedliches Verständnis – Ende-zu-Ende Verschlüsselung oder TLS

ihm verarbeitet werden. Sollte das nicht der Fall sein, ist den Anfragenden eine Negativauskunft zu erteilen.

Finden sich beim Verantwortlichen personenbezogene Daten des Betroffenen, ist diesem mitzuteilen, **welche** personenbezogenen Daten verarbeitet werden, einschließlich der weiteren Erklärungen gem. § 17 Abs. 1 lit. a) – h) KDG.

Der Anspruch auf Auskunft steht jeder natürlichen Person zu. Darüberhinausgehende Voraussetzungen sieht die Anspruchsgrundlage des § 17 KDG nicht vor. Die Bestimmungen ermöglichen dem Verantwortlichen demnach nicht, für den Auskunftsantrag der betroffenen Person eine Begründung zu verlangen.[20]

Frist

§ 14 Abs. 3 S. 1 KDG „Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den §§ 17 bis 24 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung."

Aus dieser gesetzlichen Regelung ergibt sich, dass dem Betroffenen die Auskunft unverzüglich zu erteilen ist. Eine Legaldefinition des Begriffs „unverzüglich" findet sich in § 121 BGB. Danach bedeutet „unverzüglich" ohne schuldhaftes Zögern. Der nachfolgende Halbsatz „...in jedem Fall aber innerhalb eines Monats..." eröffnet somit keine Regelfrist, sondern ist zu lesen wie „spätestens aber innerhalb eines Monats...". Damit ist eine Höchstfrist festgelegt, die nicht routinemäßig, sondern nur in schwierigeren Fällen ausgeschöpft werden darf.[21]

Nach einer Zeitspanne von mehr als einer Woche ist ohne das Vorliegen besonderer Umstände grundsätzlich keine Unverzüglichkeit mehr gegeben.[22]

In Ausnahmefällen kann der Verantwortliche die Frist um weitere zwei Monate verlängern, „wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist" (§ 14 Abs. 3 S. 2 KDG). Diese bei-

20 EuGH, Urteil vom 23.10.2023 - C-307/22
21 ArbG Duisburg, Urteil vom 03.11.2023 - 5 Ca 877/23; Kühling/Buchner/Bäcker, 3. Aufl. 2020, DSGVO Art. 12 Rn. 33
22 BAG, Urteil vom 27.02.2020 - 2 AZR 390/19

den Voraussetzungen müssen kumulativ vorliegen.[23] Andernfalls hätte es der Verantwortliche in der Hand, durch eine Unterbesetzung eine Arbeitsüberlastung herbeizuführen, die ihn zur Fristverlängerung berechtigte. Der Verantwortliche muss aber seine Datenverarbeitung vielmehr so organisieren, dass sie auch größere Fallzahlen von Anfragen bewältigt.[24]

Nur wenn der Verantwortliche eine mindestens teilweise Positivantwort beabsichtigt, darf er die Frist gem. § 14 Abs. 3 S. 2 KDG um weitere zwei Monate verlängern, wenn die Verlängerung erforderlich ist.[25]

Über die Fristverlängerung ist der Antragsteller innerhalb eines Monats nach Eingang des Antrags zusammen mit den Gründen für die Verzögerung zu informieren (§ 14 Abs. 3 S. 3 KDG). Das Gesetz schreibt hier eine Monatsfrist vor, also nicht unverzüglich. Gleichzeitig ist diese Frist aber nicht verlängerbar.

Form

Antragstellende sind an keine Form gebunden. Insbesondere kann der Verantwortlichen vom Antragsteller nicht verlangen, dass dieser seinen Antrag schriftlich stellt.

Für den Verantwortlichen wird die Form der Auskunft zunächst grundsätzlich durch § 14 Abs. 1 S. 2 KDG bestimmt: Die Übermittlung der Auskunft erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Für den Fall der elektronischen Antragstellung bestimmt § 17 Abs. 3 S. 3 KDG:

Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie (die Person) nichts anderes angibt.

Stellen Betroffene einen Auskunftsanspruch in elektronischer Form und beantragen die Auskunft schriftlich zu erhalten, ist darin also kein Widerspruch zu sehen. Vielmehr ist diesem Antrag zu entsprechen. Weiterhin können Betroffene verlangen die Information mündlich zu erhalten, wenn ihre Identität sichergestellt ist (§ 14 Abs. 1 S. 3 KDG).

23 Dix, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht Rn. 25
24 Dix, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht Rn. 25; Bäcker, in: Kühling/Buchner, DSGVO BDSG Rn. 34
25 Bäcker, in: Kühling/Buchner, DSGVO BDSG Rn. 34

Sicherheit

Wenn Betroffene einen Auskunftsanspruch schriftlich, per Briefpost, stellen und keine andere Form der Auskunftserteilung bestimmen, ist die Auskunft schriftlich, per Briefpost, an die vom Antragsteller genannte Postanschrift zu richten. Bei einem ordnungsgemäß verschlossenen Briefumschlag kann bei diesem Weg davon ausgegangen werden, dass die Information den Antragsteller sicher erreicht. Der Verantwortliche kann sich darauf verlassen, dass auf dem Postweg und im Bereich des Empfängers das Postgeheimnis (Art. 10 GG, § 206 StGB) gewahrt wird.

Die Übersendung der Information auf elektronischem Weg ist komplexer. Auch wenn Antragsteller diesen Kommunikationsweg wählen, ist darin keine Einwilligung zu sehen, die Information auf die gleiche Art zu erhalten. Auf die Sicherheit der Verarbeitung gem. § 26 KDG können Antragsteller regelmäßig auch nicht mit einer Einwilligung wirksam verzichten.[26]

Ist ein Auskunftsanspruch in elektronischer Form per E-Mail zu beantworten, ist die Information in einem zu verschlüsselnden Anhang beizufügen. Der Schlüssel ist dem Antragsteller/Empfänger auf einem anderen Weg als auf dieselbe E-Mailadresse zu übersenden. Hierfür kommen z. B. Short Message Service (SMS), sichere Messengerdienste (Threema, Signal) oder die Briefpost in Betracht.

Elektronische Kommunikation erfasst aber nicht nur Kommunikation über das Internet oder per E-Mail oder Messenger, sondern auch die Übergabe eines Datenträgers (CD, USB-Stick).[27]

Ausgeschlossen ist die Bereitstellung der Auskunft an einem Ort, den der Verantwortliche bestimmt. Auskunftsberechtigte sind nicht verpflichtet, durch eigenes Handeln an die beantragten Informationen zu gelangen. Dabei ist es völlig unerheblich, ob die Mitwirkung aus Sicht des Verantwortlichen zumutbar ist.

Zustellnachweis

Die Auskunftserteilung im Rahmen des Auskunftsanspruches gem. § 17 KDG ist eine Schickschuld. Das ergibt sich aus dem Wortlaut des § 14 Abs. 1 Satz 1 KDG „übermitteln“ bzw. § 17 Abs. 3 Satz 1 KDG „stellt zur Ver-

26 Schreibauer/Spittka, in: Wybitul, DS-GVO, Art. 32 Rn. 26; Pohle/Spittka, in: Taeger/Gabel, DS-GVO Art. 12 Rn. 17
27 Quaas, in: Wolff/Brink, BeckOK DatenschutzR, Art. 12 Rn. 28; Pohle/Spittka, in: Taeger/Gabel, DS-GVO Art. 12 Rn. 17

fügung".[28] Der Verantwortliche muss also nachweisen, dass er die Auskunft erteilt hat. Bei einer Auskunftserteilung per Briefpost wird man als geeigneten Nachweis einen Rückschein bei einem Einschreiben mit Rückschein oder die Zustellnachricht bei einem Einwurfeinschreiben ansehen können.

Der Nachweis des Zugangs einer E-Mail erfordert eine Lesebestätigung.[29] Für den Zugang einer E-Mail spricht kein Anscheinsbeweis. Auch dann, wenn der Absender die Versendung der Mail nachweisen kann. Der bloße Versand beweist also weder den Zugang noch das Lesen der E-Mail (siehe Pkt. 2.6 in diesem Bericht). Der Empfänger ist nicht verpflichtet, sein Posteingangsfach offenzulegen.

Fazit:

Eine wirksame Methode, um sich gegen ungerechtfertigte Abmahnungen oder Schadensersatzforderung zu wehren, ist die Abgabe einer korrekten Auskunft nach § 17 KDG / Art. 15 DS-GVO. Die Auskunftsanfrage gibt dem Betroffenen das Recht zu erfahren, welche personenbezogenen Daten von ihm verarbeitet werden und zu welchem Zweck. Es genügt nicht dem Ersuchenden lediglich eine Kopie seiner Daten, z. B. die Patientenakte oder Bewerbungsunterlagen, die eingereicht wurden, zurückzusenden.

Ein Handlungsleitfaden zur Auskunftserteilung befindet sich im Anhang.

2.2 Zulässigkeit von Videoüberwachung in Kirchlichen Einrichtungen

Das KDG erwähnt die Videoüberwachung explizit in § 52. In Abs. 1 dieser Vorschrift sind die Voraussetzungen benannt, unter denen Beobachtungen „öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen" zulässig sind.

1. Öffentlich zugängliche Räume

Öffentlich zugänglich sind Räume dann, wenn Berechtigte ihnen unbekannten Personen die Möglichkeit eröffnet haben, den Raum ungehindert,

28 Schmidt-Wudy, in: Wolff/Brink, Datenschutzrecht § 15 Rn. 84
29 OLG Rostock, Urteil vom 03.04.2024 - 7 U 2/24

insbesondere ohne vorherige Einlasskontrolle, zu betreten und sich darin aufzuhalten.[30]

Der Begriff des Raumes ist weit zu fassen und entspricht eher dem Begriff eines „Bereichs".[31] Die Regelung findet neben umschlossenen und überdachten Räumen auch auf umgrenzte Plätze und Bereiche außerhalb von Gebäuden Anwendung.[32]

Es kommt also zunächst auf die räumliche Gestaltung des Zuganges des überwachten Bereiches an. Können Personen dort eintreten, ohne durch Pförtner oder Sicherheitspersonal daran gehindert zu werden, handelt es sich um öffentlich zugängliche Räume. Entscheidet dagegen autorisiertes Personal darüber, ob und welche Räume betreten werden dürfen oder ist der Bereich nur befugten Personen zugänglich, findet die Vorschrift des § 52 KDG keine Anwendung. Die Prüfung der Zulässigkeit erfolgt dann nach den allgemeinen Regelungen des § 6 Abs. 1 KDG.

Beispiele für öffentlich zugängliche Räume:

- der Anmeldebereich in einem Krankenhaus
- ein kirchliches Museum
- Bereiche vor kirchlichen Einrichtungen, z.B. Fußwege, Vorplätze

2. Optisch elektronische Einrichtungen

Die Formulierung erfasst Kameras jeglicher Art und Gestaltung[33] sowie Geräte, die sich zur Videoüberwachung eignen (auch Wildkameras, Smartphones, Drohnen).[34] Dabei muss das Bild nicht aufgezeichnet werden; es genügt die Wiedergabe auf einem Monitor (Kamera-Monitor-Verfahren).[35]

Sind beide Voraussetzungen gegeben, ist zu prüfen, ob die Videoüberwachung zur Wahrnehmung des Hausrechtes oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und schutzwürdige Interessen der betroffenen Personen nicht überwiegen.

30 BVerwG, Urteil vom 27.03.2019 - 6 C 2.18
31 Reuter / Grabenschröer, in: Taeger/Gabel, DSGVO – BDSG – TTDSG § 4 BDSG Rn. 33
32 Scholz, in: NK-DatenschutzR Anhang zu Art. 6 DSGVO, Rn. 57
33 Leopold, in: Auernhammer DSGVO/BDSG § 4 BDSG Rn. 21
34 Reuter / Grabenschröer, in: Taeger/Gabel, DSGVO – BDSG – TTDSG § 4 BDSG Rn. 30-34
35 Schindler/Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht § 4 BDSG Rn. 50

„Hausrecht“ und „berechtigte Interessen“ lassen sich nicht strikt abgrenzen, sondern überschneiden sich inhaltlich. Man kann sich jedoch nicht beliebig auf das Hausrecht berufen, um eine Videoüberwachung durchzuführen. Vielmehr muss man sich auf ein berechtigtes Interesse, das heißt auf einen „guten Grund“ stützen können. Dies kann jedes subjektive Interesse sein, wenn es grundsätzlich schutzwürdig und objektiv begründbar ist.[36]

Erforderlichkeit ist anzunehmen, wenn ein Grund, etwa eine Gefährdungslage, hinreichend durch Tatsachen oder die allgemeine Lebenserfahrung belegt ist. Es muss also eine objektiv begründbare Gefahrenlage bestehen, die über das allgemeine Lebensrisiko hinausgeht und der nicht ebenso gut durch eine andere, gleich wirksame, aber schonendere Maßnahme Rechnung getragen werden kann. Schonender als die Videoüberwachung sind insbesondere Maßnahmen, die das informationelle Selbstbestimmungsrecht der Besucher der öffentlich zugänglichen Räume nicht berühren.

Bei dem Bestreben Kosten zu ersparen handelt es sich per se um ein berechtigtes Interesse. Der Verantwortliche muss aber darlegen, dass er die höheren Kosten, z. B. durch Anstellung eines Wachdienstes oder andere organisatorische Veränderungen anstatt einer Videoüberwachung nicht vermeiden konnte.

3. Nicht öffentlich zugängliche Räume

In nicht öffentlich zugänglichen Räumen richtet sich die Zulässigkeit von Videoüberwachungsanlagen ausschließlich nach den allgemeinen Regeln der Datenverarbeitung gem. § 6 Abs. 1 KDG.

Eine Rechtsgrundlage für die Datenverarbeitung kann das berechtigte Interesse der Einrichtung nach § 6 Abs. 1 lit. g) KDG darstellen, wie z.B. der Schutz vor Straftaten. Zudem dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person aber nicht schwerer wiegen. Allein das Vorliegen schützenswerter Interessen des Verantwortlichen reicht somit nicht aus. Selbst wenn die Videoüberwachung zu deren Wahrnehmung geeignet und erforderlich ist, muss in einem zweiten Schritt eine Abwägung mit den Interessen Betroffener erfolgen. Ermöglicht die aufgenommene äußere Erscheinung eine Identifizierung der Person, handelt es sich um personenbezogene Daten. Gleichzeitig kann es sich dabei auch

36 BVerwG, Urteil vom 27.03.2019 – 6 C 2.18, Rn. 25

um Gesundheitsdaten handeln, wenn die Aufnahmen z. B. in einem Krankenhaus oder einer Arztpraxis etc. erfolgen. Denn allein die Tatsache, dass eine Person eine Arztpraxis oder ein Krankenhaus aufsucht, bedeutet in der Regel eine Information über ihren Gesundheitszustand.

Es reicht daher nicht aus, dass Verantwortliche behaupten, die Videoüberwachung sei aus Sicherheitsgründen erforderlich. Diese Behauptung muss durch konkrete Vorfälle belegt werden.

Da eine nicht erforderliche Videoüberwachung immer unzulässig ist, erübrigt sich dann eine weitergehende Interessenabwägung. An dieser Rechtslage ändern auch deutlich sichtbare Hinweisschilder nichts. Insbesondere wird mit der bloßen Kenntnisnahme kein Einverständnis mit der Videoüberwachung durch Betroffene zum Ausdruck gebracht. Das Passieren eines Hinweisschilds oder das Betreten der überwachten Räume stellt keine Willenserklärung im Sinne einer Einverständniserklärung zur Überwachung dar.

Zusammengefasst ergeben sich aus den Bestimmungen des KDG drei Kriterien, die für den Betrieb von Videoüberwachungsanlagen notwendig sind:

- Wahrung berechtigter Interessen,
- Erforderlichkeit,
- Interessenabwägung.

Es ist jedoch in jedem Einzelfall zu prüfen, ob der Überwachung keine höherrangigen Interessen von Personen entgegenstehen, die Objekte der Überwachung werden können.

4. Wie lange dürfen zulässig gefertigte Videoaufnahmen gespeichert werden?

Die Daten der Videoüberwachung sind unverzüglich zu löschen, wenn sie zur Erreichung der Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind (§ 19 Abs. 1 lit. a) KDG) oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein

bis zwei Tagen geklärt werden können. Demnach wäre eine Löschung nach 48 Stunden angebracht. Da jedoch Einrichtungen über Feiertage oder Wochenenden häufig nicht besetzt sind oder eine Prüfung der Videoaufzeichnungen in diesen Zeiten nicht erfolgt, hat eine Löschung spätestens nach 72 Stunden unter Berücksichtigung des Grundsatzes der Datenminimierung gem. § 7 Abs. 1 lit. c) und e) KDG zu erfolgen.

5. Wer darf auf Videoaufnahmen zugreifen?

Bei den Aufnahmen der Videokamera handelt es sich um personenbezogene Daten gem. § 4 Nr. 1 KDG. Eine Verarbeitung ist nur zulässig, wenn die gesetzlichen Voraussetzungen erfüllt sind. Die personenbezogenen Daten dürfen dann nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden. Diese Zwecke sind im Verzeichnis der Verarbeitungstätigkeiten festzuhalten.

Der Verantwortliche hat sicher zu stellen, dass nur derjenige, der mit der legitimen Verarbeitung der personenbezogenen Daten betraut ist, auf diese zugreifen kann.

Im Berichtzeitraum gab es mehrere Beschwerden zu Videoüberwachungen in kirchlichen Einrichtungen. Einige davon werden unter Pkt. 3.3 beschrieben.

2.3 Verpflichtungserklärung zum Datengeheimnis – oft zu kurz und nicht vollumfänglich

Alle Beschäftigten, die personenbezogene Daten verarbeiten, sind gem. § 5 KDG auf das Datengeheimnis zu verpflichten. Dies ist nicht neu und hatte bereits vor Inkrafttreten des KDG bestand.

Werden uns im Rahmen einer Datenschutzüberprüfung oder Anhörung diese Dokumente vorgelegt, so konnten wir feststellen, dass diese in einigen Einrichtungen nicht abschließend und vollumfänglich ausgestaltet sind. Im Weiteren wurde die Verpflichtungserklärungen auch nicht von allen Beschäftigten i. S. d. des § 4 Nr. 24 KDG unterzeichnet.

In diesem Zusammenhang haben wir auch festgestellt, dass diese Dokumente zwar von den Mitarbeitenden unterzeichnet worden sind, aber diese

oft gar nicht wussten, welche Datenschutzregeln gelten und wie diese umzusetzen sind bzw. wo diese nachgelesen werden können.

Wer ist zu verpflichten?

Auf das KDG und die weiteren maßgeblichen Datenschutzvorschriften sind alle Mitarbeitenden zu verpflichten, die bei kirchlichen Stellen nach § 3 Abs. 1 KDG beschäftigt sind und personenbezogene Daten verarbeiten.

Der Begriff des Mitarbeitenden ist dabei weit zufassen und geht über den Kreis der Beschäftigten hinaus. Er gilt auch für alle hauptamtlichen und ehrenamtlichen Beschäftigten. Ebenso zählen Hospitanten und Praktikanten zu den Beschäftigten.

Praxisbeispiel 1:

In einem Kinder- und Jugendhaus nimmt ein Bewerber stundenweise am Gruppenleben teil. Ihm sind dabei die Gruppenräume zugänglich, in denen Namenslisten hängen, und er nimmt an einer Teamsitzung teil.
Der Bewerber muss vor der Hospitation oder einem Praktikum die Verpflichtungserklärung unterzeichnen. Eine mündliche Belehrung auf Verschwiegenheit ist nicht ausreichend.

Praxisbeispiel 2:

In einer Pfarrei wird eine FSJlerin beschäftigt. Sie unterstützt dabei die Pfarrei in allen anfallenden Arbeiten, u.a. auch in dem Versenden von E-Mails.

Die FSJlerin ist vor Beginn ihrer Tätigkeit auf die Einhaltung das Datengeheimnis zu verpflichten. Zudem hat sie auch eine Datenschutzschulung zu absolvieren und muss Hinweise bekommen, wie sie die Datenschutzregeln beim Versenden von E-Mails umsetzen kann. Merkblätter zum Datenschutz, in denen die Grundlagen des Datenschutzes sowie Praxistipps zum Umsetzen enthalten sind, können eine Lösung dafür sein.

Auf was ist zu verpflichten?

Nach § 2 Abs. 2 KDG-DVO müssen die Mitarbeitenden mit den Vorschriften des KDG sowie den anderen für ihre Tätigkeit geltende Datenschutzvorschriften vertraut gemacht werden. D.h. es muss individuell – je nach

Aufgaben- oder Tätigkeitsbereich - auf die wesentlichen Grundsätze und Erfordernisse hingewiesen werden.

Konkret müssen neben dem KDG auch die weiteren Gesetze oder Datenschutzvorschriften genannt werden, die der Mitarbeiter einzuhalten hat.

Regelungen, die neben dem KDG gelten können (Aufzählung nicht abschließend):

- SGB, z.B. SGB VIII Kinder- und Jugendhilfe
- Seelsorge-PatDSG
- Fernmeldegeheimnis gem. § 88 TKG
- Pflicht zur Verschwiegenheit nach § 203 STGB
- Schulgesetze der Länder
- Interne Dienstanweisungen

Die hier genannten Regelungen müssen zur Einsichtnahme oder Ausleihe vom Verantwortlichen bereitgehalten werden. Der Mitarbeiter, der die Verpflichtungserklärung unterzeichnet, muss darüber informiert werden, wo er diese Dokumente finden und einsehen kann.

Im Rahmen unserer anlassbezogenen oder anlasslosen Datenschutzüberprüfungen lassen wir uns regelmäßig die Verpflichtungserklärungen vorlegen. Im Großen und Ganzen sind diese Erklärungen gut aufgesetzt und werden zeitnah (teilweise vor Beginn der Beschäftigung) unterzeichnet.

Aufgefallen ist jedoch, dass diese nicht immer vollumfänglich ausgestaltet sind und oft erst nach Beginn der Beschäftigung oder im Rahmen einer Datenschutzunterweisung unterzeichnet werden. Auch wenn Beschäftigte bereits durch arbeitsvertragliche Regeln zur Verschwiegenheit verpflichtet sind, ist dies im Sinne des KDG nicht ausreichend. Die **Verpflichtungserklärung** auf das Datengeheimnis geht in ihrem Inhalt und Umfang über die arbeitsvertraglichen Regeln hinaus, gilt auch für Ehrenamtliche und Bewerber, die im Rahmen von Hospitationen die Einrichtungen kennenlernen wollen und ist die **erste Sensibilisierungsmaßnahme**, die Verantwortliche umsetzen sollten.

Eine Formulierungshilfe Verpflichtungserklärung zum Datengeheimnis gem. § 5 KDG ist auf unserer Webseite[37] veröffentlicht. Diese ist ggf. zu erweitern bzw. auf die Erfordernisse der jeweiligen Einrichtung anzupassen.

2.4 Veröffentlichen von Informationen auf Instagram

Eine Auszubildende eines Krankenhauses hat mit ihrem privaten Smartphone Inhalte eines dienstlichen Tablets fotografiert. Auf dem Tablet waren der Vor- und Nachname eines Patienten, dessen Geburtsdatum sowie Vitaldaten, wie Körpertemperatur und der Puls, abgebildet. Diese Aufnahme hat die Auszubildende auf Instagram zusammen mit einem weiteren Foto, dass mit dem Namen des Krankenhauses gekennzeichnet war, unter der sog. Story "Pflegealltag" eingestellt.

Namen und Geburtsdaten sind personenbezogene Daten i. S. v. § 4 Nr. 1 KDG. Vitaldaten, wie Körpertemperatur und Puls sind personenbezogene Daten besonderer Kategorie i. S. v. § 4 Nr. 2 KDG. Die Bekanntgabe gegenüber Dritten stellt eine Verarbeitung (Offenlegung) i. S. v. § 4 Nr. 3 KDG dar.

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

Neben der rechtmäßigen Verarbeitung müssen von der Verantwortlichen auch die Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Gem. § 7 Abs. 1 lit. f) KDG müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Es sind geeignete technische und organisatorische Maßnahmen zu treffen und einzuhalten, um die personenbezogenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung zu schützen. Insbesondere für die Verarbeitung besonderer Kategorie personenbezogener Daten, zu denen auch Angaben zu Vitaldaten eines Patienten gehören, sind an-

37 KDSA, https://www.KDSA Ost.de/images/CONTENT/INFOTHEK/Marbeitshilfen/dok/AH-FH-Verpflichtungserklaerung-Datengeheimnis-KDG-5.pdf

gemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 11 Abs. 4 KDG).

Beim Träger des Krankenhauses gelten sog. „Social Media Guidelines“, die allgemeine Regelungen / Hinweise zum Umgang mit sozialen Medien, wie z. B. Facebook, Instagram, LinkedIn etc. enthalten. Diese Guidelines erhalten alle Mitarbeiter, die u.a. regelmäßig auf die besondere Pflicht zur Vertraulichkeit und Verschwiegenheit sensibilisiert bzw. hingewiesen werden. An diese Vorgaben hatte sich die Auszubildende nicht gehalten.

Nach Bekanntwerden der Veröffentlichung wurde die Auszubildende umgehend aufgefordert die Aufnahmen zu löschen. Dieser Aufforderung ist sie nachgekommen. Wie der Arbeitgeber mitteilte, erhielt die Auszubildende arbeitsrechtlich für ihr Verhalten eine Abmahnung.

Da die Auszubildende die personenbezogenen Daten nicht im Interesse des Verantwortlichen verarbeitet hat, sondern im eigenen Interesse, lag ein sogenannter Mitarbeiterexzess vor. Dies hat zur Folge, dass unsere Dienstelle aufgrund der Zuständigkeitsregelung des § 3 KDG nicht zuständig ist und das Verfahren an die zuständige staatliche Datenschutzaufsicht abgegeben hat.

Exkurs: Soziale Medien und der Datenschutz

Inzwischen gehört Instagram zu den beliebtesten Social-Media-Kanälen überhaupt, wenn es nicht gar den Spitzenplatz einnimmt. Neben anderen Anbietern wie Facebook, YouTube, TikTok und WhatsApp ist „Insta“ inzwischen wohl zu einem der wichtigsten Kommunikations- und Marketinginstrumente bei Eltern und Kindern und vor allem aber auch für viele Unternehmen geworden. Gerade für Werbung und Marketing ist die riesige Follower Menge, die Instagram mitbringt, höchst interessant. Auch die Mitarbeitersuche von Unternehmen und Behörden erfolgt zunehmend über Instagram. Ebenso werden dort Neuigkeiten und Bekanntmachungen „geteilt“. Auch kirchliche Einrichtungen und Rechtsträger nutzen soziale Medien, wie z. B. Instagram, um sich zu präsentieren.

Die Datenschutzbehörden können bisher keine Empfehlung für eine datenschutzkonforme Nutzung von Facebook und Instagram erteilen. Viele der

damit verbundenen Pflichten sind vom einzelnen Betreiber/Verantwortliche aktuell nicht erfüllbar, weil der Mutter-Konzern Meta Platforms, Inc. die dafür notwendigen Informationen nicht zur Verfügung stellt.

Uns ist bewusst, dass Instagram und Facebook eine hohe Reichweite haben. Informationen können dort einfach abgerufen und auch zur Verfügung gestellt werden.

Auf Facebook und / oder Instagram sollten jedoch **keine personenbezogenen Daten** veröffentlicht werden.

Sollen personenbezogene (persönliche) Daten (u.a. Fotos) veröffentlicht werden, ist eine freiwillige Einwilligungserklärung zur Datenverarbeitung, mit dem Hinweis was mit den Daten im Internet passieren kann, erforderlich. Diese muss unterzeichnet werden.

Was ist bei der Nutzung von sozialen Medien noch zu beachten?

- Rechtliche Grundlagen prüfen
  (z.B. ist zu beachten, dass der Betrieb einer Facebook-Fanpage oder eines Instagram-Kanals an ein persönliches Nutzerkonto gekoppelt ist)
- Ggf. Einwilligungen der Betroffenen (Kinder bzw. Eltern, Mitarbeiter) einholen
- Datenschutzerklärung bereitstellen
- Datensparsame und datenschutzfreundliche Nutzung
  - Keine sensiblen Daten nutzen
  - Trennung von privatem und dienstlichem Account
  - Ausschöpfen sämtlicher Sicherheitseinstellungen
  - Nutzung von Daten für Training Künstlicher Intelligenz widersprechen oder deaktivieren
  - Seiten „nur“ verlinken, nicht einbinden (einbetten)
- Technische und organisatorische Maßnahmen implementieren
- Verfahren zum Auskunftsanspruch prüfen und ggf. aktualisieren
- Ggfs. Aufnahme in das Verzeichnis von Verarbeitungstätigkeiten (VVT)
- Ggf. Alternativen wie z.B. Mastodon verwenden

Was jedoch nicht vergessen werden darf: Jeder Klick, jedes Foto, jeder Kommentar und sogar unsere Aufenthaltsorte können von Instagram analysiert, gespeichert und weiterverarbeitet werden.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit in Sachsen-Anhalt, Frau Rost, hat kürzlich Empfehlungen für die Nutzung von Instagram im Schulbereich veröffentlicht. Daneben gibt es eine Checkliste mit den wichtigsten datenschutzrechtlichen Voraussetzungen.[38] Wir schließen uns diesen Empfehlungen der Datenschutzbeauftragten an.

Digitale Souveränität: Die zukünftige Strategie sollte die Unabhängigkeit von US-Konzernen und die Stärkung der Daten- und Informationssicherheit in Europa sein.

2.5 Benennung der zuständigen Aufsicht in den Datenschutzinformationen

Im Berichtszeitraum wandte sich ein Petent telefonisch mit einem Anliegen an uns. Er wollte sich über ein nicht erfülltes Auskunftsersuchen eines Krankenhauses beschweren und fragte an, ob wir zuständig seien, da auf der Internetseite der Klinik, die zu einem großen Verband gehört, unter dem Punkt „Recht auf Beschwerde und Kontaktdaten der zuständigen Behörde“ alle 5 Katholischen Aufsichtsbehörden, der Beauftrage für den Datenschutz der EKD sowie einige staatliche Aufsichtsbehörden genannt waren.

Muss die zuständige Aufsicht benannt werden?

In Art. 77 Abs. 1 DS-GVO heißt es: „ …Recht auf Beschwerde bei ***einer*** Aufsichtsbehörde“. In § 48 Abs. 1 KDG a. F. hieß es: „… Recht auf Beschwerde bei ***der*** Aufsicht“ und in § 46 Abs. 1 DSG-EKD heißt es: „…Recht sich mit einer Beschwerde an ***die*** Aufsichtsbehörde zu wenden“.

Aus welchem Grund eine unterschiedliche Formulierung gewählt wurde ist nicht bekannt. Nach der Novellierung des KDG heißt es in § 48 Abs. 1 KDG nunmehr auch: Recht auf Beschwerde ***bei einer Aufsicht.*** Die Änderung wurde vorgenommen, da die alte Regelung auslegungsbedürftig war. Es

38 https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-schule-und-kita

handelt sich dabei um eine sprachliche Anpassung, die damit an die Regelung in der DS-GVO angelehnt ist.

Es ist jedoch sinnvoll, die zuständige Aufsicht anzugeben, da der Aufwand gering ist und das Verfahren durch Ansprache der richtigen Aufsicht beschleunigt werden dürfte.

Eine Formulierung könnte lauten:

»Sie haben das Recht, sich bei einer Aufsichtsbehörde zu beschweren. Für uns zuständig ist diese Behörde ...«.

Wir haben genau diese Anregung dem Krankenhaus unterbreitet.

2.6 Nachweis des E-Mail-Empfangs

Zunehmend ersetzt die digitale Kommunikation, z. B. per E-Mail, eine schriftliche Korrespondenz, die mit Hilfe der Briefpost geführt wird. Bislang haben wir mehrfach auf die Sicherheit in diesem Themenbereich hingewiesen (sichere Übertragung, Verschlüsselung). Mehrere gerichtliche Entscheidungen befassen sich aber auch damit, wie der Absender nachweisen kann, dass eine E-Mail beim Empfänger zugegangen ist. Im Ergebnis tauchen hier dieselben Probleme auf, wie bei der Briefzustellung.

Für den Zugang einer E-Mail spricht kein Anscheinsbeweis. Auch dann, wenn der Absender die Versendung der Mail nachweisen kann. Der Empfänger ist nicht verpflichtet, sein Posteingangsfach offenzulegen. Der Nachweis des Zugangs einer E-Mail erfordert eine Lesebestätigung, so das Oberlandesgericht Rostock.[39] Der bloße Versand beweist weder den Zugang noch das Lesen der E-Mail, so auch das OLG Hamm.[40]

Versand belegt nicht Empfang

Die Gerichte entschieden, dass es keinen Anscheinsbeweis für den Empfang einer E-Mail gibt, wenn sich allein aufgrund des Sendeprotokolls beim Absender nachweisen lässt, dass diese tatsächlich versendet wurde. Aus technischen Gründen sei es möglich, dass trotz des ordnungsgemäßen Versands der E-Mail, diese den Empfänger nicht erreicht, auch wenn sich beim Versender der Versand als korrekt darstellt, insbesondere eine Un-

39 OLG Rostock, Beschluss vom 03.04.2024 – 7 U 2/24
40 OLG Hamm, Beschluss vom 18.03.2023 – 26 W 13/23

zustellbarkeitsnachricht auf Seiten des Absenders nicht erfolgt ist. In den Verfahren ging es um die Frage des Zugangs einer E-Mail (OLG Hamm, LAG Köln).[41]

Genau wie bei der Briefpost darf das Risiko der ausbleibenden Zustellung nicht auf den Empfänger übertragen werden, da der Absender die Art der Übermittlung wählt und daher auch das Zustellungsrisiko trägt. Der Absender kann aber das Zustellungsrisiko mit einer Lesebestätigung minimieren.

Aus dieser Erwägung heraus hatte das OLG Rostock auch die Aufforderung der Klägerin an die Beklagte des Verfahrens, ihren E-Mail-Zugang zum fraglichen Zeitpunkt offenzulegen, zurückgewiesen. Das Verlangen auf Offenlegung des digitalen Postzugangs sei vergleichbar mit einem Antrag, die Briefkästen oder Wohnungen und Geschäftsräume eines vermeintlichen Empfängers auf eine per Brief versandten Erklärung zu durchsuchen. Dies sei unverhältnismäßig und daher unzulässig.

Es gibt für Empfänger einer E-Mail keine Verpflichtung, deren Zugang mit einer Lesebestätigung zu quittieren, insbesondere deshalb nicht, weil eine Ablehnung nicht unredlich sein muss. Denn automatisch generierte Lesebestätigungen können sich auch nachtteilig auswirken, wenn Spammer Nachrichten mit Lesebestätigungen versenden und so feststellen können, ob die Empfänger-Postfächer existieren und sogar aktiv genutzt werden.

Verweigern Empfänger eine Lesebestätigung und geben auch auf andere Weise den Erhalt der E-Mail nicht zu erkennen, ist der Absender gezwungen, eine andere Art der Zustellung zu wählen.

Fazit:

Diese Gerichtsentscheidungen unterstreichen die Notwendigkeit, bei der E-Mail-Kommunikation für rechtliche oder wichtige geschäftliche Kommunikation vorsichtig zu sein. Denn es kann nicht davon ausgegangen werden, dass eine E-Mail den Empfänger auch tatsächlich erreicht hat, ohne dass dies durch einen zusätzlichen Nachweis bestätigt werden kann. Geeignet wäre u.a. auch eine Aufforderung zu einer kurzen Rückinformation als Bestätigung für den Empfang.

Damit schützt sich der Absender vor rechtlichen Unsicherheiten und stellt sicher, dass eine Kommunikation per E-Mail weiterhin effektiv und sicher gestaltet werden kann.

41 OLG Hamm, a.a.O.; LAG Köln Urteil vom 11.01.2022 – 4 Sa 315/21

2.7 Keine Kopien von Personalausweisen zulassen!

Einer Gruppe von Hackern ist es gelungen, in die Buchungssysteme italienischer Hotels einzudringen. Daten Zehntausender Hotelgäste wurden gestohlen. Jetzt kursieren die Dokumente im Darknet. In Italien muss man sich bei der Anmeldung im Hotel mit Ausweispapieren anmelden, die dann in der Regel an der Rezeption kopiert werden.

Wie ist die Rechtslage in deutschen Hotels?

Hotels müssen für Gäste mit deutscher Staatsangehörigkeit keinen besonderen Meldeschein mehr vorhalten, unterschreiben lassen oder archivieren, da die Meldepflicht für inländische Gäste ab dem 01. Januar 2025 entfallen ist.

Somit muss die Meldepflicht auch nicht mehr alternativ durch einen sogenannten elektronischen Meldeschein erfüllt werden (§ 29 Abs. 5 BMG). Die Hotels dürfen jedoch personenbezogene Daten ihrer Kunden erheben, soweit dies zur Erfüllung rechtlicher Verpflichtungen erforderlich ist. So ist es erlaubt, von Gästen mit deutscher Staatsangehörigkeit ohne ihre ausdrückliche Zustimmung Daten zu erheben, die zur Vertragserfüllung und ggf. zur Abrechnung kommunaler Beiträge (Kurtaxe, Tourismusabgabe, City Tax, Übernachtungssteuer etc.) erforderlich sind.

Darüber hinaus dürfen Hotels grundsätzlich auch Einsicht in den Personalausweis nehmen und die gültige Adresse der Gäste speichern, z. B. um im Nachgang Regressansprüche gegenüber den Gästen geltend zu machen (Diebstahl, Sachbeschädigung, ect.). Ansonsten gilt der Grundsatz der Datenminimierung, wonach das Erheben von Daten, die nicht erforderlich sind, unzulässig ist. Durch eine Ausweiskopie erhält ein Hotel viel mehr Daten als es zum Datenabgleich benötigt. Die auf dem Ausweis vermerkten Nummern oder auch das Passfoto sind Informationen, die das Hotel nicht erheben darf!

Dennoch verlangen einzelne Hotels bzw. Hotelketten eine Kopie des Personalausweises. In diesem Fall sollte sich der Gast an die zuständige Datenschutzaufsicht wenden und dieses Vorgehen dort benennen.

Dürfen Personalausweise allgemein kopiert werden?

Ein generelles Verbot seinen Personalausweis zu kopieren gibt es nicht. Aber § 20 Abs. 2 Personalausweis Gesetz (PAuswG) legt fest, dass der Ausweis nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden darf, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist.

Ausweiskopien können für Phishing, Schockanrufe oder Enkeltricks verwendet werden. Auch Identitätsdiebstahl ist möglich. Wenn Kriminelle an Ausweisdaten gelangen, können große finanzielle Schäden entstehen. Es gilt daher die dringende Empfehlung den Personalausweis niemals zu kopieren oder eine Kopie per E-Mail zu versenden.

Oftmals kommt es vor, dass Unternehmen zum Beispiel bei der Vermietung eines Fahrrades sich den Ausweis vom Kunden als Pfand übergeben lassen, um damit sicherzustellen, dass der entliehene Gegenstand wieder ordnungsgemäß zurückgegeben wird.

Diese Vorgehensweise ist unzulässig. Das Aushändigen des Ausweises als Pfand darf nicht verlangt werden. Denn während der Hinterlegung sind die Ausweisdaten vollständig – das heißt auch hinsichtlich der Sicherungsmerkmale – dem Zugriff Dritter preisgegeben. § 1 Abs. 1 S. 3 PAuswG verbietet eine solche Verfahrensweise ausdrücklich. „Vom Ausweisinhaber darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben“.

2.8 Klimaschutz durch Datenschutz: Datensparsamkeit als Beitrag zur Energiewende

In einer Zeit, in der der Klimawandel eine der größten Herausforderungen unserer Gesellschaft darstellt, wird der Zusammenhang zwischen Datenschutz und Klimaschutz zunehmend sichtbar. Ein zentraler Aspekt, der oft übersehen wird, ist die Rolle der Datensparsamkeit. Wer sich an die Prinzipien der Datensparsamkeit hält, leistet nicht nur einen Beitrag zum Schutz der Privatsphäre, sondern trägt auch aktiv zur Reduzierung des Energieverbrauchs von Rechenzentren, Netzwerken und Endgeräten bei.

Der CO_2-Ausstoß durch die Digitalisierung steigt stetig an. In Deutschland verursacht die Internetnutzung mittlerweile mehr Emissionen als der gesamte Flugverkehr.

Rechenzentren als Energiefresser

Allein die monatlichen Google-Suchanfragen verbrauchen genug Energie, um ein 100-Watt-Leuchtmittel über 4.500 Jahre zu betreiben. Im Schnitt schlägt eine einzelne Suchanfrage mit 0,3 Watt zu Buche. Eine durchschnittliche LED-Lampe (6W) könnte damit beispielsweise drei Minuten lang leuchten. Der Energieverbrauch einer Anfrage bei Chat-GPT ist sogar noch höher und liegt bei 2,9 Wattstunden. Mit dieser Energie könnte die LED-Lampe also schon fast eine halbe Stunde lang leuchten.[42] Dabei wird der Großteil der Energie nicht in den eigenen vier Wänden verbraucht, sondern in den Kühlungen der Rechenzentren der Anbieter und in den Telekommunikationsnetzen der Datenströme. Alles zusammen erhöht den CO_2-Fußabdruck gewaltig.

Weniger Daten bedeutet dabei weniger CO_2-Ausstoß. Zudem wird dadurch auch dem Grundsatz der Datenminimierung Rechnung getragen (§ 7 Abs. 1 lit. c) KDG).

Datenmüll auf Endgeräten treibt Energiebedarf in die Höhe

Smartphones, Tablets und PCs verbrauchen zusätzliche Energie, wenn sie große Datenmengen speichern, synchronisieren oder verarbeiten. Hier liegt großes Potenzial zur Reduzierung des digitalen CO_2-Fußabdrucks. Regelmäßige Aufräumaktionen helfen zu prüfen, welche Daten und Informationen auf den Geräten und Servern gespeichert sind und welche tatsächlich benötigt werden. Dadurch können Speicherkapazitäten eingespart, die Lebensdauer von IT-Ausrüstung verlängert und der CO_2-Ausstoß reduziert werden. Jede gelöschte Datei zählt!

E-Mail-Postfach

Der Versand, das Lesen und Speichern einer E-Mail verursacht durchschnittlich 10 g CO_2. Im Schnitt erhält jeder 21 E-Mails täglich. Dadurch

42 https://www.verbraucherzentrale-brandenburg.de/stromverbrauch-suchmaschine

werden nicht nur ca. 80 kg CO_2 pro Person jährlich generiert, sondern auch jede Menge Wasser für das Kühlen der Server verbraucht. Das eigene E-Mail-Postfach sollte daher regelmäßig aufgeräumt werden.

1. Nicht genutzte Newsletter abbestellen.
2. Alte, nicht mehr benötigte E-Mails löschen.
3. Gesendete Elemente und den Papierkorb regelmäßig leeren.

Endgeräte (Laptops, Tablets, PC`s, Smartphones)

Das Aufräumen der technischen Endgeräte, wie z. B. das Diensthandy oder die lokale Festplatte des Laptops ist wichtig, um Speicherplatz freizugeben, Datenübertragungen zu reduzieren und die Leistung der Geräte zu verbessern.

1. Unbenutzte Apps und Software löschen.
2. Unnötige Fotos, Videos und Dateien regelmäßig löschen, dabei den Desktop, den Download-Ordner und den Papierkorb nicht vergessen.
3. Dateien und Ordner sinnvoll organisieren, um unnötige Duplikate zu vermeiden.
4. Energieeffiziente Hardware und Softwarelösungen einsetzen, die den Energieverbrauch minimieren.
5. Nichtbenutzte Geräte ausschalten bzw. herunterfahren, Energiesparmodus bei längeren Pausen einschalten.

Die hier aufgezeigten Maßnahmen tragen dazu bei, den Grundsatz der Datensparsamkeit gem. § 7 Abs. 1 lit. c) KDG einzuhalten, indem nur notwendige Daten verarbeitet und vorgehalten werden.

Auch jede Geräteproduktion und -distribution erzeugt weitere Emissionen. Wer ein Arbeitsmittel nur vorübergehend benötigt, kann durch das Mieten von Hardware Kosten sparen und das Klima schützen.

Fazit:

Der digitale Datenputz kann nicht nur dazu beitragen, digitale Geräte und Daten aufzuräumen und zu organisieren, sondern führt auch zu Energieeinsparungen und hilft somit das Klima zu schonen. Durch Datenspar-

samkeit können wir einen aktiven Beitrag zur Reduzierung des Energieverbrauchs technischer Geräte und Datenverarbeitung in Rechenzentren leisten.

3 Datenschutzaufsicht

3.1 Prüfaktionen

3.1.1 Datenschutzüberprüfung – Schule

Auch im Berichtsjahr 2025 gab es verschiedene Vorort-Prüfungen der Datenschutzaufsicht. Im Kinder- und Jugendbereich haben wir eine Katholische Schule überprüft. Die Überprüfung in der Schule fand anlasslos statt.

Kurz aus dem Inhalt der Überprüfung:

Arbeitsumgebung der Schulleitung

In diesem Punkt wurden die grundlegenden Erfordernisse, die sich aus dem KDG ergeben, überprüft, wie u.a. das Vorliegen von

- Datenschutzkonzepten, Verzeichnissen von Verarbeitungstätigkeiten
- Merkblättern zum Datenschutz mit Regelungen zu „Auskunftsersuchen“ und „Meldung von Datenpannen“
- Verpflichtungserklärungen gem. § 5 KDG
- Bestellung betrieblicher Datenschutzbeauftragter
- Durchführung von Schulungs- oder Sensibilisierungsmaßnahmen

In der Schule bzw. beim Schulträger sind alle erforderlichen Unterlagen vorhanden und können von den Lehrenden im Intranet eingesehen werden.

Platzvergabe / Anmeldeverfahren

Geprüft wurde, welche personenbezogenen Daten für die Anmeldung und ggf. die Warteliste erforderlich sind und welche dieser personenbezogenen Daten in die Schülerakte übernommen werden müssen.

Einige Daten wie beispielsweise die Angaben zur Krankenkasse und Geburtsdaten der Sorgeberechtigten sahen wir nicht als erforderlich an. Die Verantwortliche hat zugesagt, diese Daten zukünftig nicht mehr zu erfassen. Da sich die Schule bewusst für eine soziale Durchmischung einsetzt, ist u.a. die als freiwillig gekennzeichnete Abfrage nach dem Beruf der Eltern statthaft.

Wir haben der Schule empfohlen den Wortlaut „Angaben zur Mutter“ und „Angaben zum Vater“ in „Sorgeberechtigter 1“ und „Sorgeberechtigter 2“ zu ändern. Diese Änderung ist erforderlich, da Kinder auch gleichgeschlechtliche Paare als Erziehungsberechtigte haben können.

Arbeitsumgebung der Lehrkräfte

In der Einrichtung werden die Klassen- und Kursbücher digital geführt. Dieses Verfahren gewährt mehr Datenschutz, soweit die jeweiligen Lehrenden nur Einsicht in die von ihnen unterrichteten Fächer haben.

Zudem nutzt die Schule digitale Anwendungen wie Lernplattformen, Bibliothekssoftware, Schul-Apps und weitere Cloudlösungen. Für alle digitalen Dienstleistungen sind Auftragsdatenverarbeitungsverträge abgeschlossen. Zudem ist die Dauer der Datenspeicherung bei jeder Anwendung je nach Zweck begrenzt.

Fotos / Webseite

Das zum Zeitpunkt der Überprüfung verwendete Einwilligungsformular für Fotos enthielt keine Auswahlmöglichkeit für die Zwecke, zu denen die erstellten Fotos verwendet werden sollten. Der Schulträger gab an, dass dieses Formular gerade überarbeitet wird und nahm sich u.a. diesem Kritikpunkt an.

Die Webseite der Einrichtung wurde von unserem IT-Referat im Vorfeld überprüft und die Ergebnisse mitgeteilt. Die Überprüfung ergab, dass noch „alte“ Bilddateien auffindbar waren, die zwar nicht mehr verlinkt, jedoch noch im Content (Inhalt) der Webseite vorhanden sind.
Die Verantwortliche hatte die Datenschutzerklärung für ihre Webseite in einem PDF-Dokument gespeichert, welche erst durch Öffnen einer neuen

Seite für den Webseitenbesucher zu erfassen war. Dieses halten wir nicht für ausreichend und haben den Verantwortlichen aufgefordert, die Datenschutzerklärung auf einer Unterseite der Webseite abzugeben und von anderen Bereichen, z.B. dem Kontaktformular, darauf zu verlinken.

Fazit:

Insgesamt verlief die Prüfung in der Katholischen Schule positiv. Die Verantwortliche hat zugesagt, die verbesserungswürdigen Punkte aufzugreifen und umzusetzen.

3.1.2 Datenschutzüberprüfung von Mitarbeitervertretungen

In diesem Berichtszeitraum haben wir damit begonnen Mitarbeitervertretungen (MAV) von Einrichtungen anlasslos zu prüfen. Die Prüfung wird im Jahr 2026 fortgeführt. Vorort-Prüfungen werden generell angemeldet.

Geprüft wurden und werden die datenschutzrechtlich relevanten Abläufe der Arbeit der Mitarbeitervertretungen.

Inhalte einer Vorort-Prüfung einer Caritas MAV

1. Datenschutzkonzept und Verzeichnis von Verarbeitungsvorgängen (VVT)

Teilweise konnte von einzelnen MAV-Mitgliedern nicht dargelegt werden, ob ein Datenschutzkonzept, welches Verzeichnisse von Verarbeitungsvorgängen enthält, existiert.

2. Verpflichtungserklärungen gem. § 5 KDG

Angegeben worden ist, dass diese Erklärungen bei Vertragsunterzeichnung mit unterschieben werden. Die musterhaft vorgelegte Erklärung ist nicht zu beanstanden.

3. Aufbewahrung von Unterlagen über Einstellungsverfahren

Im Büro der MAV-Vorsitzenden befindet sich ein abgeschlossener Aktenschrank, in dem sich die Unterlagen der MAV befinden. Das Büro ist

verschlossen. Das Büro wird nicht ausschließlich als MAV-Büro genutzt. In dem Schrank befanden sich einige Ordner, u.a. ein Ordner mit Einstellungsunterlagen aus den Jahren 2017 bis 2021 mit schätzungsweiße ca. 300 Dokumenten. Auf Nachfrage, warum diese Unterlagen immer noch aufbewahrt werden, konnte uns keine Auskunft erteilt werden. Vereinbart wurde jedoch, dass innerhalb der MAV geprüft wird, ob diese Unterlagen noch benötigt werden und wenn ja aus welchem Grund und zu welchem Zweck. Zum Ergebnis dieser Prüfung sollte uns berichtet werden. Angeregt wurde generell festzulegen, wie lange Einstellungsunterlagen aufbewahrt werden müssen und welcher Zweck mit der Aufbewahrung verfolgt wird. Angeregt worden ist ein Löschkonzept zu erstellen.

4. Verbreitung von Unterlagen innerhalb der Mitarbeitervertretung

Die MAV verfügt über eine eigene E-Mail-Adresse. Diese Adresse dient jedoch nur als Verteileradresse, d. h. Bewerbungsunterlagen werden als Anlage über diese Adresse an die Mitglieder der MAV (9 Mitglieder) unverschlüsselt versandt. Über die Einstellung entscheiden jedoch lediglich 5 Mitglieder (Mitglieder des Ausschusses). Nicht geregelt ist, wie mit diesen Unterlagen nach Abschluss des Einstellungsverfahrens zu verfahren ist (Löschung aus dem E-Mailpostfach der Mitglieder, Löschung aus dem E-Mail-Konto der MAV und aus den gesendeten Nachrichten). Nach Angabe des anwesenden MAV-Mitgliedes löscht er selbst diese nach ca. einem Jahr. Wie die anderen MAV-Mitglieder dies handhaben, war ihm nicht bekannt.

Angegeben wurde, dass die Versendung über eine verschlüsselte ZIP-Datei von den Mitgliedern der MAV als zu umständlich (Entschlüsselung) angesehen wurde. Ein Zugriff über eine VPN-Verbindung auf das E-Mail-Postfach der MAV sei von der IT-Technik mit dem Argument, der Aufwand sei zu hoch, abgelehnt worden.

Der Versandt von Unterlagen (Bewerbungen/Einstellungen/Eingruppierungen etc.) erfolgt auch über die Hauspost im verschlossenen Umschlag. Die Postbox ist jedoch nicht verschlossen und für jeden im Haus zugänglich. Ein abschließbarer Briefkasten für die MAV existiert nicht.

Entscheidungen der MAV werden unverschlüsselt per E-Mail an die Geschäftsführung des Caritasverbandes gesandt. Unterlagen werden zudem ausgedruckt und in Papierform aufbewahrt. Über den Zweck der Datenspeicherung und die Aufbewahrungsdauer konnten keine Angaben gemacht werden.

5. Datenschutzschulung der Mitarbeiter

Aus den Angaben der anwesenden MAV-Mitglieder ergab sich der Eindruck, dass regelmäßige Schulungen der Mitarbeiter und auch der Mitglieder der MAV auf die Einhaltung des Datenschutzes nicht stattfinden.

6. Führungszeugnisse

Seitens der anwesenden MAV-Mitglieder konnten keine Angaben zum Umgang mit Führungszeugnissen getätigt werden. Klar war, dass diese bei Einstellung vorzulegen sind. Eine Aussage dazu, ob eine reine Vorlage ausreichend ist oder ob diese im Original oder in Kopie zur Personalakte genommen werden, konnte uns nicht gegeben werden.

7. Ergebnis/Auflagen

Im Ergebnis war die Prüfung nicht zufriedenstellend. Angeordnet wurde, dass folgende Unterlagen nachzureichen bzw. zu erstellen und vorzulegen sind:

- das Verfahrensverzeichnis der MAV,
- das Datenschutzkonzept der MAV,
- eine Erklärung bzw. eine Erläuterung der Aufbewahrung der Bewerbungsunterlagen, insbesondere der Unterlagen für den Zeitraum 2017 bis 2021 (Zweck der Aufbewahrung),
- Benennung von Löschfristen für Einstellungsunterlagen (Zustimmungserklärungen der MAV etc.),
- Erstellung eines Löschkonzeptes für Einstellungsunterlagen bzw. Unterlagen, die Verfahren betreffen, die der Mitbestimmung der MAV bedürfen.

Die Unterlagen wurden fristgerecht erstellt und der KDSA Ost vorgelegt.

Fragenkatalog einer schriftlichen Überprüfung einer Krankenhaus-MAV

Eine weitere Prüfung einer Krankenhaus-MAV haben wir schriftlich vorgenommen und Folgendes gefragt:

- Besteht ein Datenschutzkonzept oder Verzeichnis von Verarbeitungstätigkeiten und ist dies den MAV-Mitgliedern bekannt? Um Übersendung wurde gebeten.
- Wie wird die MAV vom Dienstgeber im Fall der Beteiligung zu personellen Einzelmaßnahmen unterrichtet (analog per Brief oder per E-Mail)?
- Wer ist Adressat der Unterlagen gem. § 14 Abs. 1 a. E. MAVO (der/die Vorsitzende oder Stellvertretende oder weitere Mitglieder)?
- Werden Unterlagen verschlüsselt per E-Mail versandt?
- Werden vom Empfänger der Daten im Beteiligungsverfahren Kopien für andere oder alle MAV-Mitglieder erstellt oder wird im Falle der Information per E-Mail den weiteren Mitgliedern die E-Mail weitergeleitet?
- Werden Kopien der Unterlagen aus dem Beteiligungsverfahren bei der MAV in Kopie gespeichert (egal ob analog oder digital)?
- Wenn die MAV über Kopien der personenbezogenen Daten aus dem Beteiligungsverfahren verfügt, wann werden diese gelöscht?
- Wie ist sichergestellt, dass im Falle der Geltendmachung eines Auskunftsanspruches gem. § 17 KDG auch die personenbezogenen Daten, die sich bei der MAV befinden, beauskunftet werden?
- Haben alle MAV-Mitglieder eine Verpflichtungserklärung gem. § 5 KDG abgegeben?

Die Beantwortung der Fragen erfolgte zeitnah durch den Datenschutzbeauftragten der Einrichtung und gab keinen Anlass zu weiteren Nachfragen oder zum Tätigwerden. Der Datenschutz in der MAV wird umgesetzt.

Vorort Prüfung einer Krankenhaus-MAV

Positiv verlief eine Vorort Prüfung einer Krankenhaus MAV, da datenschutzkonforme Abläufe etabliert sind.

Für den Datentransfer vom Dienstgeber zur MAV wird für jede Sitzung ein eigener digitaler Ordner angelegt. Dort stellt der Dienstgeber seine Anträge zum Sitzungstermin ein. Nach absolvierter Sitzung legt die Mitarbeitervertretung ihre Beschlüsse in diesem Ordner ab.

Vorsitzende/r, Stellvertreter/in und Schriftführer/in der MAV und der Dienstgeber haben die Berechtigungsstufe „Kann bearbeiten", die weiteren MAV-Mitglieder haben nur die Berechtigung „Download nicht möglich" (entspricht nur Leserechte). Damit ist sichergestellt, dass alle MAV-Mitglieder in Vorbereitung auf die Sitzung bereits alle Anträge des Dienstgebers lesen können. Im Bedarfsfall wird die Berechtigung individuell für eine Sitzung geändert. Trotzdem werden alle Punkte in der Sitzung im Gremium besprochen. Die MAV-Mitglieder können die Anträge des Dienstgebers in der Sitzung am Bildschirm lesen.

Für die Datenübermittlung der MAV untereinander wird ebenfalls für jede Sitzung ein eigener digitaler Ordner angelegt. Hier werden Einladung, Tagesordnung, Protokoll und weiter Unterlagen in Vorbereitung auf die Sitzung abgelegt.

Auch für diesen Ordner haben nur Vorsitzende, Stellvertreter und Schriftführer der MAV Schreibrechte. Die anderen MAV-Mitglieder verfügen nur über die Berechtigung „Download nicht möglich", können also die jeweiligen Dateien weder verändern noch herunterladen.

Wünschen MAV-Mitglieder bestimmte Themen in die Tagesordnung aufzunehmen, werden diese Themen per E-Mail an den/die Vorsitzende bzw. Stellvertreter geschickt und von diesen dann in dem Ordner ablegt bzw. in die Tagesordnung aufgenommen. So ist sichergestellt, dass alle MAV-Mitglieder in Vorbereitung auf die Sitzung den gleichen Wissenstand haben und sich vorbereiten können. Alle Punkte werden in der Sitzung gemeinsam am Bildschirm besprochen. Die MAV-Mitglieder haben dadurch die Möglichkeit auch im Nachhinein Unterlagen einzusehen (Berechtigungen können bedarfsgerecht vergeben werden). Schriftstücke, die in Papierform an die MAV gesendet wurden, werden eingescannt und in dem entsprechenden Ordner abgelegt.

Durch dieses Verfahren ist gewährleistet, dass ausschließlich die Dienstgeberin als auch MAV-Vorsitzende über die personenbezogenen Daten verfügen.

Weiterhin haben sich die Parteien auf kurze Löschungsfristen geeinigt, sodass personenbezogene Daten der Beschäftigten nicht über den erforderlichen Zweck hinaus bei der Mitarbeitervertretung verbleiben.

3.2 Datenschutzvorfälle – Auskunftsersuchen

Der Auskunftsanspruch ist eines der zentralen Betroffenenrechte des KDG und der DS-GVO. Jedermann hat das Recht, von Verantwortlichen zu erfahren, ob ihn betreffende personenbezogene Daten beim Verantwortlichen verarbeitet werden (§ 17 KDG).

Wird der Auskunftsanspruch gegenüber Verantwortlichen geltend gemacht, kommt es bei diesen häufig zu Fehlern in der Bearbeitung dieser Anträge.

Die Beschwerden wegen nicht erteilter, zu spät erteilter oder unvollständig erteilter Auskünfte reißen auch 2025 nicht ab. Immer wieder passiert es, dass Verantwortliche Auskunftsersuchende vertrösten oder erst gar nicht wahrnehmen, dass es sich um ein Auskunftsersuchen handelt. Wir haben bereits mehrfach über die Folgen dieses Handelns berichtet[43] sowie auch den Umfang von Auskunftsersuchen besprochen.[44]

3.2.1 Wann ist ein Auskunftsanspruch erfüllt?

Ein Betroffener stellte per E-Mail gegenüber einem Verantwortlichen einen Auskunftsanspruch. Der Verantwortliche betreibt eine Gemeinschaftsunterkunft dessen Bewohner der Betroffene ist. Die Auskunft wurde dem Betroffenen innerhalb einer Woche per E-Mail zugesendet. Dabei befand sich die Auskunft selber in einem verschlüsselten Anhang. Der Betroffene wurde darüber informiert, dass das Passwort zum Öffnen der verschlüsselten An-

43 KDSA, TB 2024, Pkt. 1.2.4 Schadenersatz wegen verspäteter Auskunft & Pkt. 4.3.2 Beschwerden wegen fehlender oder verspäteter Erfüllung von Auskunftsersuchen
KDSA, TB 2023, Pkt. 3.5.2 Keine Auskunft unter dieser Nummer & Pkt. 4.2 Beschwerden wegen fehlender oder verspäteter Erfüllung von Auskunftsersuchen

44 KDSA, TB 2024, Pkt. 1.2.3 Neues zum Auskunftsrecht

hänge in einem verschlossenen Umschlag für ihn in der Verwaltung (Büro im selben Gebäude) hinterlegt sei und er sich dieses dort während der Büroöffnungszeiten abholen könne. Nachdem der Betroffene den Umschlag nicht abgeholt hat, händigte der Verantwortliche ihm den Umschlag noch innerhalb der Monatsfrist persönlich aus, nachdem sich dieser bei unserer Aufsicht beschwert hatte und wir den Verantwortlichen darauf hingewiesen hatten, dass die Auskunft gem. § 14 KDG unverzüglich, in jedem Fall aber innerhalb eines Monats zur Verfügung zu stellen ist.

Die Form der Auskunft ist im KDG nicht explizit festgeschrieben. Erwägungsgrund 58 zur DS-GVO legt aber fest: „Der Grundsatz der Transparenz setzt voraus, dass eine für die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich zu erteilen ist". Da die Regelungen der DS-GVO und die Regelungen im KDG in diesem Punkt identisch sind, ist auch die Auslegungshilfe im Erwägungsgrund auf die Formulierung im KDG anzuwenden.

Das Kriterium „leicht zugänglich" bezieht sich sowohl auf den Inhalt als auch auf die Form. Es sollen keine Hürden aufgestellt werden, vielmehr soll der Betroffenen die Information mit den ihm zur Verfügung stehenden Mitteln erreichen können.[45] Sie muss ohne wesentliche Mitwirkung des Betroffenen wahrnehmbar sein.[46]

Die Voraussetzung lag im dargestellten Fall nicht vor.

Zunächst war die dem Betroffenen zu erteilende Auskunft für diesen nicht zugänglich, mithin also nicht zugegangen. Eine Auskunft ist zugegangen, wenn unter regelmäßigen Umständen eine Kenntnisnahme zu erwarten ist. Zwar hat die E-Mail den Betroffenen erreicht, aber der Verantwortliche wusste, das eine Kenntnisnahme erst nach Bekanntwerden des Passwortes erfolgen konnte. Wird das Passwort schriftlich mitgeteilt, muss diese Mitteilung der betroffenen Person physisch zugänglich sein.[47]

Wenn der Betroffenen gezwungen ist, erst Räume des Verantwortlichen aufzusuchen, um an das Passwort zu gelangen, ist die Mitteilung nicht in

45 Paal, in: Paal/Pauly DSGVO Artikel 12 Rn. 32
46 Quaas, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg Art. 12 Rn. 16
47 Heckmann/Paschke, in: Ehmann/Selmayr DS-GVO Art. 12 Rn. 14

seinen Machtbereich gelangt und ihm deshalb auch nicht zugegangen. Mutmaßungen darüber, ob dem Betroffenen eine Abholung zumutbar gewesen wäre, erübrigen sich, da sie von einer Wertung des Verantwortlichen abhängen, die der Forderung nach leichter Zugänglichkeit widersprechen.

Im zu beurteilenden Fall hat der Verantwortliche durch sein Handeln zunächst zu erkennen gegeben, dass eine Auskunftserteilung innerhalb einer Woche möglich gewesen ist. Dadurch ist der Zeitraum der Unverzüglichkeit bestimmt worden, die im Gesetz benannte Höchstfrist von einem Monat kommt deshalb nicht zum Tragen.

Durch die spätere persönliche Übergabe des Passwortes hat der Verantwortliche darüber hinaus belegt, dass es ihm möglich und zumutbar war, den Betroffenen in die Lage zu versetzen, die Auskunft zur Kenntnis zu nehmen.

Da das Passwort erst einen Monat nach dem Zugang des Auskunftsantrages dem Betroffenen zugegangen ist und eine Kenntnisnahme erst zu diesem Zeitpunkt erfolgen konnte, liegt hier ein Datenschutzverstoß vor. Dieser Verstoß wurde von uns förmlich durch Bescheid festgestellt.

Wir verweisen zum Umgang mit Auskunftsersuchen auf unsere Handlungsanleitung zum Erfüllen von Auskunftsersuchen im Anhang dieses Berichtes.

3.2.2 Auskunftsersuchen ignoriert – Bußgeld kassiert I

Eine betroffene Person begehrte von einer Einrichtung Videoaufnahmen zu einem Verkehrsunfall (siehe auch Pkt. 3.3.2 in diesem Bericht), in dem diese verwickelt war. Die Videoaufnahmen enthielten, da der Petent gefilmt wurde, seine personenbezogenen Daten (KFZ-Kennzeichen, Personenaufnahmen). Zudem hatte die Einrichtung seine Kontaktdaten, um sich bezüglich des Unfalls mit ihm auszutauschen.

Etliche Versuche des Petenten sowie auch der Datenschutzaufsicht die Einrichtung zur unverzüglichen Beantwortung des Auskunftsersuchens zu bewegen schlugen fehl. Darüber hinaus verlief die anfängliche Zusammenar-

beit mit der Einrichtung alles andere als bereitwillig. Erst nach mehrfachem Intervenieren und nach mehr als 15 Monaten erteilte die Einrichtung die begehrte Auskunft. Die Videoaufnahmen gab es nicht mehr, da diese bereits gelöscht waren.

Unsere Behörde hat das Verhalten des Verantwortlichen als Verstoß gegen § 17 Abs. 1 i. V. m. § 14 Abs. 3 KDG bewertet. Aufgrund des nicht unerheblichen Verstoßes, der mehrfachen Hinweise und insgesamt verspäteter Reaktion wurde gegenüber dem Verantwortlichen ein Bußgeld im vierstelligen Bereich verhängt.

Fazit:

Auskunftsersuchen, die ignoriert oder verspätet bearbeitet werden, sind bußgeldbewährt. In diesem und im Fall unter Pkt. 4.2.3 zeigte sich: erst nach Hinweisen und intervenierender Aufsicht wurden die Anfragen schließlich erfüllt.

Auskunftsersuchen müssen zeitnah, vollständig und nachvollziehbar beantwortet werden, unabhängig von organisatorischen oder qualitätsmanagementbezogenen Gründen.

3.3 Datenschutzvorfälle - Videoüberwachung

3.3.1 Videoüberwachung von Bereichen in Krankenhäusern

Zahlreiche Meldungen in der Presse von Belästigungen und Handgreiflichkeiten durch Patienten haben in vielen Krankenhäusern dazu geführt Sicherheitsdienste mit der Bewachung von öffentlich zugänglichen Räumen zu beauftragen. Häufig ist aber festzustellen, dass Krankenhäuser die damit verbundenen Kosten sparen wollen und auf den deutlich billigeren Einsatz von Videoelektronik setzen.

Aus datenschutzrechtlicher Sicht ist fraglich, ob und wo solche Systeme in einem Krankenhaus datenschutzkonform verwendet werden dürfen. Die Voraussetzungen zur Zulässigkeit von Videoüberwachungen haben wir unter Pkt. 2.2 in diesem Bericht dargelegt.

a.) Kamera im Behandlungsraum

Ein Petent beschwerte sich bei uns über ein Krankenhaus. Der Petent suchte dieses mit seinem Sohn auf, um ein akutes medizinisches Problem abklären zu lassen. Nachdem der Petent mit seinem Sohn zunächst im Wartezimmer gewartet hatte, wurde er zur Untersuchung in den Kurzliegebereich der Notaufnahme gebeten. Der Sohn musste sich dort für die ärztliche Untersuchung entkleiden. In diesem Behandlungsraum entdeckte der Petent an der Decke eine Videokamera in Form einer Domekamera. Ein Schild an der Wand wies auf den Umstand der Videoüberwachung hin. Der Petent vertrat die Ansicht, in einem derart sensiblen Bereich eines Krankenhauses sei eine Videoüberwachung unangemessen.

Zur Untersuchung der Beschwerde haben wir uns in dem Krankenhaus zu einem Vorort-Termin angemeldet, um die Gesamtsituation in Augenschein zu nehmen. Dabei haben wir den Verantwortlichen aufgefordert, uns bereits vorab auf einer Skizze zu erläutern, wo die Videokameras angebracht sind und wo sich die Monitore befinden bzw. ob eine Aufzeichnung der Bilder stattfindet.

Die Situation stellte sich so dar, wie von dem Petenten geschildert. Vom Verantwortlichen wurde zur Begründung der Installation die Überwachung instabiler Liegend-Patienten angeführt. Wir konnten uns aber bei einem Blick auf den Monitor davon überzeugen, dass diese Funktion gar nicht umsetzbar war, da die Entfernung zu groß war, um die Patienten diesbezüglich zu beobachten.

Wir haben angewiesen, die Kameras aufgrund der besonderen Sensibilität und Persönlichkeitssphäre in einem Behandlungszimmer umgehend abzuschalten. Darüber hinaus haben wir dem Verantwortlichen dringend geraten, die Kameras auch abzubauen. An dieser Stelle kam dann plötzlich der wahre Grund zur Sprache, als der Justiziar dem widersprach und meinte, eine abgestellte Kamera könne ja immer noch zur Abschreckung dienen. Wenn die Kameras tatsächlich der Überwachung instabiler Liegend-Patienten hätte dienen sollen, wäre nicht verständlich, wofür eine Abschreckung erforderlich sein sollte. Nach diesem Fauxpas haben wir uns dann darauf geeinigt, dass die Kameras umgehend beseitigt werden.

b) Wartebereich der Anmeldung

Bei dieser Vorort-Prüfung wurde ferner festgestellt, dass der Wartebereich der Anmeldung per Videotechnik überwacht wird. Nach der Darstellung des Verantwortlichen dient die Videoüberwachung in diesem Bereich dem Schutz der Beschäftigten sowie dem Schutz der Patienten, wenn die Anmeldung nicht besetzt ist.

Besucher bzw. Patienten müssen eine mit einem Mitarbeiter besetzte Anmeldung passieren, um in die hinter der Anmeldung liegenden Warteräume zu gelangen.

Vor der Eingangstür befindet sich zudem eine Säule, an der eine Klingel und eine sogenannte Klingelkamera angebracht sind. Wenn die Anmeldung nicht besetzt ist, müssen Personen, die Einlass in das Krankenhaus begehren, die Klingel betätigen. Durch die Kamera sieht der Mitarbeiter wer Einlass begehrt und kann die Tür öffnen.

Es handelt sich bei den Wartebereichen mithin nicht um öffentlich zugängliche Räume (zur Unterscheidung zwischen öffentlichen und nicht öffentlichen Bereich haben wir bereits unter Pkt. 2.2 ausgeführt).

Als Rechtsgrundlage für die Datenverarbeitung kann das berechtigte Interesse des Verantwortlichen nach § 6 Abs. 1 lit. g) KDG, beispielsweise der Schutz vor Straftaten, in Betracht kommen.

Es genügt jedoch nicht, dass der Verantwortliche behauptet, die Videoüberwachung sei aus Sicherheitsgründen erforderlich. Vielmehr muss diese Behauptung durch konkrete Vorfälle belegt werden können.

Angeführt wurde, dass Patienten häufig von einer größeren Zahl von Angehörigen begleitet würden, konkrete Gefährdungen konnten jedoch nicht benannt werden. Strafanzeigen sind nicht erstattet worden. Aufgrund der bestehenden Einlasskontrollen erschien nicht ersichtlich, warum zudem noch eine Videoüberwachung erforderlich sein soll. Personen, von denen vermutet wird, dass von Ihnen eine Gefährdung ausgeht oder denen ein berechtigtes Interesse am Besuch der Einrichtung abgesprochen wird, können bereits an der Eingangskontrolle zurückgewiesen werden.

Eine pauschale, phrasenhafte Behauptung von Sicherheitsgründen reicht nicht aus, um den Betrieb einer Videoanlage zu rechtfertigen.

Eine nicht erforderliche Videoüberwachung ist immer unzulässig. Dem Verantwortlichen wurde daher die Auflage erteilt, die Kameras im Wartebereich abzuschalten. Es erging ein dementsprechender Bescheid.

3.3.2 Videoüberwachung im Eingangsbereich einer Einrichtung und des davor befindlichen Straßenraumes

Ein Verantwortlicher installierte zur Überwachung seines Grundstücks eine Videokamera. Diese erfasste den Zugangsbereich des Grundstücks, aber auch die vor dem Grundstück verlaufende öffentliche Straße.

Zum Hinweis auf diese Überwachung war neben dem Klingelschild der Einrichtung ein Aufkleber angebracht, der eine Videokamera abbildete.

An einem Tag kam es zu einem Verkehrsunfall vor der Einrichtung. Ein Beschäftigter kollidierte mit seinem Fahrzeug mit dem Fahrzeug eines Verkehrsteilnehmers, der die öffentliche Straße benutzte.

In der Folge kam es zum Streit zwischen den Unfallbeteiligten über die Schuldfrage. Der Beschäftigte verschaffte sich daraufhin Zugang zu den Videoaufzeichnungen des Verantwortlichen und leitete diese an seine Kraftfahrzeugversicherung weiter.

Eine Videoüberwachung greift in das allgemeine Persönlichkeitsrecht der Betroffenen in seiner Ausprägung als Recht der informationellen Selbstbestimmung ein; dieses Recht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen.[48]

Jeder Eigentümer hat das Recht, sein Grundstück mit Hilfe von Videokameras zu überwachen. Das bezieht sich jedoch ausschließlich auf eine

48 BVerfGE 65, 1, 42 f.; 67, 100, 143; BVerfG, NVwZ 2007, 688 ff.; NJW 2009, 3293 f.

Überwachung innerhalb der Grenzen dieses eigenen Grundstücks. Bei der Installation von Anlagen der Videoüberwachung auf einem Privatgrundstück muss deshalb sichergestellt sein, dass weder der angrenzende öffentliche Bereich noch benachbarte Privatgrundstücke oder der gemeinsame Zugang zu diesen von den Kameras erfasst werden. Eine Begrenzung des Erfassungsbereiches von Kameras auf das eigene Grundstück ist am zuverlässigsten mit fest installierten Kameras umzusetzen. Eine dreh- oder schwenkbare Kamera (Dome-Kamera) kann jederzeit anders ausgerichtet werden und andere Grundstücke oder öffentliche Bereiche erfassen. Das allein kann im Einzelfall zu Unterlassungsansprüchen von Nachbarn oder anderen Betroffenen führen.

Eine Videoüberwachung über die Grundstücksgrenzen hinaus ist regelmäßig unzulässig!

a) Überwachung des privaten Bereichs (Eingangsbereich/Vorgarten)

Der Eingangsbereich zum Objekt war nicht öffentlich zugänglich, da die Tür zum Vorgarten verschlossen war. Die Überwachung wurde mit dem besonderen Status der Einrichtung und mit kritischen Auftritten von Eltern der betreuten Kinder und Jugendlichen begründet. Eine Erforderlichkeit der Überwachung war nicht gegeben, da das festgelegte Ziel mit der Überwachung tatsächlich nicht erreicht werden kann und durch eine Videoaufzeichnung ein unberechtigtes Betreten des Gebäudes nicht verhindert werden kann. Die Videoüberwachung war mithin rechtswidrig. Vom Verantwortlichen wurde eingeräumt, dass die zunächst angeführten Gründe nicht mehr zutrafen und die Kamera hätte bereits abgebaut sein müssen.

b) Überwachung des öffentlichen Verkehrsraumes und Aufzeichnung des Unfalls

Eine permanente anlasslose Videoüberwachung des öffentlichen Raums (öffentlichen Straßen, Gehwegen und Plätzen) auch zu präventiven Zwecken durch Private (Kamera am Haus) ist, wie bereits ausgeführt, generell unzulässig.

Der Verantwortliche konnte keine Erforderlichkeit für eine Überwachung des öffentlichen Raumes darlegen. Hinzu kam, dass der Verantwortlichen

erklärt hat, an der Überwachung des öffentlichen Verkehrsraumes besteht kein Interesse. Da die Überwachung des öffentlichen Verkehrsraumes unzulässig war, war auch die Aufzeichnung des Unfalles unzulässig.

Zudem entsprach die Anbringung des Aufklebers, der auf eine Videoüberwachung hinweisen sollte, nicht den Mindestanforderungen. Der Verantwortliche hatte auch keine Maßnahmen getroffen, die einen Zugriff auf personenbezogene Daten durch unautorisierte Personen verhindern konnten. Auch entsprechende Belehrungen des Personals waren nicht vorhanden.

Die Verstöße gegen das KDG wurden förmlich durch Bescheid beanstandet.

3.3.3 Videoüberwachung im Jugendraum

Das Thema Videoüberwachung zieht sich in diesem Berichtsjahr durch alle Facetten. Bei nicht öffentlich zugänglichen Räumen, wie z.B. einen Jugendraum in einer Pfarrei, fallen die installierten Kameras jedoch nicht in den Anwendungsbereich von § 52 KDG (Videoüberwachung öffentlich zugänglicher Räume), sondern in die Rechtmäßigkeit der Verarbeitung personenbezogener Daten (§ 6 Abs. 1 KDG).

So war nach einer Beschwerde eines Pfarreimitgliedes abzuwägen, ob die Videokamera, welche im Jugendraum angebracht ist, rechtmäßig ist oder nicht.

Die Kamera, so wurde uns mitgeteilt, wurde in Folge diverser Eigentumsdelikte von den Jugendlichen selbst installiert. Folgende Spielregeln legte der Jugendseelsorger zusammen mit den Jugendlichen fest:

- Zugriff und Pflege der Kamera übernimmt der volljährige Jugendsprecher.
- Die Aufnahmen werden nach 72 h durch Überschreiben gelöscht.
- Sobald sich Personen erlaubter Weise in dem Raum aufhalten, wird die Kamera abgeschaltet.
- Sind auf den Aufnahmen außerhalb der Öffnungszeiten des Raumes Personen zu erkennen, ist der Jugendseelsorger zu informieren.

- Sollte das Problem (Diebstahl) gelöst sein, sind alle Aufnahmen zu löschen.

Für die Datenschutzaufsicht war die einzige infrage kommende Zulässigkeitsvorschrift § 6 Abs. 1 lit. g) KDG, das berechtigte Interesse des Verantwortlichen. Die schutzwürdigen Interessen der Jugendlichen oder anderen standen dem nicht entgegen, da die Kamera abgeschaltet worden ist, sobald sich Personen im Raum aufhielten. Da es jedoch wiederholt zu nicht unerheblichen Eigentumsdelikten im Jugendraum gekommen ist, erfolgte die Installation der Videokamera verdachtsbezogen und sollte dem Schutz des Eigentums dienen. Nach Prüfung des Sachverhalts haben wir festgestellt, dass diese Datenverarbeitung rechtmäßig ist und keinen Datenschutzverstoß darstellt.

Im Weiteren war die Kamera ausgeschaltet sobald sich die Jugendlichen im Raum aufgehalten haben. Da somit faktisch keine Aufnahme außerhalb des verfolgten Zwecks erfolgt, werden auch keine personenbezogenen Daten verarbeitet und es kann in Folge keine Datenschutzverletzung eintreten.

Kurz nach Inbetriebnahme der Kamera konnte eine Person überführt werden, die etwas aus diesem Raum entwendet hat. Über den Kirchenvorstand sind dann weitere Konsequenzen erfolgt, die Aufnahmen wurden gelöscht und die Kameras wieder deinstalliert.

Während dieses Vorgehen keinen Anlass zur Beanstandung gab, gab es jedoch einen „Nebenschauplatz“, der zwar nicht direkt dem verantwortlichen Kirchenvorstand angelastet werden konnte, aber trotzdem beanstandet worden ist. So wurden die Aufnahmen des mutmaßlichen Täters entgegen der festgelegten Spielregeln an einen privaten Chat der Jugendlichen geleitet. Auch wenn die Weitergabe der Aufnahmen nur im Interesse der Jugendlichen war, dass jetzt ein „Täter festgestellt werden konnte“ liegt hierhin ein Verstoß gegen das KDG. Der Weitergabe hätte es nicht bedurft.

3.4 Datenschutzvorfälle – Offene E-Mailverteiler

Wie jedes Jahr wurden uns auch im zurückliegenden Berichtszeitraum Datenpannen gemeldet, bei denen ein offener E-Mailverteiler ursächlich war. Damit bleibt es auch im vergangenen Berichtszeitraum beim Dauerbrenner

Nr. 1 der Datenpannen. Die Verstöße betreffen eine große Bandbreite unserer Einrichtungen, wie Krankenhäuser, Kindertagesstätten, Schulen, aber auch Pfarrgemeinden. Obwohl wir häufig, insbesondere auf unserer Homepage und in unseren Tätigkeitsberichten darauf hinweisen, keine offenen E-Mailverteiler zu verwenden, passieren diese Fehler immer wieder.

So hatte z. B. eine FSJlerin einer Pfarrei die Online-Ausgabe des Pfarrbriefes in einem offenen-Verteiler verschickt. Insgesamt waren ca. 215 E-Mail-Adressen in dem Verteiler. Eine Kunsttherapeutin einer Klinik hatte Patienten und Patientinnen, die aufgrund einer psychischen Erkrankung eine Kreativtherapie erhielten, E-Mails im offenen Verteiler versandt. Es handelte sich jeweils um Einladungen zu Veranstaltungen. Betroffen waren 63 Datensätze. In einem weiteren Fall hat eine Sozialarbeiterin Bewohner einer Gemeinschaftsunterkunft per E-Mail kontaktiert. Die E-Mail wurde im offenen Verteiler an 47 Empfänger versandt.

Das Verwenden des offenen Verteilers ist in den meisten Fällen nicht erforderlich. Regelmäßig stellen wir bei derartigen Vorfällen ein Datenschutzverstoß förmlich durch Bescheid fest.

Auch wenn derartige Verstöße geeignet wären eine Geldbuße zu verhängen, wie z. B. im Fall der Versendung des Pfarrbriefes über einen offenen Verteiler an eine Vielzahl von Adressaten, ist gem. § 51 Abs. 6 KDG die Verhängung von Geldbußen gegen kirchliche Stellen im Sinne des § 3 Abs. 1 KDG, soweit sie im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind, nicht möglich.

4 Datenschutz im Gesundheitswesen

4.1 Neuregelung zum Datenschutz im Krankenhausgesetzes Berlin

In § 24 Abs. 7 Landeskrankenhausgesetz (LKHG) wurde eine Regelung aufgenommen, nach der die Erteilung eines Auftrages i. S. d. Art. 28 DS-GVO zum Zwecke der Verarbeitung von genetischen Daten und Gesundheitsdaten i. S. d. Art. 9 Abs. 1 DS-GVO nur zulässig ist, wenn der Verantwort-

liche jeweils zum 31. März eines Jahres der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit

a) die Anzahl der im vorangegangenen Kalenderjahr von ihm neu geschlossenen Auftragsdatenverarbeitungsverträge i. S. d. Art. 28 DS-GVO sowie

b) die Anzahl der Personen, von denen im Rahmen dieser neu geschlossenen Verträge zur Auftragsdatenverarbeitung genetische Daten und Gesundheitsdaten i. S. d. Art. 9 Abs. 1 DS-GVO seitdem jeweils verarbeitet wurden,

elektronisch oder schriftlich anzeigt.

In dem Änderungsantrag der Fraktion der CDU und der Fraktion der SPD wird die Vorlagepflicht wie folgt begründet:

Mit der Verpflichtung zur jährlichen Meldung der Anzahl der neu geschlossenen Auftragsdatenverarbeitungsverträge an die Berliner Beauftragte für Datenschutz und Informationsfreiheit und der Übermittlung der betroffenen Personenzahl wird dem Betreiber bewusst, dass ein besonders sorgsamer Umgang mit den zum Teil besonderen personenbezogenen Daten im Sinne von Art. 9 DS-GVO von Nöten ist.

Zudem kann die Berliner Beauftragte für Datenschutz und Informationsfreiheit auf diese Weise bei Meldung besonders auffälliger Zahlen gezielt nachfragen, um Unregelmäßigkeiten nachzugehen.

Dem Geltungsbereich des LKHG unterfallen grundsätzlich auch Krankenhäuser, die sich in Trägerschaft Katholischer Einrichtungen befinden. Über diese Krankenhäuser wird die Datenschutzaufsicht von der KDSA Ost wahrgenommen. Es erscheint an dieser Stelle zweifelhaft, dass über ein Landesgesetz die in der DS-GVO geregelte Zuständigkeit für Datenschutz, insbesondere für die Aufsicht über die Einhaltung des Datenschutzes, abweichend von der europarechtlichen Vorschrift geregelt wird. Aus diesem Grunde haben wir die Landesbeauftragte für Datenschutz Berlin darum gebeten, gemeinsam nach einer Vorgehensweise zu suchen, die dem Gesetzeswortlaut gerecht wird und gleichzeitig die Rechte der kirchlichen Aufsichten wahrt.

In einer Videokonferenz mit Vertreter:innen der Landesbeauftragten für Datenschutz Berlin und der KDSA Ost, zu der auch eine Vertreterin der Datenschutzaufsicht der evangelischen Kirche hinzugezogen wurde, konnte folgende Übereinkunft erzielt werden:

Dem Gesetz ist von den verantwortlichen Krankenhausbetreibern nachzukommen. Die im Gesetz festgelegten Meldepflichten sind gegenüber der Berliner Beauftragten für Datenschutz zu erfüllen.

Sollte die Berliner Beauftragte für Datenschutz „besonders auffällige Zahlen" feststellen, die ein kirchliches Krankenhaus betreffen, wird die zuständige Datenschutzaufsicht der evangelischen oder katholischen Kirche darüber informiert, um entsprechende Nachprüfungen anzustellen.

Mit dieser Vereinbarung wird der Intention des Gesetzes entsprochen und gleichzeitig die Zuständigkeit der jeweiligen Aufsichten gewahrt.

4.2 Datenschutzvorfälle im Gesundheitswesen

Dauerbrenner – Datenschutzepisoden im Klinikalltag

Medizinische Unterlagen enthalten sensibelste Kategorie personenbezogener Daten. Missbrauch kann erhebliche Folgen haben – von Identitätsdiebstahl bis zu Gesundheits- oder Versicherungsnachteilen. Uns wurden im vergangenen Berichtzeitraum zahlreiche Datenpannen gemeldet, von denen wir nachfolgend einige darstellen, ihre Ursachen bewerten und aufzeigen, wie sich die daraus resultierenden Risiken verringern lassen.

4.2.1 Klassischer Fall: Verlust physischer Dokumente

Befunde oder Laborausdrucke oder auch Einverständniserklärungen– in hektischen Situationen landen solche Unterlagen häufig in Kitteltaschen oder auf dem Empfangstresen.

So kam es vor, dass eine Stationsliste im öffentlichen Raum gefunden worden ist. Die Stationsliste enthielte die Vor- und Zunamen, Geburtsdaten und aktuelle Behandlungsdiagnosen. Nach Auskunft des Verantwortlichen

dienen diese Stationslisten als sog. Laufzettel und enthalten häufig wichtige Informationen, wie Notizen der Mitarbeiter über den Patienten.

In einem anderen Fall wurden Unterlagen (Patiententaschen) aus dem Bereich der Notaufnahme entwendet und „tauchten in den Unterlagen" eines Patienten in einem anderen Krankenhaus auf. Der Verantwortliche hat angegeben, dass die Patiententaschen bei der Aufnahme von Patienten in das Krankenhaus angelegt werden. Die Patiententaschen enthalten: Behandlungsvertrag, Angaben zu Namen, Geburtsdatum, Anschrift, Krankenkasse, aber keine Angaben zu Diagnosen.

Es handelt sich dabei um Papierumschläge, die nicht verschlossen sind. Sie werden über den Tag gesammelt und am nächsten Tag dem Patientenmanagement übergeben. Nicht geklärt werden konnte, wie der Patient in den Besitz der Unterlagen gekommen ist, da angegeben worden ist, dass Patienten in der Regel im Anmeldebereich nicht allein gelassen werden.

Bewertung: Hier handelt es sich unter Umständen um organisatorische Defizite. Der Vorfall zeugt davon, dass möglicherweise sichere Ablagen nicht vorhanden oder Prozesse ineffizient sind. Gleichzeitig unterschätzen Mitarbeitende die Verantwortung, die mit Papierdokumenten einhergeht, da in einigen Fällen auch Vorfälle auftraten, obwohl konkrete Anweisungen bestanden.

Der Verantwortliche hat aufgrund des Vorfalles erklärt, künftig die Patiententaschen bis zur Weitergabe in einem verschließbaren Schrank aufzubewahren. Der Verstoß wurde förmlich durch Bescheid festgestellt.

4.2.2 Falsch versandte Patientenunterlagen

Auch im vergangenen Berichtszeiträumen wurden uns wieder Fälle gemeldet, bei denen Entlassungsberichte, Befundberichte, Arztbriefe etc. und Rechnungen falsch versandt worden sind oder sich „fremde" Unterlagen in den Patientenakten befanden. 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.

In den meisten Fällen waren in den Einrichtungen entsprechende Datenschutzunterlagen vorhanden und die Verantwortlichen ihren Verpflichtungen gem. § 26 KDG nachgekommen. Die Verstöße waren in der Regel auf Versäumnisse der Mitarbeitenden zurückzuführen. Dies wurde von den Verantwortlichen zum Anlass genommen die Mitarbeiter auf die Einhaltung der vorhandenen Regelungen zur Herausgabe und Übersendung von Unterlagen, die Gesundheitsdaten enthalten, erneut zu schulen und entsprechend zu sensibilisieren. Diese Vorfälle wurden förmlich durch Bescheid festgestellt.

4.2.3 Auskunftsersuchen ignoriert – Bußgeld kassiert II

Wir mussten auch in diesem Berichtszeitraum feststellen, dass der Umgang mit Auskunftsersuchen nicht mit der erforderlichen Sorgfalt nachgekommen wird. Es kam vermehrt zu Beschwerden von Petenten, die angegeben hatten, ihr Auskunftsersuchen sei nicht, nicht vollständig oder erst verspätet erfüllt worden. Auch in diesem Berichtszeitraum waren nicht alle Beschwerden berechtigt. In einigen Fällen wurden förmliche Beanstandungen ausgesprochen und im folgenden Fall ein Bußgeld verhängt. Die Bescheide sind rechtskräftig.

Ein Patient begehrte in seinem Auskunftsersuchen die Herausgabe seiner Patientenakte nach § 17 KDG (Art. 15 DS-GVO). Zunächst mündlich, später telefonisch und dann schriftlich. Das Auskunftsersuchen wurde zwar von der verantwortlichen Einrichtung als solches erkannt und man nahm mit dem Patienten Kontakt auf, jedoch wollte die Einrichtung die Patientenakte persönlich übergeben, um eventuelle Nachfragen des Patienten zu klären.

Aufgrund organisatorischer Umstände (Personalausfall, Lehrverpflichtungen, Notfalleinsätze), so die Verantwortliche, ist die persönliche Übergabe mehrfach gescheitert. Zwischenzeitlich wurde der Patient an einem anderen Standort weiterbehandelt. Nach 4 Monaten ohne Antwort auf sein Auskunftsersuchen hat sich der Patient bei unserer Dienststelle beschwert.

Erst danach ist die Einrichtung seinem Wunsch nachgekommen und hat das Auskunftsersuchen beantwortet.

Dabei lagen die ausgedruckten Unterlagen des Patienten in der Einrichtung zeitnah vor. Die geplatzten Übergaben hatte man damit begründet, dass diese ausschließlich persönlich erfolgen sollte, um den Patienten im Rahmen des Qualitätsmanagements nach seinen Beweggründen für einen Arztwechsel zu befragen.

Im Sinne des Qualitätsmanagements mag es durchaus richtig sein, nachzufragen, warum der Patient einen Arztwechsel erwogen hat, jedoch dürfen Auskunftsersuchen dem nicht nachstehen und müssen fristgerecht beantwortet werden.

In diesem Fall haben wir einen Verstoß gegen § 17 Abs. 1 i. V. m. § 14 Abs. 3 KDG gegenüber der Einrichtung festgestellt und eine Geldbuße im vierstelligen Bereich verhängt.

4.2.4 Cyberangriffe und Ransomware

Das Gesundheitswesen ist ein attraktives Ziel für Hacker. Ausfälle können lebensbedrohlich sein, weshalb der Druck hoch ist, bei einer Erpressung zu zahlen. Neben Verschlüsselungsangriffen häufen sich auch Datenexfiltrationen, bei denen Angreifer Patientendaten kopieren und drohen, diese zu veröffentlichen.

Hoch problematisch ist es, wenn in Krankenhäusern Netzwerke von Hackern verschlüsselt werden. Vorfälle können zur sofortigen Abmeldung von der Notfallversorgung führen. Ohne Notfallpläne müssen Mitarbeitende auf Papier zurückgreifen, analog diktieren und eventuell sogar Türen mit elektronischen Schlössern ausbauen.

Bewertung: Cyberangriffe sind eine gravierende Bedrohung. Häufig führen veraltete Systeme, fehlende Patches oder unzureichende Netzwerksegmentierung dazu, dass sich Schadsoftware ungehindert ausbreiten kann. Angreifer nutzen außerdem Phishing, um Passwörter zu erbeuten.

Handlungsempfehlungen:

- **Informationssicherheits-Managementsystem (ISMS) einführen:** Ein strukturiertes ISMS gemäß ISO/IEC 27001 hilft, Risiken systematisch zu identifizieren und Gegenmaßnahmen zu entwickeln.

- **Netzwerk segmentieren:** Medizinische Geräte, Verwaltungsrechner und öffentliches WLAN sollten strikt getrennt sein. Zwei-Faktor-Authentifizierung ist Pflicht.
- **Wiederherstellung üben und Offline-Backups:** Regelmäßig Backups offline ablegen und die Wiederherstellung üben, um eventuelle Lösegeldforderungen abzuwehren.
- **Mitarbeiterschulungen gegen Phishing:** Sensibilisierung in Bezug auf E-Mail-Anhänge und Links reduziert das Risiko deutlich.

4.2.5 Neugierige Mitarbeiter

Es wird uns immer wieder mal gemeldet, dass Mitarbeitende die Grenze zwischen beruflicher Nutzung und Privatleben nicht klar ziehen. Die Versuchung, mal eben in Erfahrung zu bringen, warum der Kollege oder die Kollegin immer noch krank ist oder warum er/sie im „eigenen Haus" behandelt worden ist, ist groß, besonders wenn vorgegebene Regeln im Alltag vergessen werden, oder schlimmer noch, gar nicht erst bestehen.

Die Beschäftigten wissen, dass die Daten vertraulich sind, verlieren jedoch manchmal den Zweck der Daten aus den Augen. Dabei geht es nicht immer um Neugier, sondern auch um eine gefährliche Vermischung von Beruflichem und Privatem: Für Beschäftigte gehören sensible Daten zum Alltag und sie unterschätzen leicht die besondere Schutzbedürftigkeit. Eine einmalige Unterweisung reicht nicht aus – nur eine gelebte Struktur, regelmäßige Sensibilisierung und klare Grenzen zwischen dienstlicher und privater Nutzung wirken nachhaltig.

Empfehlungen:

- **Zweckbindung schriftlich fixieren:** Patientenakten dürfen ausschließlich für medizinische Zwecke von den Behandlern eingesehen werden. Dies muss in Dienstanweisungen klar geregelt sein.
- **Zugriffsprotokolle führen:** Jeder Abruf muss protokolliert werden; analoge Akten sollten nur mit Unterschrift einsehbar sein.
- **Sensibilisierung:** Regelmäßige Schulungen helfen, die Konsequenzen von Neugier und Missbrauch zu verdeutlichen.

- **Aktenversiegeln:** Nach Abschluss der Behandlung Akten versiegeln. Akten von behandelten Beschäftigten zusätzlich schützen.

Fazit und Ausblick:

Als Datenschutzaufsicht sehen wir immer wieder, dass menschliches Fehlverhalten und organisatorische Lücken die häufigsten Ursachen für Datenschutzverstöße im Gesundheitsbereich sind. Für Beschäftigte im Gesundheitswesen ist der Umgang mit hochsensiblen Daten Alltag. Dabei kann schnell vergessen werden, wie schutzbedürftig ein Befund oder eine Diagnose sein können. Deshalb gilt: Menschliche Fehler lassen sich nie vollständig ausschließen. Es liegt jedoch in der Verantwortung der Einrichtungen und jedes einzelnen Mitarbeitenden, größtmögliche Sorgfalt walten zu lassen und sensibilisiert zu bleiben.

Das bedeutet:

- **Datenschutz etablieren:** Datenschutz ist kein einmaliges Projekt, sondern Teil der Einrichtungs-DNA. Verantwortliche müssen dies vorleben.
- **Regelmäßige Prüfung der Prozesse:** Regelmäßige Kontrollen decken Schwachstellen auf, bevor sie zu Pannen führen und helfen dabei, Lehren aus Vorfällen zu ziehen.
- **Digitale Transformation aktiv gestalten:** Elektronische Patientenakte, Telemedizin und Cloudlösungen benötigen sichere Implementierungen. Wenn sie richtig eingesetzt werden, können Datenpannen verringert werden.
- **Verantwortung übernehmen:** Es ist normal, dass in stressigen Situationen nicht alles perfekt läuft, entscheidend ist aber, dass Einrichtungen klare Strukturen schaffen, Fehler transparent machen und daraus lernen. Gleichzeitig bleibt jeder Einzelne in der Pflicht, die vertraulichen Informationen von Patienten zu respektieren.
- **Mit gezielten Maßnahmen**, regelmäßiger Schulung und einer gelebten Datenschutzpraxis lassen sich viele der oben beschriebenen Pannen vermeiden. Der Aufwand lohnt sich. Er schützt Patienten, bewahrt das Vertrauen in das Gesundheitswesen und spart im Ernstfall viel Geld und Ärger.

4.2.6 Kostenvoranschlag per E-Mail

Einem Patienten wurde auf seinen ausdrücklichen, telefonisch geäußerten Wunsch ein Kostenvoranschlag für eine anstehende medizinische Behandlung per E-Mail zugesandt. Zuvor wurde dem Patienten dargelegt, eine postalische Übersendung sei möglich und sicherer. Dennoch hatte sich der Patient für die Übersendung per E-Mail entschieden, da er den Kostenvoranschlag kurzfristig zur Vorlage bei seiner Krankenkasse benötigte.

Nach Absendung der E-Mail wurde aufgrund einer Nachfrage des Patienten, der die E-Mail nicht erhalten hatte, festgestellt, dass die E-Mail-Adresse nicht richtig erfasst worden ist. Der Kostenvoranschlag wurde an eine andere, ebenfalls existierende Adresse, gesendet. Dem unberechtigten Empfänger wurden auf diesem Weg personenbezogene Daten besonderer Kategorie übermittelt.

Dieser Fall zeigt folgendes Problem auf:

Eine Versendung personenbezogener Daten, auch solche besonderer Kategorien, per unverschlüsselter E-Mail ist grundsätzlich möglich. Darauf haben wir bereits in unserem Tätigkeitsbericht 2021[49] hingewiesen.

Voraussetzungen sind:

Die Betroffenen müssen darauf hingewiesen werden, dass die Möglichkeit eines sicheren, datenschutzkonformen Versandes, z. B. per Briefpost oder mit einer Verschlüsselung besteht und den Betroffenen bei Wahl einer solchen Möglichkeit keine Nachteile drohen.

Betroffene müssen dem Versand per unverschlüsselter E-Mail ausdrücklich zugestimmt haben. Der Nachweis für eine solche Einwilligung ist vom Verantwortlichen zu führen.

Im Falle einer Verschlüsselung ist eine reine Transportverschlüsselung nicht ausreichend. Vielmehr ist eine Ende-zu-Ende Verschlüsselung zu wählen.

Im vorliegenden Fall ist nach den Angaben des Verantwortlichen der Betroffene zunächst auf die Möglichkeit eines datenschutzkonformen Versands hingewiesen worden. Aufgrund der nur telefonischen Anforderung

49 KDSA, TB 2021, Pkt. 2.8 Keine Abdingbarkeit von technischen und organisatorischen Maßnahmen

des Betroffenen konnte aber dessen Einwilligung in den unverschlüsselten Versandt nicht nachgehalten werden. Hier wäre mindestens eine Einwilligung in Textform (nach der KDG-Reform demnächst ausdrücklich zulässig), z. B. in Form einer E-Mail, erforderlich gewesen. Hätte der Verantwortliche auf eine solche E-Mail mit der Funktion „Antworten" reagiert, wäre ein Verschreiben bei der E-Mail-Adresse ausgeschlossen gewesen.

Die Kommunikation mittels obligatorisch transportverschlüsselter E-Mails ist im geschäftlichen Verkehr durchaus als sozialadäquat und wohl derzeit noch als Stand der Technik einzustufen.

Eine Ende-zu-Ende-Verschlüsselung zeichnet sich demgegenüber dadurch aus, dass eine Entschlüsselung des Inhalts nur an den Endpunkten der Kommunikation (Absender und Empfänger) erfolgt.

Bei Daten und Verarbeitungen, die unter § 4 Nr. 2, § 11 KDG fallen, sind in jedem Fall besondere Schutzmaßnahmen zu ergreifen, da insoweit schon aufgrund der allgemeinen datenschutzrechtlichen Wertung stets von einem hohen Risiko ausgegangen werden muss.

Wenn der Patient, wie hier behauptet worden ist, den Kostenvoranschlag kurzfristig dringend benötigte, wäre dennoch eine verschlüsselte Versendung erforderlich gewesen. Bei einem verschlüsselten Versandt hätte der entstandene Datenschutzverstoß nicht eintreten können, da der unberechtigte Empfänger den Inhalt der E-Mail (Kostenvoranschlag) nicht hätte öffnen können.

5 Datenschutz in Kita und Schule

5.1 Fotos im Kindergarten – Risiken minimieren – TOMs etablieren

Fotos im Kindergarten und damit verbundene Datenschutzvorfälle sind über die Jahre hinweg ein Klassiker in vielen Tätigkeitsberichten der Datenschutzaufsichten.

Es kommt trotz zahlreicher Arbeitshilfen, Handlungsempfehlungen und Tipps der Aufsichten immer wieder vor, dass Geräte oder Speichermedien

mit Fotos abhandenkommen, Fotos trotz nicht vorhandener Einwilligung erstellt werden oder Mitarbeitende nicht ausreichend sensibilisiert sind.

So hat unsere Dienststelle im letzten Jahr auch wieder Datenschutzvorfälle gemeldet bekommen, in denen Fotos aufgrund abhandengekommener Geräte oder Speicher "verschwunden" sind. Dabei ist es in der datenschutzrechtlichen Bewertung unerheblich, ob die Geräte bzw. Speicher mit Fotos unabsichtlich abhandengekommen oder gestohlen worden sind.

Durch den Verlust von Fotos verlieren Verantwortliche die Kontrolle über diese Daten. Zudem ist nicht auszuschließen, dass unbefugte Dritte auf die abhandengekommenen Fotos zugreifen können.

Deshalb sind Verantwortliche verpflichtet, **TOM**s (Technische und Organisatorische Maßnahmen) zu etablieren, um Risiken bei der Datenverarbeitung zu minimieren.

> *Fotos von Kindern in kirchlichen Einrichtungen sind personenbezogene Daten (§ 4 Nr. 1 KDG), die in die Schutzklasse II gem. § 12 KDG-DVO einzuordnen sind. Deren missbräuchliche Verarbeitung kann die Betroffenen in ihrer gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen. Daher sind Fotos als besonders schutzwürdig anzusehen und entsprechend zu schützen.*

Regelmäßig stellt unsere Dienststelle dabei fest, dass Endgeräte nicht angemessen gesichert und/oder aufbewahrt waren bzw. ein nachlässiger Umgang erfolgte.[50] Zudem gab es in einigen Einrichtungen nur unzureichende Datenschutzkonzepte, noch lagen Löschkonzepte noch Verfahrensverzeichnisse oder Prozessregelungen vor. Auch wenn es aufgrund technischer Maßnahmen (z.B. Festplattenverschlüsselung) nicht zu einem Datenabfluss des verlorengegangenen Gerätes gekommen war, kann dennoch ein Verstoß gegen Regelungen aus dem KDG vorliegen, wenn beispielsweise die Datenverarbeitung nicht auf ein notweniges Maß beschränkt war. So enthielt beispielsweise ein verlorenes Gerät, welches ver-

50 KDSA, TB 2024, Pkt. 5.3.1 Fotos auf Abwegen
KDSA, TB 2023, Pkt. 5.2.3 Speichermedien auf Abwegen

schlüsselt war, 3.000 Fotoaufnahmen von Kindern und Mitarbeitenden der Einrichtung aus den vergangenen 10 Monaten.

Um alles, was mit den Fotos in Verbindung steht – die angemessene Verarbeitung, der Umgang, die Geräte, Speicherdauer und Löschfristen – zu etablieren, bietet sich eine Prozessregelung oder Verfahrensbeschreibung an, welche im Anhang dieses Berichts zu finden ist.

Welche Folgen ein unautorisierter Umgang mit Fotos in Verbindung mit einer fehlenden Verpflichtungserklärung haben kann, haben wir im Tätigkeitsbericht 2021[51] geschildert. Dort ist auch ausführlich beschrieben, welche Informationspflichten im Zusammenhang mit Fotos zu erfüllen sind.

Fazit:

Der richtige Umgang mit Fotos setzt **T**echnischen und **O**rganisatorischen **M**aßnahmen voraus. Können diese vom Verantwortlichen nicht erfüllt werden, erhöhen sich automatisch die Risiken bei der Verarbeitung von Fotos mit Personenbezug.

Um diese Anforderungen aus dem Datenschutz gerecht zu werden, können Fotos ohne personenbezogene Daten Anwendung finden. Fotos ohne Personenbezug, beispielsweise von hinten oder von oben, können genauso gut den Inhalt oder den Kontext des Bildes vermitteln. Sie können grundsätzlich einfacher verwendet oder veröffentlicht werden und die Privatsphäre bleibt trotzdem geschützt.

5.2 Datenschutzvorfälle

5.2.1 Einbruchdiebstahl in Kita mit gravierenden Folgen

Wie im vorherigen Beitrag erwähnt, müssen Verantwortliche Technische und Organisatorische Maßnahmen treffen, um die Risiken bei der Datenverarbeitung zu minimieren. Die TOMs sollen auch die Verfügbarkeit der zu verarbeitenden Daten sicherstellen.

51 KDSA, TB 2021, Pkt. 5.4 Ungewollt Kinderfotos im Netz, Pkt. 5.5 Informationspflichten

Um dieses Schutzziel umzusetzen, hatte der Verantwortliche einer Kindertageseinrichtungen einen zentralen Datenspeicher angeschafft, um mit verschiedenen Endgeräten auf diesen zugreifen zu können. Als Back-Up sollte eine externe Festplatte dienen, die im Büro der Leiterin aufbewahrt worden ist. Der zentrale Speicher war in einem anderen Gebäudeabschnitt sicher untergebracht. Auf dem zentralen Speicher sollten alle Daten der Kinder, die für die Betreuung notwendig sind, verarbeitet werden. Der Zugriff auf die Daten erfolgte vom PC der Leiterin, der in ihrem Büro stand. Zum Verwalten und Verarbeiten der Daten wurde eine standardmäßige Kita-Verwaltungssoftware eingesetzt.

Im Berichtsjahr ist es zu einem Einbruchdiebstahl in dieser Einrichtung gekommen. Die Diebe hatten es auf alle frei verfügbaren technischen Geräte abgesehen und nahmen u.a. den PC der Leiterin, Tastatur, Maus und eine externe Festplatte mit. Im weiteren Verlauf der Ermittlungen stellte die Einrichtung fest, dass auch die personenbezogenen Daten der betreuten Kinder sowie Daten der Sorgeberechtigten aus ca. 1,5 Jahren auf dem zentralen Speicher nicht mehr vorhanden sind. Das Back-Up, die verschlüsselte Festplatte, war Diebesgut und stand nicht mehr zur Verfügung.

Die nachfolgende Aufarbeitung des Vorfalls hatte ergeben, dass im Dezember 2023 Wartungsarbeiten an der Hard- und Software durchgeführt worden sind. Vermutlich wurde dabei der Datenspeicherort auf die Standard-Einstellung zurückgesetzt und die Daten wurden ab diesem Zeitpunkt lokal auf dem Gerät der Leiterin gespeichert. Da dieses Gerät jedoch entwendet worden ist, waren die Daten weg.

Zusätzlich wurde auch festgestellt, dass der PC „nur“ mit der Windows-Anmeldung gesichert war. Die Festplatte des PC`s war damit nicht verschlüsselt und ein Zugriff auf die Daten durch Unbefugte ist möglich.

Fazit:

Die Verantwortlichen sind verpflichtet die technischen oder organisatorischen Maßnahmen zur sicheren Datenverarbeitung – hier Speicherung – regelmäßig zu überprüfen. Insbesondere nach Wartungsarbeiten muss

der „IST"-Zustand dem vorgegeben „SOLL"-Zustand entsprechen. Idealerweise hält man schon bei der Beauftragung der Wartungs- oder Installationsarbeiten in einem Netzplan fest, wo die Datenspeicherorte sind.

5.2.2 Schusselige Lehrer oder wie können analoge Unterlagen besser transportiert werden?

Dass Lehrer einen Teil ihrer Arbeitszeit im häuslichen Umfeld leisten ist allgemein bekannt. Unterrichtsvorbereitungen, Kontrolle von Klassenarbeiten oder Abiturklausuren, Schreiben von Bewertungen oder Zeugnissen sind dabei die zu erledigenden Aufgaben.

Zum Schutz der dabei verarbeiteten personenbezogenen Daten der Schülerinnen und Schüler sind etliche technische und organisatorische Maßnahmen etabliert. So werden entweder dienstliche Endgeräte gestellt oder der Zugriff auf die Daten der Schule erfolgt mittels einer gesicherten VPN-Verbindung vom privaten Computer. Auch ist es selbstverständlich, dass Lehrende ihre Unterlagen zu Hause gesichert aufbewahren.[52]

Doch wie schützt man analoge Daten, die von der Schule in das häusliche Umfeld transportiert werden, wie z.B. Kursmappen, Zeugnisse oder Klausuren? Diese Frage haben wir im Berichtsjahr gleich 2-mal Verantwortlichen stellen müssen.

Fall 1)

Ein Lehrer hat seine Aktentasche mit Kursmappen der Mittel- und Oberstufe im Zug auf dem Nachhauseweg verloren. In den Kursmappen waren die Vor- und Zunamen, einzelne Noten und unentschuldigte bzw. entschuldigte Fehlzeiten der Schülerinnen und Schüler vermerkt. Insgesamt waren 90 Datensätze betroffen.

Fall 2)

An einer anderen Schule wollte ein Lehrer Abiturklausuren zur Korrektur mit nach Hause nehmen. Die Klausuren wurden in einem Beutel transpor-

52 KDSA, TB 2020, Pkt. 5.2 Datenverarbeitung durch Lehrkräfte

tiert und in der S-Bahn liegen gelassen. Auf den Abiturklausuren sind die Vor- und Zunamen der Schülerinnen und Schüler sowie deren Begutachtung und Bewertung notiert. Es waren in diesem Fall 14 Datensätze betroffen.

Bei Schulnoten bzw. Bewertungen oder Angaben über Fehlzeiten in Verbindung mit Vor- und Zunamen handelt es sich um personenbezogene Daten i. S. v. § 4 Nr. 1 KDG. Zudem kann der Missbrauch dieser Daten die Betroffenen in ihrer gesellschaftlichen Stellung (Stigmatisierung, Bloßstellung) beeinträchtigen. Daher sind die Daten der Kursmappen bzw. der Abiturklausuren in die Datenschutzklasse II nach § 12 KDG-DVO einzuordnen.

Beide Verantwortlichen haben angegeben, dass für den Transportweg von Unterlagen keine Regelungen etabliert sind. Diese Aussage überraschte, da es ja betriebliche Praxis der Lehrerinnen und Lehrer ist, personenbezogene Daten von Schülerinnen und Schülern mit nach Hause zu nehmen.

Während es für die Transportwege von digitalen Daten sehr gute und etablierte Schutzmechanismen wie VPN, Verschlüsselung oder Passwörter gibt, hat man die herkömmlichen (analogen) Wege aus dem Blick verloren. Beide Verantwortlichen haben verkannt, dass auch solche Unterlagen angemessen zu schützen sind, um u.a. Vertraulichkeit und Verfügbarkeit sicherzustellen.

Fazit:

In beiden Fällen haben wir die Vorfälle beanstandet und die Auflage erteilt, entsprechende Schutzmechanismen zu etablieren und alle Mitarbeitenden anlassbezogen zu sensibilisieren.

Im ersten Fall hat uns der Verantwortliche bereits mitgeteilt, dass man digitale Kurshefte einführen wird, um so einem Datenverlust auf analogen Weg auszuschließen.

Dies wird im zweiten Fall nicht umsetzbar sein, da Abiturklausuren derzeitig noch analog (schriftlich) vorliegen. Der Transport in einem Beutel stellt unabhängig davon auf jeden Fall keinen hinreichend gesicherten Transport dar.

6 Datenschutz im Beschäftigungsverhältnis

6.1 Zum Auskunftsersuchen

6.1.1 Kann ein Arbeitnehmer auf einen Auskunftsanspruch verzichten?

Immer wieder stellt sich im Datenschutzrecht die Frage, ob Betroffene wirksam auf im Datenschutzgesetz festgeschriebene Rechte verzichten können.

Im arbeitsrechtlichen Kontext stellt sich darüber hinaus die Frage, ob dies in einem arbeitsgerichtlichen Vergleich möglich ist.

Fall:

Konkret hatte das Oberverwaltungsgericht (OVG) des Saarlandes[53] zu entscheiden, ob die in arbeitsgerichtlichen Vergleichen übliche Formel

„Mit Erfüllung dieses Vergleichs sind alle Ansprüche aus dem Arbeitsverhältnis und dessen Beendigung, gleich ob bekannt oder unbekannt, gleich aus welchem Rechtsgrund, abgegolten mit Ausnahme der Arbeitspapiere."

auch den Ausschluss eines Auskunftsanspruches gem. Art. 15 DS-GVO (§ 17 KDG) umfasst. Der Kläger stellte gegenüber seinem Arbeitgeber am 14.01. einen Antrag auf umfassende Auskunft gem. Art. 15 DS-GVO. Dieser antwortete auf das Auskunftsersuchen nicht. Am 28.01. wurde das Arbeitsverhältnis aus betrieblichen Gründen gekündigt. Am 17.02. rügte der Kläger gegenüber der Datenschutzaufsicht des Landes die Nichtbeantwortung seines Auskunftsersuchens. Am 24.02. schlossen der Kläger und sein Arbeitgeber einen gerichtlichen Vergleich, der die oben dargestellte Formulierung beinhaltete. Daraufhin stellte die Datenschutzaufsicht mit Bescheid vom 26.07. das Verwaltungsverfahren gegen den Arbeitgeber ein. Gegen diese Einstellung richtete sich der Kläger. Er beantragte vor dem Verwaltungsgericht die Datenschutzaufsicht zu verpflichten, den Einstellungsbescheid aufzuheben und das gegen den Arbeitgeber eingeleitete datenschutzrechtliche Verfahren fortzuführen.

53 OVG Saarland, Urteil vom 13.05.2025 – 2 A 165/24

Zunächst war zu klären, ob Betroffene überhaupt auf ein Datenschutzrecht verzichten können, welches ihnen durch die DS-GVO eingeräumt wird. Eine Aussage dazu findet sich zunächst weder in der DS-GVO selbst, noch in deren Erwägungsgründen. Das Gericht stellt dazu fest, die Möglichkeit des Verzichts folge aus dem Datenschutzrecht selbst. Gem. Art. 7 i. V. m. Art. 4 Nr. 11 DS-GVO stehe es dem Betroffenen frei, in die Verarbeitung seiner personenbezogenen Daten einzuwilligen. Darin kommt das Prinzip der Selbstbestimmung zum Ausdruck. Wenn dieses Prinzip es ermöglicht, über die Zulässigkeit der Datenverarbeitung selbst zu bestimmen, muss es aus Sicht des Gerichtes auch möglich sein, eine Disposition über das Auskunftsrecht zu treffen, das nur einen Einblick in das Ergebnis der Datenverarbeitung ermöglicht. Das Datenschutzrecht sei daher kein unabdingbares Gleichheits- oder Menschenwürderecht, sondern ein Freiheitsrecht. Zu einem solchen gehöre es auch, darauf verzichten zu können. Eine Disposition über den Auskunftsanspruch sei deshalb für ein Arbeitsverhältnis, welches in der Vergangenheit bestanden hat, möglich. Dies insbesondere deshalb, weil nach Beendigung des Arbeitsverhältnisses eine Schutzbedürftigkeit aufgrund struktureller Unterlegenheit des Arbeitnehmers nicht mehr bestehe.

Weiterhin war zu entscheiden, ob die Formulierung des Vergleiches auch den datenschutzrechtlichen Auskunftsanspruch mitumfasst. Dazu stellt das Gericht fest, die Formulierung „gleich aus welchem Rechtsgrund“ lässt keinen Grund erkennen, warum gerade der Auskunftsanspruch davon nicht erfasst sein sollte. Schließlich beziehe sich der Anspruch auf das frühere Arbeitsverhältnis bzw. resultiere daraus.

Ebenso, wie zuvor auch die Datenschutzaufsicht, legt das Gericht damit die Formulierung „Ansprüche aus dem Arbeitsverhältnis“ weit aus.

Der Kläger hat von der Datenschutzaufsicht verlangt, seinem Anspruch auf Auskunft zur Durchsetzung zu verhelfen, insoweit ist der Einstellungsbeschluss der Datenschutzaufsicht gerechtfertigt.

Offen bleibt aber, ob nicht dennoch eine Sanktion des Arbeitgebers durch die Datenschutzaufsicht hätte erfolgen müssen, da der Arbeitgeber dem Auskunftsanspruch gem. Art 15 DS-GVO nicht fristgerecht nachgekommen ist. Diesbezüglich hat der Arbeitgeber aber bestritten eine Aufforderung zur Auskunftserteilung vom Kläger erhalten zu haben.

Fazit:

Beschäftigte, die sich die Möglichkeit eines Auskunftsanspruchs für das vergangene Arbeitsverhältnis offenhalten wollen, müssen dies in einem Vergleich ausdrücklich darlegen, wenn sie die übliche Formulierung verwenden.

Im Bestreitensfall müssen Betroffene belegen können, einen Auskunftsanspruch gegenüber dem Verantwortlichen geltend gemacht zu haben. Der Nachweis des Absendens einer E-Mail ist kein Anscheinsbeweis dafür, dass der Empfänger die E-Mail tatsächlich auch erhalten hat (siehe Pkt. 2.6 in diesem Bericht). Geeignet wäre u.a. eine Aufforderung zu einer kurzen Rückinformation als Bestätigung für den Empfang.

6.1.2 Wo haben Sie sich beworben? - Annahmeverzugslohn und Auskunftspflicht des Arbeitnehmers

Das Bundesarbeitsgericht (BAG)[54] hat eine Entscheidung zum Annahmeverzugslohn getroffen. Es ging um die Frage, ob Arbeitnehmer böswillig im Sinne des § 615 BGB anderweitigen Verdienst unterlassen, wenn sie innerhalb der Kündigungsfrist, in der sie vom Arbeitgeber von der Arbeitsleistung freigestellt wurden, kein anderes Beschäftigungsverhältnis eingehen. Im konkreten Fall wurde ein Arbeitnehmer ordentlich gekündigt und für die Kündigungsfrist vom Arbeitgeber unwiderruflich von der Arbeitspflicht freigestellt. Im Zeitraum der Kündigungsfrist übersandte der Arbeitgeber dem Arbeitnehmer mehrere Stellenangebote. Auf diese bewarb sich der Arbeitnehmer nicht. Daraufhin weigerte sich der Arbeitgeber Annahmeverzugslohn zu zahlen.

Das BAG stellt fest, dass sich der Arbeitgeber in Annahmeverzug befindet, wenn er die Arbeitsleistung des Arbeitnehmers im Zeitraum der Kündigungsfrist ablehnt. Zwar muss sich der Arbeitnehmer grundsätzlich nicht erzielten anderweitigen Verdienst anrechnen lassen, wenn er wider Treu und Glauben untätig geblieben ist, jedoch kann diese Obliegenheit nicht losgelöst von den Pflichten des Arbeitgebers betrachtet werden. Der Arbeitgeber muss Arbeitnehmer während der Zeit bis zum Ablauf der Kündigungsfrist weiterbeschäftigen, solange dies für ihn nicht unzumutbar

54 BAG, Urteil vom 12.02.2025 – 5 AZR 127/24

ist. Während dieser Zeit sind Arbeitnehmer deshalb nicht verpflichtet, zur finanziellen Entlastung des Arbeitgebers beizutragen, wenn dieser die angebotene Arbeitsleistung ablehnt.

Anders ist die Rechtslage zu beurteilen, wenn es um den Annahmeverzugslohn nach Ablauf der Kündigungsfrist im laufenden Kündigungsschutzverfahren geht. Unterlassen Arbeitnehmer zu dieser Zeit Bewerbungen allgemein oder bei den vom Arbeitgeber dargelegten Stellen, ist eine fiktive Anrechnung des nicht erworbenen Verdienstes gerechtfertigt.

Erhebt der Arbeitgeber entsprechende Einwendungen nach § 11 Nr. 2 KSchG und verweigert die vertraglich vereinbarte Vergütung, ist er für die Einwendung, der Arbeitnehmende sei böswillig untätig geblieben und hätte sich damit bewusst und entgegen Treu und Glauben jeder neuen Beschäftigung verweigert, darlegungs- und beweispflichtig.[55]

Der Arbeitgeber kann aber regelmäßig weder darlegen und beweisen, dass Arbeitnehmer überhaupt anderweitige Verdienste hatten, noch kann er Angaben zur Höhe des anderweitigen Erwerbs machen. Er kann sich die notwendigen Informationen auch nicht selbst auf zumutbare rechtmäßige Weise beschaffen.

Der Arbeitnehmer ist deshalb nach der Rechtsprechung des 5. Senats des BAG[56] aufgrund der Regelung des § 2 Abs. 5 SGB III zur aktiven Mitarbeit bei der Vermeidung oder Beendigung von Arbeitslosigkeit angehalten und daneben verpflichtet, sich unverzüglich nach Kenntnis des Beendigungszeitpunkts des Arbeitsverhältnisses persönlich bei der Agentur für Arbeit arbeitssuchend zu melden, § 38 Abs. 1 SGB III.[57] Auch wenn es sich bei der Vorschrift primär um eine rein sozialversicherungsrechtliche Meldeobliegenheit handelt, hat die Meldepflicht nach Ansicht des BAG auch im Rahmen der Anrechnungsvorschriften beim Annahmeverzug Beachtung zu finden, weil dem Arbeitnehmer arbeitsrechtlich das zugemutet werden kann, was ihm das Gesetz ohnehin abverlangt.[58]

Darüber hinaus kann der Arbeitgeber den Arbeitnehmer über konkrete Stellenangebote informieren, ihn dadurch in „Zugzwang“ versetzen und Bewerbungen veranlassen, um gegebenenfalls die Ansprüche aus Annah-

55 BAG, Urteil vom 25.10.2007 – 8 AZR 917/06
56 BAG, Urteil vom 27.05.2020 – 5 AZR 387/19
57 anders noch BAG, Urteil vom 16.05.2000 – 9 AZR 203/99
58 BAG, Urteil vom 16.05.2000 – 9 AZR 203/99

meverzug dann kürzen zu können, wenn der Arbeitnehmer auf diese Mitteilungen hin vorsätzlich das Zustandekommen eines Arbeitsverhältnisses verhindert.[59]

Nach der Rechtsprechung des BAG (5 AZR 387/19) hat der Arbeitgeber gegen den Arbeitnehmer einen Auskunftsanspruch über Vermittlungsvorschläge der Agentur für Arbeit. Der Arbeitnehmer hatte zuvor im Rahmen des Kündigungsschutzprozesses obsiegt und anschließend einen Annahmeverzugslohn geltend gemacht.

Aus datenschutzrechtlicher Sicht ist eine Verarbeitung personenbezogener Daten, um die es sich bei den hier in Rede stehenden Auskunftsansprüchen handelt, gem. § 6 Abs. 1 lit. c) KDG rechtmäßig, wenn damit der Zweck verfolgt wird, festzustellen, ob ein Anspruch auf ausstehendes Entgelt besteht. Grundsätzlich kann man die Verarbeitung personenbezogener Daten zum Zweck der Feststellung der noch zu zahlenden Vergütung aufgrund der Beweislast, die beim Arbeitgeber liegt, als erforderlich gem. § 6 Abs. 1 lit. c) KDG ansehen. Dies gilt aber nur dann, wenn die Verarbeitung zur Erreichung des angestrebten Zwecks erforderlich ist.

Erforderlich ist eine Datenverarbeitung dann, wenn ohne sie die Erreichung des Zwecks nicht möglich ist. Wenn der Zweck darin besteht, Ansprüche des Arbeitnehmers durch eine Einwendung abzuwenden, müssen solche Ansprüche aber zunächst geltend gemacht worden sein. Entgegen der Auffassung des BAG reicht es hierfür aber nicht aus, dass eine Geltendmachung entsprechender Ansprüche durch den Arbeitnehmer nach einem Obsiegen im Kündigungsschutzprozess wahrscheinlich ist. Solange der Arbeitgeber etwaigen Annahmeverzugslohnforderungen noch nicht konkret ausgesetzt ist, fehlt es für die Geltendmachung von Auskunftsansprüchen an der, für die Verarbeitung dieser personenbezogenen Daten, notwendigen Erforderlichkeit gem. § 6 Abs. 1 lit. c) KDG (Art. 6 Abs. 1 lit. b) DS-GVO).

Fazit:

Solange der Arbeitnehmer beim Arbeitgeber keine Vergütung wegen Annahmeverzugs gefordert hat, besteht kein Anspruch auf Auskunft über Bewerbungen auf Stellenangebote bzw. erzielte anderweitige Einkünfte,

59 BAG, Urteil vom 16.05.2000 – 9 AZR 203/99

da die Datenerhebung „noch“ nicht erforderlich ist. Auch, wenn im Fall des Obsiegens des Arbeitnehmers im Kündigungsschutzverfahrens, in der Regel mit der Geltendmachung des Annahmeverzugslohns zu rechnen ist, kann dies nicht dazu führen, dass diese Daten „rein vorsorglich“ gefordert und damit verarbeitet werden. Die Einwendungen des § 11 Nr. 1 KSchG muss einem geltend gemachten Anspruch entgegengehalten werden.

6.2 Krankenstand / Arbeitsunfähigkeit

6.2.1 Zwischen Datenschutz und Informationspflicht - Krankmeldungen mit der eAU

Während die Einführung der elektronischen Patientenakte (ePA) stockte, sind die elektronischen Arbeitsunfähigkeitsbescheinigungen (eAU) mittlerweile Stand der Dinge. In unserem Tätigkeitsbericht 2022[60] haben wir uns bereits umfassend zu dem Verfahren geäußert.

Jedoch kommen dabei immer wieder Fragen in Bezug auf das “Handling“ auf, da es in caritativen sowie kirchlichen Strukturen nicht nur den einen Arbeitgeber bzw. eine Dienststelle gibt. Mitarbeitende sind oft bei einem Arbeitgeber angestellt, werden in einer weiteren Dienststelle eingesetzt und die Gehaltsstelle, welche auch von der Arbeitsunfähigkeit (AU) zu unterrichten ist, wird von einer weiteren Stelle übernommen.

- Bei wem müssen sich die Mitarbeitenden nun krankmelden?
- Welche Daten müssen sie dabei mitteilen?
- Auf welchem Weg müssen die Mitarbeitenden dies tun?

Unstreitig ist, Mitteilungen zur Arbeitsunfähigkeit in Verbindung mit einem Namen sind personenbezogene Daten besonderen Kategorie (§ 4 Nr. 2 KDG), die besonders schützenswert sind und nur auf gesichertem Weg verarbeitet werden dürfen (§ 7 Abs. 1 lit. f) KDG). Die Speicherung entsprechender Informationen ist dadurch nur solange gestattet, wie dies für einen konkreten Zweck erforderlich ist.

Mitarbeitende sollten sich zuerst bei ihrem direkten Vorgesetzten bzw. ihrer Dienststelle krankmelden. Diese muss u.U. für die Vertretung des Er-

60 KDSA, TB 2022, Pkt. 4.2 Die elektronische Arbeitsunfähigkeitsbescheinigung

krankten sorgen und daher auch über die Dauer der AU informiert werden. Dies reicht aus Gründen der Datensparsamkeit mündlich völlig aus.

Möchte der Arbeitgeber per E-Mail über die Arbeitsunfähigkeit informiert werden, weil er z.B. eine telefonische Erreichbarkeit nicht sicherstellen kann oder er so die Daten der Krankmeldung zur Weitergabe an die Personalstelle oder Gehaltstelle gleich schriftlich vorliegen hat, so gibt es hierbei folgendes zu beachten:

- Verwendet der Mitarbeitende seine private E-Mail-Adresse für die AU-Meldung, bekommt der Arbeitsgeber ein personenbezogenes Datum übermittelt, dass er eigentlich für diese Datenverarbeitung nicht benötigt. Daher ist der Arbeitgeber bzw. die Stelle, bei dem sich der Mitarbeitende krankmeldet, angehalten, dieses Datum nicht unbefugt für andere Zwecke zu verarbeiten, weiterzugeben oder zu speichern.
- Eine Weitergabe der Arbeitsunfähigkeit an Personal- oder Gehaltsstelle ist auch ohne Weitergabe der privaten E-Mail-Adresse möglich.
- Eine Weiterleitung an das gesamte Kollegium ist nicht erforderlich und sollte unterbleiben.
- Die Daten der Krankmeldung sollten nur für einen möglichst kurzen Zeitraum in einem E-Mail-Postfach vorgehalten werden, da E-Mail-Postfächer keine Datenspeicher sind. Auf eine vollständige Löschung (auch in gelöschte Elemente) ist zu achten.
- Der Zugriff auf das E-Mail-Postfach, auf dem die AU-Meldung eingeht, darf nur von autorisierten Personen erfolgen.
- Der Arbeitgeber bzw. die Dienststelle darf bei der Übermittlung der Arbeitsunfähigkeit keine Kopien oder Fotos vom Krankenschein verlangen, den der Mitarbeitende für seine Unterlagen vom Arzt noch ausgehändigt bekommt.

Eine Übermittlung dieser sensiblen Informationen per E-Mail ist weitestgehend unkritisch. E-Mails, auch vom privaten Account, verfügen in der Regel über eine Transportverschlüsselung. Eine Einsichtnahme vom Adressaten zum Empfänger ist somit nahezu ausgeschlossen.

6.2.2 Umgang mit Gesundheitsdaten – Entgeltfortzahlung

Werden Beschäftigte infolge Krankheit an der Arbeitsleistung verhindert, ohne dass sie ein Verschulden trifft, so haben sie Anspruch auf Entgeltfortzahlung im Krankheitsfall durch den Arbeitgeber für die Zeit der Arbeitsunfähigkeit (AU) bis zur Dauer von sechs Wochen.

Die Arbeitsunfähigkeit musste früher durch eine ärztliche Bescheinigung auf einem einheitlichen Formular (gelber Schein) erbracht werden. Die Diagnose war auf dem Formular nicht aufgeführt, jedoch war durch den auf dem Formular aufgebrachten Arztstempel ggf. zu erkennen, um welche Art der Erkrankung es sich handelte.

Seit Anfang Januar 2023 übermitteln Arztpraxen und Krankenhäuser elektronische Arbeitsunfähigkeitsbescheinigungen digital an die Krankenkassen. Arbeitgeber sind seitdem verpflichtet, die AU-Daten der gesetzlich versicherten Beschäftigten elektronisch von den Krankenkassen abzurufen. Die Krankenkasse darf dabei weder Diagnosedaten noch die ausstellende Ärztin oder den ausstellenden Arzt bekanntgeben, hat aber mitzuteilen, ob es sich um eine Erst- oder Folgebescheinigung handelt.

Für Arbeitgeber stellt sich immer dann, wenn Beschäftigte länger erkranken, die Frage, ob der jeweilige Arbeitnehmer weiterhin einen Anspruch auf Entgeltfortzahlung hat. In der Regel wird nur in den ersten sechs Wochen einer Erkrankung der Lohn weitergezahlt. Anschließend zahlt die Krankenkasse Krankengeld.

Ist der Arbeitnehmer hintereinander an der gleichen Krankheit erkrankt, läuft nicht bei jeder Erkrankung wieder die Sechs-Wochen-Lohnfortzahlung erneut. Die Zeiten der „fortgesetzten“ Erkrankungen werden addiert.

Damit der Arbeitgeber beurteilen kann, ob eine solche „Fortsetzungserkrankung“ vorliegt, ist unter Umständen die Mitteilung von Gesundheitsdaten erforderlich. Da diese Informationen jedoch besonders sensibel sind, sieht das KDG für deren Verarbeitung strenge Regelungen vor.

Arbeitgeber, die im Zusammenhang mit der Entgeltfortzahlung ggf. berechtigt sind, bestimmte Gesundheitsdaten zu verarbeiten, dürfen dies nur

dann, wenn die Verarbeitung erforderlich ist und keine milderen Alternativen bestehen.

Danach darf die Anfrage des Arbeitgebers nur dann erfolgen, wenn folgende Voraussetzungen erfüllt sind:

- Für die aktuelle Arbeitsunfähigkeit liegt ein Nachweis vor,
- in den letzten sechs Monaten vor Beginn der aktuellen Arbeitsunfähigkeit liegt mindestens eine bescheinigte Vorerkrankung vor,
- die kumulierten AU-Zeiten (in den letzten zwölf Monaten) aller potenziellen Vorerkrankungen inklusive der aktuellen Arbeitsunfähigkeit müssen mindestens 30 Tage (6 Wochen) ergeben.

Liegen diese Voraussetzungen vor, ergibt sich die Erforderlichkeit aus der gesetzlichen Verpflichtung von Arbeitgebern zur Lohnfortzahlung im Krankheitsfall (§ 3 EFZG). Rechtsgrundlagen für die Verarbeitung dieser besonderen Kategorie personenbezogener Daten sind dann § 53 KDG i. V. m. § 11 Abs. 2 lit. b) KDG.

Eine pauschale Erhebung von Diagnosen oder die Abfrage nach chronischen Vorerkrankungen außerhalb des Entgeltfortzahlungszeitraums ist aber generell unzulässig. Besonders sensible Gesundheitsdaten müssen zudem sicher verwahrt, frühzeitig gelöscht und dürfen nicht beliebig weitergegeben werden. Datenschutz gilt auch im Krankheitsfall – und schützt damit die Gesundheitsdaten der Beschäftigten gegenüber Arbeitgebern.

In welchem Maß Arbeitgeber Kenntnis vom Gesundheitszustand eines Angestellten erhalten dürfen, dazu hat sich im Berichtsjahr auch die LDI NRW, Bettina Gayk, geäußert.[61]

Auch das Bundesarbeitsgericht hat in einem Urteil[62] ausgeführt, in welchem abgestuften Umfang Arbeitnehmende an der Überprüfung der Entgeltfortzahlung mitwirken müssen. Danach muss der Arbeitnehmer unter Vorlage ärztlicher Bescheinigungen vortragen, dass keine Fortsetzungserkrankung besteht. Bleibt der Arbeitgeber auf dem Standpunkt, dass es sich um eine Fortsetzungserkrankung handelt, muss der Arbeitnehmer konkrete Tatsachen vortragen, die eine solche ausschließen. Dazu muss er Tatsachen

61 LDI Nordrhein-Westfalen, https://www.ldi.nrw.de/Fortsetzungserkrankung
62 BAG, Urteil vom 18.01.2023 – 5 AZR 93/22

vortragen, die den Schluss erlauben, dass keine Fortsetzungserkrankung besteht. Er also muss bezogen auf den gesamten maßgeblichen Zeitraum schildern, welche gesundheitlichen Beeinträchtigungen und Beschwerden mit welchen Auswirkungen auf seine Arbeitsfähigkeit bestanden und die behandelnden Ärzte von der Schweigepflicht entbinden, so das BAG.

Das Bundesarbeitsgericht stellt zudem fest:
„Beschäftigte können diese Auskünfte nicht mit Blick auf den Datenschutz verweigern, und zwar auch nicht mit Blick auf die Krankenkasse, die Arbeitgebern ja auch Auskunft über das Bestehen einer Fortsetzungs- oder Ersterkrankung erteilen muss."

6.2.3 Mitteilung über den Krankenstand kann teuer werden

Wahrscheinlich hat es jeder schon mindestens einmal erlebt. Man möchte eine Person telefonisch oder persönlich erreichen und man erhält die Auskunft, dies sei leider nicht möglich, denn die Person sei krank.

Eine solche Information mag für den Fragesteller zunächst hilfreich sein, allerdings wird sie auch regelmäßig über sein Informationsinteresse hinausgehen. Denn warum man jemanden nicht erreichen kann, dürfte im beruflichen Kontext nicht von Interesse sein. Vielmehr wird es in diesem Zusammenhang nur wichtig sein, wann man die Person wieder sprechen kann oder wer sie vertritt.

Demgegenüber stellt die Mitteilung jemand sei krank die Bekanntgabe personenbezogener Daten dar. Darüber hinaus handelt es sich dabei um Gesundheitsdaten. Gemäß Erwägungsgrund 35 zur DS-GVO S. 1 werden damit alle Daten erfasst, „die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen". Damit fallen neben dem Datum der medizinischen Arbeitsunfähigkeit auch Informationen über eine Kur- oder Reha-Maßnahme unter diese Definition.

Wird gegenüber Dritten eine Abwesenheit bekannt gegeben und mit einer solchen Information verbunden, stellt dies einen Datenschutzverstoß dar.

Dies gilt erst recht, wenn solche Informationen einem größeren Empfängerkreis kundgetan werden, beispielsweise in einer Mail an die Belegschaft oder eine Abteilung oder durch Aushang.

Bereits im letzten Jahr hatte das Arbeitsgericht Duisburg[63] einen solchen Fall verhandelt und den Verantwortlichen zur Zahlung eines Schmerzensgeldes an den Betroffenen in Höhe von 10.000, - € verurteilt. Auch wenn in diesem Fall die hohe Anzahl der Adressaten zu dem eheblichen Schadenersatz beigetragen hat, bleibt doch festzustellen, dass eine ungerechtfertigte Verarbeitung von Gesundheitsdaten Schmerzensgeldforderungen der Betroffenen nach sich ziehen kann.

Verantwortliche sollten, um solche Konsequenzen zu vermeiden, Auskunft nur im erforderlichen Umfang erteilen: „Der Mitarbeiter/die Mitarbeiterin ist in der nächsten Woche nicht im Haus." Eine solche Sprachregelung sollte allen Beschäftigten vorgegeben werden.

Etwas anderes kann nur gelten, wenn eine Mitteilung an Vorgesetzte oder andere Personen, die für eine Vertretung sorgen müssen, gemacht werden muss.

6.3 Dürfen Regelungen einer Betriebs- oder Dienstvereinbarung das Schutzniveau des Datenschutzes unterschreiten?

Gem. Art. 88 DS-GVO können die Mitgliedstaaten der EU bei der Datenverarbeitung im Beschäftigungskontext durch Kollektivvereinbarungen spezifischere Vorschriften erlassen.

Unter solchen kollektiven Vereinbarungen sind sowohl Tarifverträge als auch Betriebsvereinbarungen zu verstehen. Dies ergibt sich bereits aus Erwägungsgrund 155 zur DS-GVO.

Wenn die Verordnung spezifischere Verarbeitungen personenbezogener Daten erlaubt, stand gelegentlich die Frage, ob solche Vereinbarungen das Schutzniveau der DS-GVO unterschreiten dürfen. Teilweise wurde dies

63 AG Duisburg, Urteil vom 26.09.2024 - 3 Ca 77/24

unter Berufung auf eine Entscheidung des BAG[64], die vor in Kraft treten der DS-GVO ergangen ist, befürwortet.[65]

Das Bundesarbeitsgericht (BAG) hatte zur Klärung dieser Frage dem Europäischen Gerichtshof (EuGH) in einem Vorabentscheidungsverfahren u. a. die Frage vorgelegt, ob bei einer solchen Kollektivvereinbarung auch die in der Verordnung geregelten Grundsätze der Datenverarbeitung gem. Art. 5 DS-GVO sowie die Regelungen über die Rechtmäßigkeit der Datenverarbeitung einzuhalten sind.

Der EuGH[66] hat dies in einer Entscheidung, die bereits am 19.12.2024 ergangen ist, bestätigt. Danach dürfen Festlegungen in einer Betriebsvereinbarung das Schutzniveau der Verordnung nicht unterschreiten. Der in der Kollektivvereinbarung enthaltene Datenschutz darf nicht hinter der DS-GVO zurückbleiben. Regelungen in einer Betriebsvereinbarung, die dagegen verstoßen, sind insoweit unwirksam.

Zwar beruhe die Öffnungsklausel auf der Erkenntnis, dass die Betriebsparteien aufgrund ihrer Sachnähe umfangreiche Kenntnisse in Bezug auf die speziellen Bedürfnisse im Beschäftigungs- und Tätigkeitsbereich ihres Betriebes und damit einen Gestaltungsspielraum hinsichtlich der spezifischen Vorschriften haben, allerdings erfordere das Schutzziel der DS-GVO, dass die Gerichte die Einschätzungen der Betriebsparteien vollumfänglich überprüfen können.

Werden vom Arbeitgeber mehr personenbezogene Daten verarbeitet als es die Betriebsvereinbarung erlaubt, begründet dies grundsätzlich einen Schadensersatzanspruch der betroffenen Arbeitnehmer.

Um im Rahmen der Einführung eines cloudbasierten Personalinformationssystems die Software zu testen, erlaubte eine Betriebsvereinbarung die Übermittlung von Namen, Eintrittsdatum, Arbeitsort sowie geschäftlichen Kontaktdaten. Tatsächlich wurden darüber hinaus vom Verantwortlichen aber auch Gehaltsdaten, private Wohnanschriften und Steuer-ID verarbeitet. In dem Kontrollverlust über die personenbezogenen Daten liegt nach Ansicht des BAG ein immaterieller Schaden des Arbeitnehmers, der durch

64 BAG, Beschluss vom 27.5.1986 – 1 ABR 48/84
65 Kort RDV 2012, 8 (15)
66 EuGH, Urteil vom 19.12.2024 - C-65/23.

die unzulässige Datenweitergabe an die Konzernobergesellschaft verursacht worden sei. Dieser Kontrollverlust sei als ein immaterieller Schaden gemäß Art. 82 Abs. 1 DS-GVO zu ersetzen.

Fazit:

Betriebs- oder Dienstvereinbarungen können grundsätzlich als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dienen, müssen jedoch mit dem KDG / der DS-GVO vereinbar sein, deren Anforderungen vollständig erfüllen, ohne diese zu unterschreiten oder zu umgehen. Das bedeutet datenschutzwidrige Datenverarbeitungen können nicht durch eine Betriebsvereinbarung legitimiert werden. Nur wenn eine Betriebsvereinbarung das Datenschutzniveau erhöht, kommt sie als Rechtsgrundlage in Betracht. Ob eine Betriebsvereinbarung die rechtlichen Anforderungen erfüllt, unterliegt der vollumfänglichen Kontrolle durch die nationalen Gerichte.

6.4 Elektronische Entgeltabrechnungen: BAG erlaubt rein digitale Bereitstellung

Die Digitalisierung verändert unseren Alltag und macht auch vor dem Arbeitsplatz nicht halt. Immer mehr Prozesse werden von Papier auf digitale Formate umgestellt. Eine zentrale Frage dabei war lange: Gilt das auch für die monatliche Gehaltsabrechnung, ein wichtiges Dokument für jeden Arbeitnehmer? Diese Frage erreichte auch uns im Berichtszeitraum.

Das Bundesarbeitsgericht (BAG)[67] hat dazu entschieden, dass Unternehmen Gehaltsabrechnungen auch rein digital zur Verfügung stellen dürfen.

Die gesetzliche Pflicht nach § 108 Gewerbeordnung (GewO) erfüllen Arbeitgeber bereits dann, wenn sie ihren Mitarbeitenden die Entgeltabrechnungen in einem geschützten Online-Postfach bereitstellen. Papierausdrucke sind demnach nicht zwingend erforderlich, solange Arbeitnehmer ohne digitalen Zugang alternative Einsichtsmöglichkeiten haben.

Hintergrund

Die Entscheidung basiert auf einem Streitfall, in dem eine Supermarktverkäuferin sich gegen die ausschließlich elektronische Bereitstellung ihrer

67 BAG, Urteil vom 28.01.2025 -9 AZR 487/24

Gehaltsabrechnungen wehrte. Gemäß einer Konzernbetriebsvereinbarung wurden alle Personaldokumente – insbesondere Entgeltabrechnungen – in einem digitalen Mitarbeiterpostfach bereitgestellt, das durch einen externen Anbieter betrieben wurde. Die Arbeitnehmerin forderte aber weiterhin eine Abrechnung in Papierform, was der Arbeitgeber ablehnte.

Das Landesarbeitsgericht Niedersachsen[68] hatte der Klage der Arbeitnehmerin zunächst stattgegeben. Es argumentierte, dass die digitale Bereitstellung nicht genüge, da Entgeltabrechnungen zugangsbedürftige Erklärungen seien und ein digitales Mitarbeiterpostfach nur dann eine geeignete Empfangsvorrichtung darstelle, wenn der Arbeitnehmer es explizit für den Empfang von Erklärungen bestimmt habe.

Das BAG sah dies anders und gab der Revision des Arbeitgebers statt. Es stellte klar, dass die Bereitstellung von Entgeltabrechnungen in einem digitalen Mitarbeiterpostfach die in § 108 Abs. 1 GewO gesetzlich geforderte Textform wahrt.

Bei dem Anspruch des Arbeitnehmers auf eine Entgeltabrechnung handele es sich um eine sogenannte Holschuld. Das bedeutet, dass der Arbeitgeber die Abrechnung lediglich an einer zugänglichen elektronischen Ausgabestelle bereitstellen muss, ohne dass er für den tatsächlichen Zugang beim Arbeitnehmer verantwortlich ist, so das BAG.

Das Gericht betonte aber auch, dass der Arbeitgeber sicherstellen muss, dass Arbeitnehmer ohne private Online-Zugriffsmöglichkeiten ihre Abrechnungen im Betrieb einsehen und ausdrucken können.

Die Entscheidung des BAG schafft Rechtssicherheit für Arbeitgeber, die bereits auf digitale Gehaltsabrechnungen setzen oder dies planen. Die Entscheidung bestätigt, dass eine elektronische Bereitstellung grundsätzlich ausreicht und eine papierhafte Abrechnung nicht erforderlich ist.

Fazit:

Unternehmen müssen gewährleisten, dass Arbeitnehmer ohne eigene digitale Zugangsmöglichkeiten alternative Wege zur Einsicht und zum Ausdruck der Dokumente erhalten.

68 LAG Niedersachsen, Urteil vom 16.01.2024 -9 Sa 575/23

Ob für die Einführung und den Betrieb digitaler Mitarbeiterpostfächer der Konzernbetriebsrat zuständig ist, oder Mitbestimmungsrechte anderer, insbesondere der örtlichen Betriebsräte bestehen, hat das BAG in seiner Entscheidung offengelassen und das Verfahren diesbezüglich an das LAG zurückverwiesen.

Arbeitgeber sollten ihre bestehenden Verfahren zur Bereitstellung von Entgeltabrechnungen auf deren Rechtskonformität hin prüfen und sicherstellen, dass sie allen Arbeitnehmern den notwendigen Zugang zu ihren Dokumenten gewährleisten.

6.5 Darf der Arbeitgeber die Freigabe von Outlook-Kalendern verpflichtend anordnen?

Der Arbeitgeber stellt den Beschäftigten einen Outlook Kalender als dienstliches Arbeitsmittel zur Verfügung und hat grundsätzlich das Recht, darüber zu bestimmen, wie von ihm gestellte Arbeitsmittel verwendet werden. Ordnet er verpflichtend an, dass die Kalender der Beschäftigten für alle anderen Teammitglieder einsehbar sein müssen, ist das zunächst nicht zu beanstanden. Dadurch sollen Terminkoordinierungen vereinfacht und Arbeitsabläufe optimiert werden.

Zu berücksichtigen ist dabei, dass dies ein Tatbestand ist, der der Mitbestimmung durch die MAV oder den Betriebsrat unterliegt, da es sich hierbei um eine technische Einrichtung handelt, die dazu bestimmt ist, Verhalten und Leistung der Beschäftigten zu überwachen.[69]

„Bestimmt“ sind technische Einrichtungen schon dann, wenn sie „lediglich“ objektiv geeignet sind, Verhaltens- oder Leistungsinformationen der Arbeitnehmer zu erheben und aufzuzeichnen. Auf die subjektive Überwachungsabsicht des Arbeitgebers kommt es nicht an.[70]

Ist diese Voraussetzung erfüllt, spricht nichts gegen die Anweisung einer verpflichtenden Einrichtung eines für alle Teammitglieder einsehbaren Kalenders, soweit dort nur solche Daten eingetragen werden müssen, die für

69 VG Sigmaringen, Beschluss vom 28.07.2020 - PL 11 K 4795/18
LAG Nürnberg, Urteil vom 21.02.2017 – 7 Sa 441/16
70 BAG, Beschluss vom 13.12.2016 – 1 ABR 7/15

die ausgewiesenen Zwecke und zwar die vereinfachte Teamkoordination sowie vereinfachte Terminvereinbarungen erforderlich sind.

Das heißt, im Wesentlichen ist für den Arbeitgeber oder die anderen Teammitglieder nur wichtig zu wissen, ob jemand anwesend oder abwesend ist.

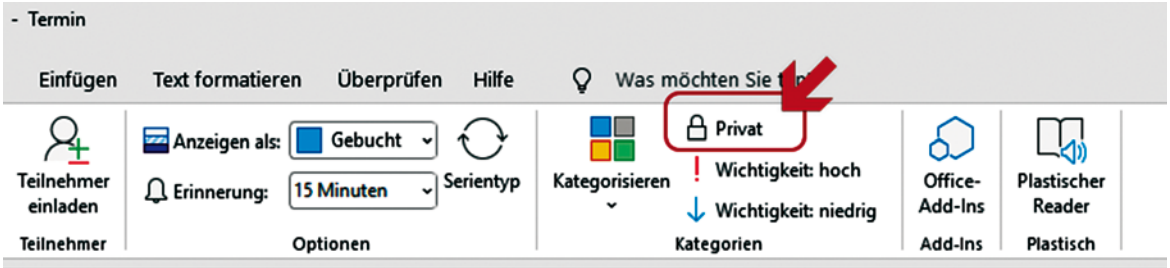
Detaillierte Eintragungen wie z.B. krank, Kind krank, Urlaub, Sonderurlaub, Weiterbildung, MAV-Schulung u. ä. sind für diesen Zweck nicht erforderlich und dürfen damit auch nicht vom Arbeitgeber verpflichtend angeordnet werden.

Grundsätzlich reicht deshalb die Angabe im Outlookkalender „abwesend“ aus. Damit wissen alle, die in den Kalender einsehen können, dass Beschäftigte bei dieser Eintragung nicht erreichbar sind.

Ggf. kann es zur Zweckerreichung auch erforderlich sein, „Homeoffice“ in den Kalender einzutragen, weil durch diese Eintragung klar wird, dass Beschäftigte nicht im Büro sind, ein Präsenztermin also nicht vereinbart werden kann. Ein telefonischer Termin oder eine Videokonferenz sind dann aber möglich.

Manche Mitarbeitende tragen sich auch private Termine in ihren dienstlichen Kalender ein. Das ist oft sinnvoll und regelmäßig auch vom Arbeitgeber zugelassen.

Private Termine (Arztbesuch, Friseur, Kind abholen ...) können im Outlook entsprechend gekennzeichnet werden und sind dann nur für den jeweiligen Nutzer einsehbar, für alle anderen erscheint nur „privat“.



Da es sich um ein dienstliches Arbeitsmittel handelt, kann der Arbeitgeber anordnen, dass alle Beschäftigten dies nutzen und alle Beschäftigten dies auch für alle Beschäftigten oder Teammitglieder öffnen. Ob der Arbeitgeber es zulässt, dass er oder andere Teammitglieder bei Beschäftigten

Termine in den Kalender verpflichtend eintragen, mag eine Frage der Unternehmenskultur sein. Datenschutzrechtlich bestehen diesbezüglich keine Bedenken.

Fazit:

Schreibt der Arbeitgeber die Nutzung des Outlook Kalenders verpflichtend vor und verpflichtet er die Beschäftigten für alle anderen Beschäftigten und den Arbeitgeber selbst den Kalender zu öffnen, ist dies zulässig, wenn die dargestellten Bedingungen erfüllt sind:

1. Zustimmung der Mitarbeitervertretung
2. Reduzierung auf erforderliche Eintragungen („abwesend")
3. Möglichkeit private Termine nur unter der Bezeichnung „privat" einzutragen

Eine solche Datenverarbeitung ist gem. § 53 Abs. 1 KDG zulässig, weil sie für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Persönlichkeitsrechte, die vom KDG geschützt werden sollen, werden durch eine solche Anweisung nicht gefährdet.

Für eine Einwilligung ist kein Raum, da der angestrebte Zweck nicht erreicht werden kann, wenn einzelne dem Verfahren nicht zustimmen. Auch wenn Beschäftigte die Einwilligung verweigern, darf der Arbeitgeber die Daten verarbeiten.

6.6 Weiterleitung dienstlicher E-Mails an private Accounts

Das Landesarbeitsgericht Hessen[71] hat entschieden, dass die Weiterleitung personenbezogener Beschäftigtendaten durch einen Betriebsratsvorsitzenden an sein privates E-Mail-Postfach einen groben Pflichtverstoß darstellt und somit den Ausschluss aus dem Betriebsrat rechtfertigt.

Hintergrund

Der Vorsitzende des Betriebsrats einer Klinik mit etwa 400 Beschäftigten leitete wiederholt personenbezogene Daten von seiner dienstlichen an seine private E-Mail-Adresse weiter.

71 LAG Hessen, Beschluss vom 10.03.2025 - 16 TaBV 109/24

Da die Klinik darin einen Datenschutzverstoß sah, erteile sie dem Betriebsratsvorsitzenden eine Abmahnung. Die Klinik stellte danach fest, dass der Betriebsratsvorsitzende nunmehr Informationen an eine neu eingerichtete private E-Mail-Adresse weiterleitet. Unter den übermittelten Daten befand sich unter anderem eine vollständige Liste aller Mitarbeitenden mit Angaben zur Stellung im Betrieb, Tarifgruppe, Vergütung, Eingruppierung sowie weiteren sensiblen personenbezogenen Informationen.

Zur Begründung für die Weiterleitung führte der Betriebsratsvorsitzende an, die Daten auf seinem privaten Endgerät mit größerem Bildschirm auswerten zu müssen, um die Vorbereitung einer Betriebsvereinbarung sachgerecht durchführen zu können. Der Arbeitgeber wertete das Verhalten als schwerwiegenden Verstoß gegen datenschutzrechtliche Bestimmungen und stellte beim Arbeitsgericht Wiesbaden einen Antrag nach § 23 Abs. 1 BetrVG auf Ausschluss aus dem Betriebsrat. Gegen die Entscheidung des Arbeitsgericht Wiesbaden, das dem Antrag stattgab, legten der Betriebsrat und der Betriebsratsvorsitzende Beschwerde ein.

Das LAG entschied, dass der Ausschluss zu Recht erfolgte. Nach Ansicht des Gerichts war die Weiterleitung der personenbezogenen Daten der Beschäftigten an den privaten E-Mail-Account des Betriebsratsvorsitzenden nicht erforderlich und stellt einen Verstoß gegen Art. 5 DS-GVO, insbesondere gegen den Grundsatz der Datenminimierung, dar. Zudem sei eine wirksame Rechtsgrundlage für diese Datenverarbeitung nicht ersichtlich und es fehlt an einer Information der Betroffenen über die Datenverarbeitung. Das LAG sah einen Verstoß gegen die dem Betriebsratsvorsitzenden aus § 79a S. 1 BetrVG obliegenden Pflichten bei der Verarbeitung personenbezogener Daten.

Maßnahmen für Arbeitgeber

Aus datenschutzrechtlicher Sicht sollte allen Mitarbeitern generell untersagt werden, dienstlicher E-Mails an private E-Mail-Konten weiterzuleiten.

Denn: Bezüglich aller personenbezogenen Daten, die der Arbeitgeber als verantwortliche Stelle verarbeitet, haftet dieser grundsätzlich für Rechtsverletzungen. Gem. Art. 32 DS-GVO (§§ 26, 27 KDG) ist der Verantwortliche verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um so die Datensicherheit zu gewährleisten.

Genau solche Sicherheitsmaßnahmen werden bei einer Weiterleitung an private E-Mail-Accounts gerade umgangen. Der Versand von geschäftlichen E-Mails auf private Accounts stellt daher einen Datenschutzverstoß dar. Hinzukommt, dass dienstliche personenbezogene Daten, die auf private E-Mail-Accounts weitergeleitet und dort verarbeitet werden, kaum vom Arbeitgeber im Rahmen von Betroffenenanfragen berücksichtigt werden können.

Fazit:

Sämtliche Mitarbeiter sollten von einer Weiterleitung dienstlicher E-Mails auf private E-Mail-Konten absehen, um Datenschutzverstöße zu vermeiden. Arbeitgeber sollten die Nutzung privater E-Mail-Accounts im beruflichen Kontakt, z.B. über eine Richtlinie, ausdrücklich verbieten.

6.7 Vorlage erweiterter Führungszeugnisse bei Sozialhilfeträgern

Ein caritativer Verband bietet als Leistungserbringer über sein Beratungszentrum eine Migrationsberatung für erwachsene Zugewanderte an. Die dort beschäftigten Personen wurden aufgefordert, dem verantwortlichen Verband ein erweitertes Führungszeugnis vorzulegen.

Der Verband sieht sich zu einer solchen Anforderung berechtigt und verweist dafür auf die Präventionsordnung der deutschen Bischofskonferenz sowie die dazu erlassenen Ausführungsbestimmungen, die beide im dem betroffenen Bistum in Kraft gesetzt worden sind und auf § 75 SGB XII beruhen.

Unsere Behörde vertrat die Ansicht, dass für eine solche Vorlagepflicht, die einen Eingriff in den Persönlichkeitsbereich der Beschäftigten darstellt, die von dem verantwortlichen Verband dargelegten rechtlichen Grundlagen nicht geeignet sind.

Ein erweitertes Führungszeugnis enthält zunächst die Eintragungen eines „einfachen“ Führungszeugnisses nach § 30 BZRG und ist ggf. erweitert um Eintragungen zu Sexualstraftaten.

Eine allgemeine Pflicht zur Vorlage eines Führungszeugnisses besteht nicht und würde die von der Rechtsprechung entwickelten Grundsätze zum

Fragerecht aushöhlen. Durch die verpflichtende Vorlage eines Führungszeugnisses könnte der Arbeitgeber Kenntnisse erlangen, die ihm durch die von der Rechtsprechung entwickelten Einschränkungen des Fragerechts verwehrt blieben. § 12 KDG schränkt deshalb die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten und damit in Zusammenhang stehende Sicherungsmaßregeln auf die Fälle, nach denen sie durch kirchliches oder staatliches Recht verarbeitet werden dürfen, ein.

Um sicher zu stellen, dass Personen, die rechtskräftig wegen einer Straftat nach den §§ 171, 174 bis 174c, 176 bis 180a, 181a, 182 bis 184g, 184i, 201a Absatz 3, den §§ 225, 232 bis 233a, 234, 235 oder 236 des Strafgesetzbuchs verurteilt worden sind, nicht im Bereich der Kinder- und Jugendarbeit tätig werden, sollen sich die Arbeitgeber zu diesem Zweck bei der Einstellung oder Vermittlung und in regelmäßigen Abständen von den betroffenen Personen ein Führungszeugnis nach § 30a Abs. 1 BZRG vorlegen lassen. Das erweiterte Führungszeugnis ist als zielgerichtete Maßnahme für alle kinder- und jugendnahen Tätigkeiten eingerichtet worden. Nur Personen, die in diesem Bereich tätig sind, dürfen verpflichtet werden, ein erweitertes Führungszeugnis vorzulegen.

Dies bestätigen auch die Ausführungsbestimmungen zur Rahmenordnung, wenn dort in § 5 Abs. 2 gefordert wird, dass alle Mitarbeiter und Mitarbeiterinnen „soweit sie Kontakt zu Jugendlichen … oder zu Erwachsenen mit Behinderung in Einrichtungen und Diensten nach § 75 SGB XII haben“, verpflichtet sind ein erweitertes Führungszeugnis vorzulegen.

Personen, die die Migrationsberatung für erwachsene Zugewanderte aufsuchen, können nicht zu diesem Personenkreis gehören.

Die zuständige Landeshauptstadt, als Träger der Sozialhilfe, bestand jedoch dennoch auf einen Nachweis des erweiterten Führungszeugnisses. Da die Landeshauptstadt außerhalb unserer Zuständigkeit lag, baten wir die Landesbeauftragte mit der Landeshauptstadt zu klären, ob ein erweitertes Führungszeugnis auch dann vorzulegen sei, wenn der Personenkreis, den die entsprechende Vorschrift schützen soll, nicht betroffen ist.

Gegenüber der Landesbeauftragten berief sich die Landeshauptstadt auf § 75 Abs. 2 SGB XII. Nach dieser Vorschrift dürfen geeignete Leistungserbrin-

ger nur Personen beschäftigen, die ein erweitertes Führungszeugnis vorgelegt haben.

Der Leistungserbringer darf jedoch nur den Umstand der Einsichtnahme, das Datum des Führungszeugnisses und die Information, ob die das Führungszeugnis betreffende Person wegen einer in Satz 3 genannten Straftat rechtskräftig verurteilt worden ist, speichern. Die Weitergabe des erweiterten Führungszeugnisses an die Landeshauptstadt darf ebenso wenig erfolgen, wie die Speicherung des Führungszeugnisses bei der Personalakte.

Das Verlangen der Verantwortlichen zur Vorlage eines erweiterten Führungszeugnisses ist somit zunächst rechtmäßig. Es sind aber weitere Voraussetzungen zu schaffen, um einen datenschutzkonformen Umgang mit diesen Zeugnissen bei der Verantwortlichen zu gewährlisten.

6.8 Datenschutzvorfälle

6.8.1 Falscher Drucker für Personaldaten

Ein Trägerverband betreibt mehrere katholische Altenpflegeheime. Die Einrichtungen sind mit ihrer IT, zu denen auch die Drucker zählen, auf einem Server eingebunden. Dadurch ist es technisch auch möglich Druckaufträge von einer Einrichtung auf Druckern anderer Einrichtungen auszudrucken.

Auch der Personalabteilung war es möglich Ausdrucke auf allen Druckern in den anderen Einrichtungen anzufertigen, so dass es in Folge dessen zu einer Datenschutzverletzung gekommen ist. Ein Mitarbeitender der Personalabteilung hatte 2 Ausdrucke mit Pfändungsbeträgen eines Mitarbeiters versehentlich in einer anderen Einrichtung ausgedruckt. Die Ausdrucke nahmen dort der Einrichtungsleiter und ein Verwaltungsmitarbeiter zur Kenntnis, da sie die Ausdrucke dem Drucker entnommen haben.

Bei Finanzdaten, so auch Pfändungsbeträge, handelt es sich um personenbezogene Daten, die der Datenschutzklasse III nach § 13 KDG-DVO einzuordnen sind. Deren Missbrauch kann den Betroffenen in seiner gesellschaftlichen Stellung erheblich beeinträchtigen.

Auch wenn die Einrichtung angegeben hat, dass die Mitarbeitenden, die die Ausdrucke zur Kenntnis genommen haben, zur Verschwiegenheit verpflichtet sind und den betroffenen Mitarbeitenden nicht kennen, haben wir die Auflage erteilt, den Betroffenen über diese Datenschutzverletzung zu informieren.

Im Zuge dieses Vorfalls hat die Verantwortliche das Verfahren zum Ausdruck von Personalunterlagen umgestellt. Den Mitarbeitenden der Personalabteilung steht nur noch der zentrale Drucker mit Druckboxen zur Verfügung. Somit wird wirksam verhindert, dass Ausdrucke der Personalabteilung in anderen Einrichtungen, auch nicht mehr versehentlich, ankommen.

Fazit:

Auch wenn es praktisch erscheint, dass Ausdrucke einrichtungsübergreifend angefertigt werden können, so sind trotzdem die Informationen nicht außeracht zu lassen, die später auf den Ausdrucken sein können. Eine Einordnung aller druckbaren personenbezogener Daten in Datenschutzklassen sollte daher vor Inbetriebnahme der Drucker vorgenommen werden. Anhand dieser kann dann ein entsprechendes Schutzniveau festgelegt und umgesetzt werden. Denn auch der Ausdruck von personenbezogenen Daten auf einem Blatt Papier ist immer eine Verarbeitung i. S. d. § 4 Nr. 3 KDG.

6.8.2 Vervielfältigen von Personalunterlagen durch die MAV[72]

Auf dem Parkplatz vor einer Einrichtung sind zwei Ausdrucke einer E-Mail gefunden worden. Nach den Angaben des Verantwortlichen handelt es sich bei dem Inhalt der Ausdrucke um Daten aus einem Beteiligungsverfahren zu einer personellen Einzelmaßnahme. Dabei gingen aus den Ausdrucken folgende personenbezogenen Daten hervor: Name, Geburtsdatum, Berufsausbildung und Eingruppierung der betroffenen Person.

Weiterhin ging aus den Ausdrucken auch das Abstimmungsergebnis der MAV-Beratung hervor. Deshalb geht der Verantwortliche davon aus, dass ein MAV-Mitglied diese Ausdrucke verloren hat.

Der MAV-Vorsitzende teilt mit, die ihm vom Arbeitgeber im Anhörungsverfahren per Brief zugesandten Unterlagen würden von ihm kopiert und den MAV-Mitgliedern zur Verfügung gestellt.

1. Mitteilung des Arbeitgebers der personenbezogenen Daten an die MAV

Unterrichtet der Arbeitgeber die MAV über eine beabsichtigte personelle Einzelmaßnahme, übergibt er ihr dabei personenbezogene Daten von Beschäftigten i. S. v. § 4 Nr. 24 KDG.

72 Ullrich, in: ZMV 2025, 306 ff. „Die Verarbeitung personenbezogener Daten im Bereich der MAV“

Die Unterrichtung stellt eine Verarbeitung i. S. v. § 4 Nr. 3 KDG in Form der Offenlegung durch Übermittlung dar.

Diese Verarbeitung ist nur rechtmäßig, wenn sie durch eine Regelung des KDG erlaubt ist.

Gemäß § 34 MAVO bedürfen Einstellungen der Zustimmung der Mitarbeitervertretung (MAV). Das gleiche gilt für weitere personelle Einzelmaßnahmen gem. § 35 MAVO, wie z. B Ein- und Höhergruppierungen, Abordnung von mehr als drei Monaten oder Versetzung an eine andere Einrichtung. Auch nach § 42 MVG-EKD bedarf die jeweilige Maßnahme der Zustimmung der MAV.

Der Arbeitgeber muss vor der Durchführung der beabsichtigten Maßnahme die MAV unterrichten und ihre Zustimmung beantragen (§ 33 Abs. 2 S. 1 MAVO). Die Mitteilung erfolgt durch Übermittlung personenbezogener Daten durch den Dienstgeber an die MAV.

Zur Entgegennahme von Erklärungen sind Vorsitzende, Stellvertreter oder ein von der MAV benanntes Mitglied berechtigt (§ 14 Abs. 1 MAVO).

Diese Verarbeitung ist gem. § 53 Abs. 1 KDG rechtmäßig, da sie für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach dessen Begründung für die Durchführung oder Beendigung erforderlich ist.

2. Verfahren innerhalb der MAV

Das Kopieren oder Einscannen von personenbezogenen Daten sowie das Ausdrucken stellen jeweils eine Verwendung und mithin eine Verarbeitung i. S. v. § 4 Nr. 3 KDG dar. Wird die Unterrichtung der MAV vom Arbeitgeber durch Übersendung einer E-Mail an das MAV-Postfach vorgenommen und vom Empfangsberechtigten (regelmäßig dem Vorsitzenden) an die persönliche E-Mail-Adresse (auch die dienstliche) einzelner Mitglieder weitergeleitet, stellt dies eine Verbreitung bzw. eine Offenlegung durch Übermittlung und somit ebenfalls eine Verarbeitung i. S. v. § 4 Nr. 3 KDG dar. Eine solche Verarbeitung ist nur bei Vorliegen einer Rechtsgrundlage rechtmäßig.

Das Anfertigen von Kopien für die einzelnen MAV-Mitglieder kann nicht auf § 53 KDG gestützt werden, da sie nicht für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Eine andere Rechtsgrundlage ist ebenfalls nicht ersichtlich.

Wenn das Gesetz die Übergabe der Unterlagen an die einzelnen MAV-Mitglieder nicht vorsieht, ist die Verarbeitung nicht notwendig. Die Verarbeitung muss zwingend für die Erreichung des Zwecks erforderlich sein. Reine Nützlichkeit reicht nicht aus!

Hätte sich die MAV an die Vorschriften des Datenschutzgesetzes gehalten und über die vom Arbeitgeber vorgelegten Unterlagen nur in der MAV-Sitzung beraten, wäre der beschriebene Datenschutzverstoß nicht eingetreten.

Hinweis: Die KDSA Ost wird verstärkt den Datenschutz bei Mitarbeitervertretungen in den Fokus nehmen. Dabei wird ein Schwerpunkt auf das Vorhandensein von Datenschutzkonzepten bei den MAV'en liegen. Solche werden nach § 26 c der Neuregelung zur MAVO ausdrücklich gefordert.

7 Technische Datenschutzprüfungen

In der heutigen digitalen Welt, in der personenbezogene Daten in großem Umfang verarbeitet werden, ist der Schutz dieser Daten von größter Bedeutung. Technische Datenschutzprüfungen spielen eine entscheidende Rolle dabei, sicherzustellen, dass Einrichtungen, Betriebe und Organisationen die geltenden Datenschutzgesetze einhalten.

Technische Datenschutzprüfungen sind systematische Überprüfungen der technischen und organisatorischen Maßnahmen, die Unternehmen implementiert haben, um personenbezogene Daten zu schützen. Diese Prüfungen können verschiedene Formen annehmen, darunter z.B.:

- Audits: Umfassende Bewertungen der Datenverarbeitungspraktiken
- Inspektionen: Vorort-Prüfungen der Sicherheitsmaßnahmen
- Überprüfungen von IT-Systemen: Technische Analysen der eingesetzten Systeme und Software

Die Prüfungen dienen der Kontrolle, ob ein Verantwortlicher (z.B. eine Einrichtung, ein Betrieb oder eine Organisation) die technischen und organi-

satorischen Maßnahmen nach § 26 KDG (Art. 32 DS-GVO) korrekt umsetzt. Im Fokus stehen u. a.:

- IT-Sicherheit und Verschlüsselung
- Zugriffskontrollen und Protokollierung
- Speicherung und Löschung personenbezogener Daten
- Konfiguration von Webservern oder E-Mail-Systeme und Anwendungen
- Einbindung von Drittanbietern (z. B. Trackingdienste)

Solche Prüfungen erfolgen teils vor Ort, zunehmend aber auch remote durch Auswertung technischer Merkmale, etwa durch die Analyse von öffentlichen Web-/Internetschnittstellen, Subdomains oder mobilen Anwendungen. Sie können aber auch auf Systeme im Netzwerk des Verantwortlichen ausgeweitet werden, wenn dies zur Überprüfung der Einhaltung der Datenschutzgesetze erforderlich ist.

Erlaubt der Verantwortliche die Datenverarbeitung auch auf privaten Endgeräten und im Homeoffice, so ist auch hier die Aufsichtsbehörde befugt, Überprüfungen durchzuführen.[73]

Datenschutzaufsichtsbehörden haben somit auch im technischen Bereich weitreichende Prüf- und Auskunftsrechte, wenn sie auf der Grundlage von gesetzlichen Befugnissen handeln, die ihnen durch nationale und kirchliche Datenschutzgesetze verliehen werden. Die Zulässigkeit technischer Datenschutzprüfungen ist somit in den Datenschutzgesetzen verankert.

Fazit:

Technische Datenschutzprüfungen sind ein unverzichtbarer Bestandteil eines effektiven Datenschutzmanagements. Sie ermöglichen es, die Sicherheit personenbezogener Daten zu gewährleisten und die Einhaltung der Datenschutzgesetze sicherzustellen.

7.1 IT-Labore für technische Überprüfungen

IT-Labore sind technische Einheiten, die u.a. auch von Datenschutzaufsichtsbehörden betrieben werden, um IT-Systeme und -Dienste proaktiv

73 https://www.KDSA Ost.de/aktuelles/datenschutzpruefung-im-home-office-oder-auf-privaten-geraeten.html

auf Datenschutzkonformität und Sicherheit zu überprüfen. Sie dienen dazu, technische Sachverhalte im Umfeld der Verarbeitung personenbezogener Daten praxisnah nachzustellen und zu analysieren.

Funktionen und Ziele der IT-Labore:

- **Technische Prüfung**: Überprüfung der Sicherheit von Webseiten und mobilen Anwendungen in Bezug auf die Verarbeitung personenbezogener Daten.
- **Schwachstellenanalyse**: Proaktive Analyse von Schwachstellen, die über das Internet erreichbar sind (wie z.B. Exchange).
- P**raxisnahe Überprüfung**: Nachstellen technischer Sachverhalte, um Datenschutzverstöße besser bewerten zu können.
- **Forensische Analyse**: Analyse von Daten und Datenträgern. Dazu gehört u.a. die Analyse von Phishing-Methoden, wie z.B. E-Mails, zur Vermeidung von Datenpannen.

Es gibt spezielle Treffen, an denen die KDSA Ost mitwirkt, bei denen sich IT-Expertinnen und -Experten der verschiedenen Datenschutzbehörden austauschen und praxisnah zusammenarbeiten.

7.2 Technische Überprüfungen – anlasslos

7.2.1 Websites

Mit zunehmender Digitalisierung sind Formulare zu einem festen Bestandteil von Webseiten geworden. Allerdings bleiben diese für Kriminelle nicht verborgen. Nach einer erfolgreichen Analyse, setzen sie überwiegend raffinierte Automatismen (Robots) zum Missbrauch ein. Dabei spielt es keine große Rolle, um welche Art von Formularen es sich handelt, wie z.B. zur Benutzerregistrierung, Newsletter-Anmeldung, Kontaktformular, etc.

Um dem Missbrauch an ihren Webanwendungen vorzubeugen, rüsten einige Webseitenbetreiber diese mit zusätzlichen Plugins aus.

Auffälligkeiten CleanTalk

Einige überprüfte Websites setzen CleanTalk.org ein. Das ist ein Anti-Spam-Dienst, der sich nahtlos in verschiedene Content-Management-Systeme

(CMS) wie WordPress, Joomla und Drupal integriert. Ziel ist es, Spam-Kommentare und -Anfragen zu reduzieren und Websites vor böswilligen Angriffen zu schützen. Dadurch kommt es zu Datenübermittlungen an einen weiteren Dritthost.

Fazit: Sensibilisierung 2026

Website-Betreiber sollten unbedingt die Datenschutzbestimmungen und die rechtlichen Grundlagen prüfen, um diese vollständig zu erfüllen.

```
HTTPS OPT… ….cleantalk.org /api3.0/frontend_data          204
HTTPS POST ….cleantalk.org /api3.0/frontend_data          200 …pli
```

7.2.2 E-Mail

Ähnlich wie bei Websites, werden auch bei der E-Mail-Kommunikation Sicherheitsmechanismen von externen Dienstleistern als Service eingekauft.

Ein am Markt bekannter Dienstleister ist u.a. Hornetsecurity, der bei unseren Überprüfungen zum Einsatz kam. Im Berichtsjahr (Dezember 2025) wurde die Übernahme von Hornetsecurity durch Proofpoint bekannt. Proofpoint ist ein US-amerikanisches Unternehmen.

```
Received: from mx-relay21-hz1-if1.hornetsecurity.com
([94.100.128.31])
```

Fazit: Sensibilisierung 2026

Nutzer sollten die spezifischen Bedingungen und Vereinbarungen prüfen, um sicherzustellen, dass weiterhin alle Anforderungen erfüllt sind.

7.3 E-Mail-Kommunikation

7.3.1 Die unsichtbare Spam-Welle – Warum wir plötzlich fremde Autoresponder erhalten?

Rätselhafte Antworten statt offensichtlicher Hacks

Im aktuellen Berichtsjahr berichten Nutzer vermehrt über ein rätselhaftes Phänomen: Ihre Postfächer füllen sich mit automatischen Abwesenheits-

notizen, Systembestätigungen und manchmal sogar persönlichen Antworten auf Nachrichten, die sie nie verschickt haben. Der erste Gedanke – ein gehacktes E-Mail-Konto oder ein kompromittierter Mailserver – liegt nahe. Doch in den meisten aktuellen Fällen trifft diese Annahme nicht zu. Die Ursache ist subtiler und entfaltet ihre Wirkung über einen scheinbar legitimen Weg: Google Gruppen.

Wie die Spam-Welle technisch funktioniert?

Google Gruppen ist ein Dienst zur Verwaltung von Mailinglisten und Diskussionsforen. Nachrichten, die an eine Gruppenadresse gesendet werden, werden von Google automatisch an alle eingetragenen Mitglieder verteilt. Das Problem: Viele Tausende dieser Gruppen sind öffentlich oder so konfiguriert, dass auch Nicht-Mitglieder Nachrichten an sie senden können.

Spammer nutzen diese Lücke aus. Sie tragen fremde E-Mail-Adressen in diese Gruppen ein oder verwenden sie als Absenderadresse für ihre Spam-Nachrichten, die sie an die Gruppe schicken. Da die Nachrichten über die seriöse Google-Infrastruktur laufen, erscheinen sie für Empfänger und Filtersysteme technisch einwandfrei und legitim.

Warum Ihr Postfach mit Antworten überflutet wird?

Die Konsequenz dieser Methode ist ein indirekter Spam-Effekt:

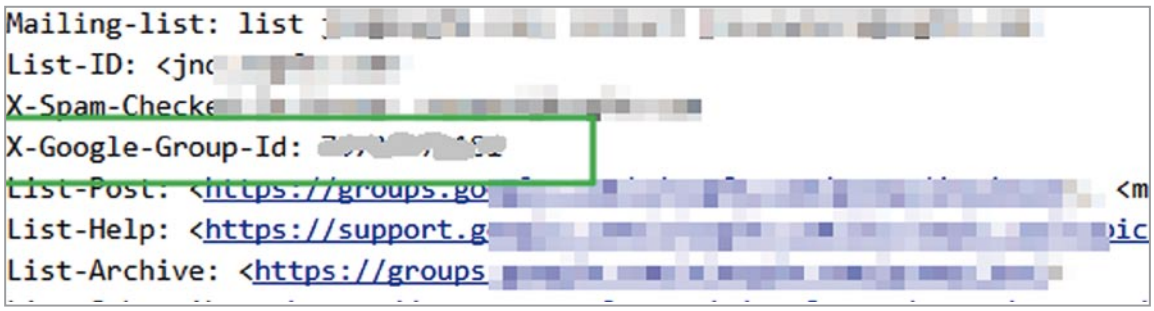
1. Ihre E-Mail-Adresse erscheint als Absender einer Nachricht an Hunderte von Gruppenmitgliedern.
2. Empfänger, deren Systeme automatische Empfangsbestätigungen, Abwesenheitsnotizen (Out-of-Office) oder Ticket-System-Antworten versenden, schicken diese nun an Sie.
3. In besonders unglücklichen Fällen können sich zwei automatische Systeme gegenseitig antworten und eine Endlosschleife auslösen, die manuell unterbrochen werden muss.

Der Nutzer wird so zum unfreiwilligen Empfänger der Reaktionen auf Spam, ohne den ursprünglichen Spam jemals gesehen zu haben.

Wer trägt die Verantwortung und was kann getan werden?

Die Hauptverantwortung für das Problem liegt in der Konfiguration der Google Gruppen. Viele Gruppen, oft ältere oder unmoderierte, haben zu offene Einstellungen. Hier ist Google gefordert, durch strengere Standardeinstellungen oder die automatische Deaktivierung inaktiver, offener Gruppen gegenzusteuern.

Für Betroffene gibt es leider wenige direkte Abwehrmöglichkeiten, da der Spam nicht aus einer identifizierbaren Quelle auf sie zukommt. Eine proaktive Maßnahme für technisch versierte Administratoren oder Nutzer mit entsprechenden Filtertools ist das Prüfen der „E-Mail-Header". Spam-Nachrichten, die über Google Gruppen laufen, tragen oft den Header „X-Google-Group-Id:". Filterregeln, die Nachrichten mit diesem Header markieren, in einen separaten Ordner verschieben oder direkt löschen, können Abhilfe schaffen.



Fazit: Ein Fall von indirektem Spam

Die aktuelle Welle zeigt eine evolutionäre Anpassung der Spammer. Sie nutzen legitime Dienste, um ihre Aktivitäten zu verschleiern und die Last ihrer Aktion auf die Infrastruktur und die Zeit der Betroffenen abzuwälzen. Während man auf Anpassungen von Google-Gruppen-Einstellungen hofft, bleibt für Nutzer vorerst nur das Wissen um den Mechanismus – und die Beruhigung, dass ihr eigenes Postfach sehr wahrscheinlich nicht gehackt wurde, sondern Opfer eines indirekten und besonders lästigen Spam-Tricks geworden ist.

Wer kann oder wo die Technik es zulässt, könnte ein Filter helfen, z.B. der „X-Google-Group-Id" im E-Mail-Header prüft und ggfs. solche Nachrichten kennzeichnet oder gar nicht erst annimmt.

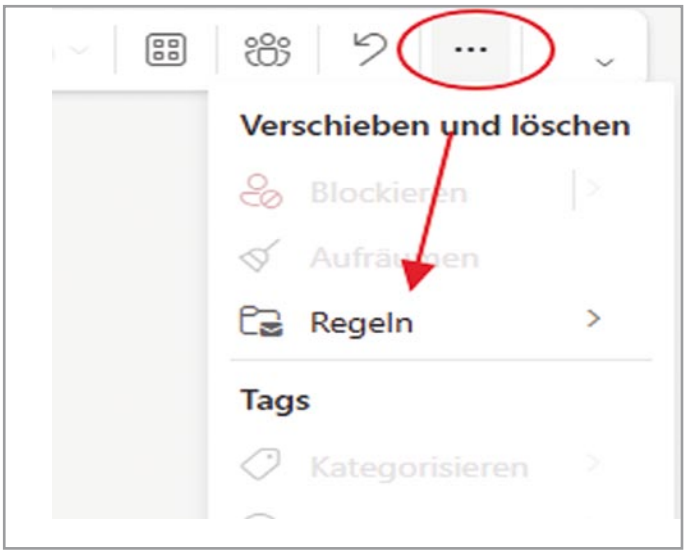
Beispiel für eine Filter-Regel in Outlook-Web (OWA):

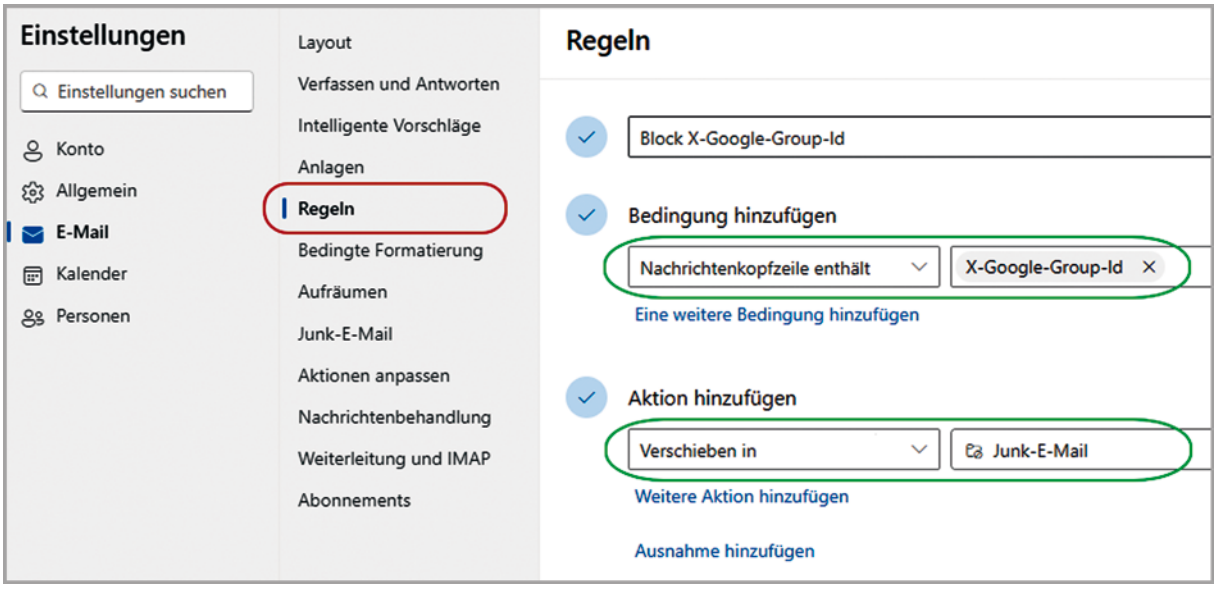
Über das Menü eine neue Regel nachfolgender Bedingung erstellen:

`Nachrichtenkopfzeile enthält`

`X-Google-Group-ID`

Einziger Nachteil ist, alle Nachrichten, die diese Bedingung erfüllen, werden in den „Junk-E-Mail“ Ordner verschoben.





7.3.2 Ein „Bcc“ Missverständnis auf den Punkt gebracht

Datenschutzaufsichten raten in bestimmten Kontexten zu „Bcc“ (versteckter Empfänger) – aber dies gilt explizit NICHT für Newsletter oder systematische Mailings, sondern für die ad-hoc Kommunikation in kleinen bis mittleren Gruppen (z.B. innerhalb eines Vereins oder mit einer Kundengruppe). Folgende Erklärung gibt es für die differenzierte Einordnung:

1. Das spezifische Szenario der Empfehlung

Das Problem, das Datenschutzaufsichten adressieren, ist der **„offene Verteiler“ - oder die „Cc-Datenpanne“!**

Szenario: Jemand schickt eine E-Mail an 30 Teilnehmer eines Kurses und setzt alle Adressen sichtbar ins „Cc-Feld“. Dadurch erfährt jeder Empfänger die E-Mail-Adressen aller anderen – eine unzulässige Weitergabe personenbezogener Daten ohne Rechtsgrundlage.

Lösungsempfehlung datenschutzfreundlich: In genau diesem Fall sollte der Absender das „Bcc“ Feld nutzen, um die Privatsphäre der Empfänger zu schützen. Jeder erhält die Nachricht, sieht aber keine anderen Adressen.

In diesem spezifischen Kontext ist der Rat der Aufsichten absolut korrekt und die einzig datenschutzkonforme Methode mit Standard-E-Mail-Programmen.

2. Der Unterschied zum Newsletter / Massenversand

Die Empfehlung der Datenschutzaufsichten bezieht sich nicht auf den wiederkehrenden, systematischen Versand an viele Personen (Marketing, Information, Rundschreiben). Hier gelten andere Maßstäbe:

- „Bcc“ ist keine angemessene Lösung, da die technischen und praktischen Grenzen (Limits, etc.) greifen. Ein Versand an hunderte Bcc-Empfänger kann zur Ablehnung der gesamten Nachricht an alle Adressaten führen.
- Risiko für Spam-Filter: Ein einzelner E-Mail-Header mit extrem vielen Bcc-Empfängern kann Spam-Filter misstrauisch machen und die Zustellrate verringern.
- Das manuelle Pflegen und Einfügen langer Empfängerlisten in das Bcc-Feld ist ineffizient und fehleranfällig.
- Einrichtung eines automatisierten, zuverlässigen Abmeldeverfahrens (Opt-out) – mit „Bcc“ ist kaum praktikabel umsetzbar. Das betrifft u.a. auch die Nachweispflicht, wer wann eingewilligt hat.

3. Die Wahl der richtigen Technik hängt vom Zweck und Umfang ab:

Anwendungsfall	Empfohlene Methode	Warum?
Einmalige E-Mail an eine geschlossene Gruppe** (z.B. Kurs-Teilnehmer, Vereinsmitglieder)	Bcc (im Standard-E-Mail-Client)	Schützt die Privatsphäre der Empfänger untereinander; einfache, direkte Lösung für ein definiertes Ad-hoc-Szenario.
Regelmäßiger Versand (Newsletter, Kundeninformationen, Marketing)	Dediziertes E-Mail-Marketing-/Newsletter-Tool verwenden	Erfüllt alle Anforderungen an den Datenschutz (Einwilligung, Abmeldung, Dokumentation), ermöglicht Personalisierung, ist technisch robust.
Interne Information an alle Mitarbeiter	Verteilerliste / Verteilergruppe / Mailingliste auf der betrieblichen Umgebung (z.B. Exchange)	Zentrale, verwaltete Liste; Empfänger müssen nicht manuell ausgewählt werden; interne Adressen bleiben geschützt.

Fazit:

Verwendung von „Bcc“ nur für kleine, informelle Gruppen, bei denen es darum geht, die Privatsphäre einer Handvoll Empfänger untereinander zu wahren. Beispiele: Einladung an mehrere Kunden, die sich nicht kennen sollen.

Für jeden formellen, regelmäßigen oder massenhaften Versand, wie z.B. Newsletter, Kundeninformationen oder Einladungen ist die Nutzung eines dedizierten E-Mail-Tools erforderlich. Es schützt vor Datenpannen, spart Zeit und macht eine Kommunikation messbar und effektiver.

Bei der Verwendung von „Bcc“ wie auch von „To“ oder „Cc“ handelt es sich um eine Nachricht mit ggfs. vielen Empfängern, die an das E-Mail-System übergeben wird. Bei der Verwendung von speziellen Programmen oder ei-

ner Serienbrief-Funktion werden die Nachrichten pro Empfänger als separate E-Mail erstellt.

7.4 E-Mail - Serienbrief mit Outlook und Word

Voraussetzungen für die hier beschriebene Anwendung sind: Outlook, Word und eine Datenquelle mit Kontaktdaten. Diese Variante ist nur für Informationen ohne Anlage geeignet und soll kein Ersatz für eine dedizierte Newsletter-Anwendung darstellen. Rechtlichen Aspekten, wie z.B. die Einwilligung, werden hier nicht weiter betrachtet.

Als Datenquelle kann Excel dienen oder eine Textdatei mit Trennzeichen verwendet werden, zum Beispiel als CSV-Export aus einer anderen Anwendung heraus. Auch können die Kontakte in Outlook als Datenquelle dienen.
Beispiel Datenquelle in Excel

H18

	A	B	C	D	E
1	Vorname	Name	Email	Einwilligung am	
2	Elfrieda	Egbers	elfrieda.egbers@omail.none	26.04.2000	
3	Tabea	Blasius	t-blasius@open-mail.none	22.11.1922	
4	Evelinde	Schrewe	evelindeschrewe@justmail.none	01.03.2018	
5	Edda	Hinke	eddahinke@omail.none	11.08.2017	
6	Gunthard	Hardy	gunhard@justmail.none	02.11.2017	
7	Reinholdine	Wolber	reinholdine_17@funmail.none	26.01.1948	
8	Roger	Mertens	roger-mertens@ultramail.none	19.11.2013	
9				11.12.2018	
10	Diese Daten sind Dummy-Daten!				

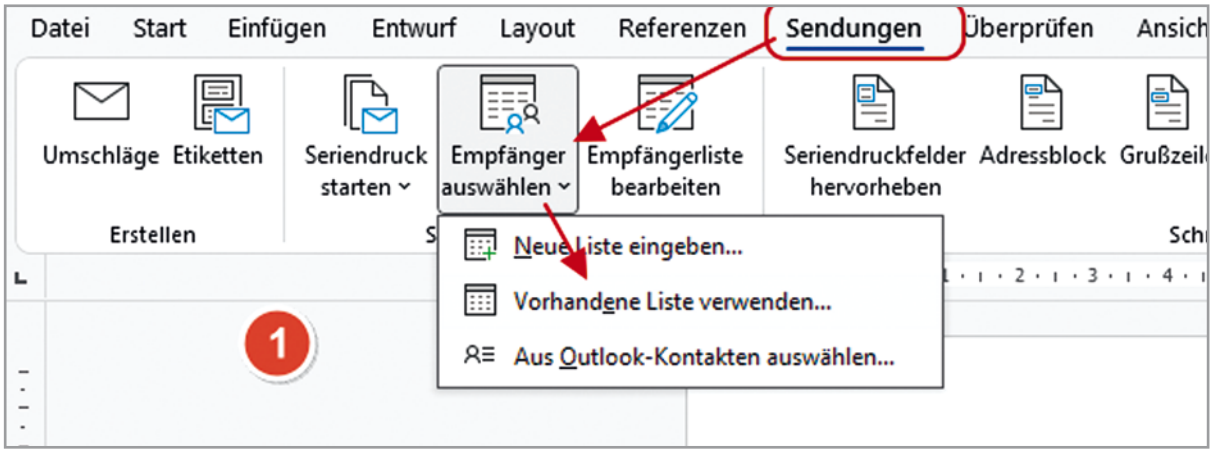
Beispiel Datenquelle in Textdatei

Serienmail.csv.txt.csv

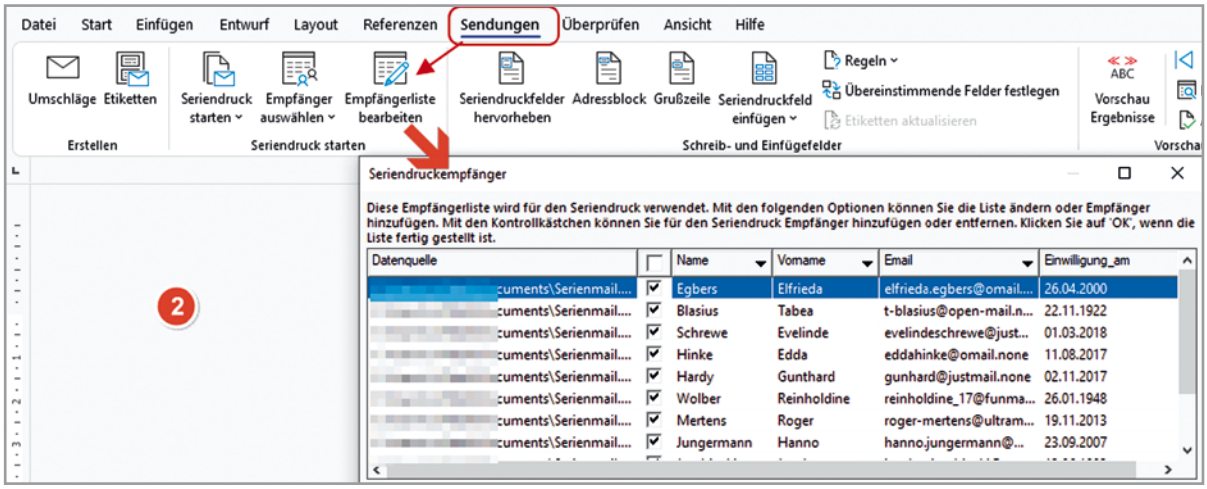
```
Vorname;Name;Email;Einwilligung am
Elfrieda;Egbers;elfrieda.egbers@omail.none;26.04.2000
Tabea;Blasius;t-blasius@open-mail.none;22.11.1922
Evelinde;Schrewe;evelindeschrewe@justmail.none;01.03.2018
Edda;Hinke;eddahinke@omail.none;11.08.2017
Gunthard;Hardy;gunhard@justmail.none;02.11.2017
Reinholdine;Wolber;reinholdine_17@funmail.none;26.01.1948
Roger;Mertens;roger-mertens@ultramail.none;19.11.2013
Hanno;Jungermann;hanno.jungermann@mymail.none;23.09.2007
Joschua;Jaschinski;joschuajaschinski@open-mail.none;13.06.1983

Diese Daten sind Dummy-Daten!;;;
```

Die Information, die per E-Mail an die Empfänger aus der Datenquelle versendet werden soll, wird in Microsoft Word geschrieben. Am einfachsten gestaltet sich dies mit einer Vorlage, die speziell für den E-Mail-Versand mit vorbereiteten „Platzhaltern“ erstellt wurde.

Sobald der Text fertiggestellt ist, kann die Datenquelle unter dem Menü „Empfänger auswählen“ eingebunden werden (Bild 1).

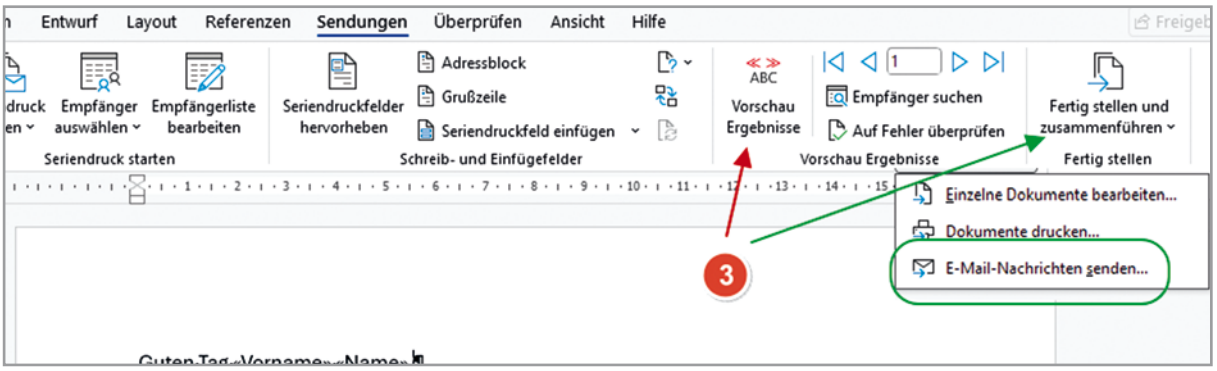


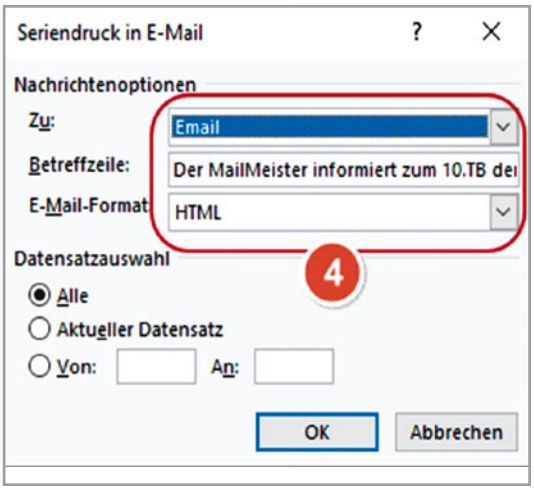
Zur Kontrolle, ob es sich um die richtigen Empfänger handelt oder falls die E-Mail nicht an alle Empfänger gesendet werden soll, kann die Empfängerliste bearbeitet werden (Bild 2).



Nachdem alle Einstellungen getroffen wurden, kann unter dem Menü „Vorschau Ergebnisse“ überprüft werden, ob die Platzhalter korrekt mit

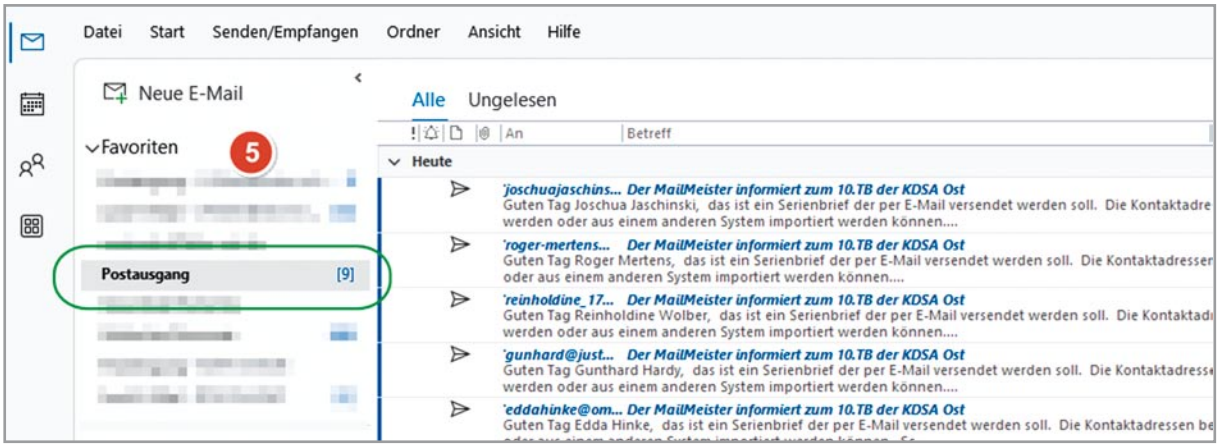
den Daten gefüllt werden. Ein Durchblättern innerhalb der Datenbasis, ist mit den Pfeiltasten möglich (Bild 3).





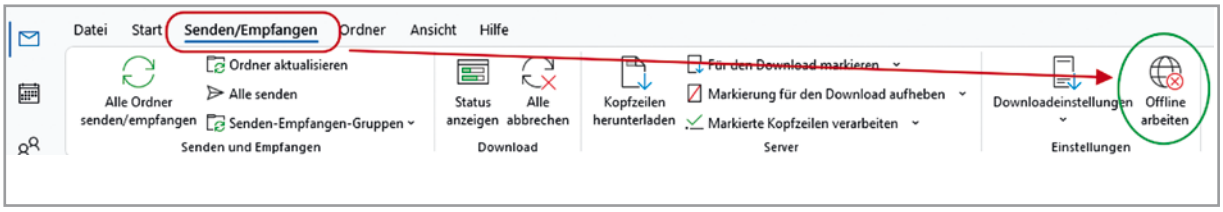
Sobald alles korrekt erscheint, können die Serien-E-Mails im Menü „Fertig stellen und zusammenführen“ generiert und an Outlook übergeben werden. Zuvor erfolgt noch der Eintrag für die Betreffzeile (Bild 4).

Wenn alles korrekt abläuft, befinden sich die Nachrichten im Postausgang von Outlook (Bild 5). Sollte Outlook grundsätzlich Nachrichten automatisch versenden, kann es sein, dass die E-Mails hier zeitnah verschwinden. Eine Kontrolle ist danach unter „Gesendete Elemente“ möglich.



Praxis-Tipp: Damit die Nachrichten nicht automatisch versendet werden, kann vor der Übergabe an Outlook, das Programm in einen „Offline-Mode“ geschalten werden. So erfolgt kein automatischer Versand von Nachrichten

aus dem Postausgangsorder bis der „Offline-Mode“ deaktiviert wird. Ein manuelles Versenden kann z.B. mit der Taste „F9“ gestartet werden.



7.5 E-Mail-Verschlüsselung mit S/MIME nicht ohne Tücken

Regelmäßig kommt das Thema auf, eine E-Mail-Kommunikation ist nicht sicher, E-Mails müssen Ende-zu-Ende verschlüsselt werden.[74] Eine standardisierte Variante ist das zertifikatsbasierte S/MIME Verfahren (Secure/Multipurpose Internet-Mail-Extensions) mit privatem und öffentlichem Schlüssel. Vernachlässigt wird in der Regel eine Unterscheidung zum eigentlichen Inhalt der E-Mail – es wird wie so oft pauschalisiert. Auf die Komplexität und evtl. Fallstrike wird in der Regel nicht weiter hingewiesen.

7.5.1 Schwierigkeiten bei der Langzeitarchivierung von E-Mails mit S/MIME

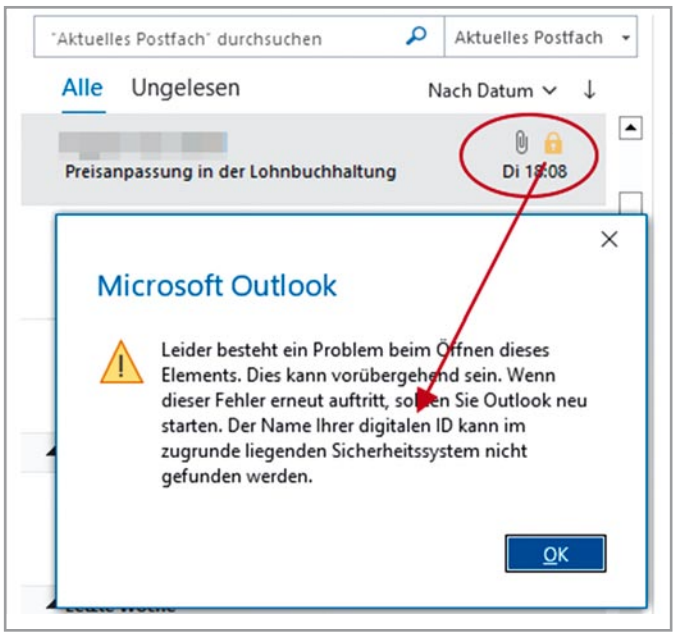
Die Langzeitarchivierung von E-Mails ist ein entscheidendes Thema für viele Organisationen und Verantwortliche, insbesondere hinsichtlich der rechtlichen und geschäftlichen Anforderungen. Während S/MIME eine sichere Methode zur Verschlüsselung und Signatur von E-Mails bietet, birgt sie auch einige Herausforderungen, die die Langzeitarchivierung erschweren.

Ein zentrales Problem bei der Nutzung von S/MIME für die Langzeitarchivierung sind die begrenzten Laufzeiten der digitalen Zertifikate. Jedes S/MIME-Zertifikat hat eine definierte Gültigkeitsdauer, typischerweise von

74 KDSA, TB 2020, Pkt. 7.2 Unterschiedliches Verständnis – Ende-zu-Ende Verschlüsselung

einem bis zu drei Jahren. Nach Ablauf dieser Zeit kann das Zertifikat nicht mehr verwendet werden, das bedeutet u.a.:

- Verlust der Signaturgültigkeit: Eine E-Mail, die mit einem abgelaufenen Zertifikat signiert wurde, wird als nicht mehr gültig angesehen. Dies kann Schwierigkeiten bei der Authentifizierung der E-Mail und ihrer Inhalte mit sich bringen.



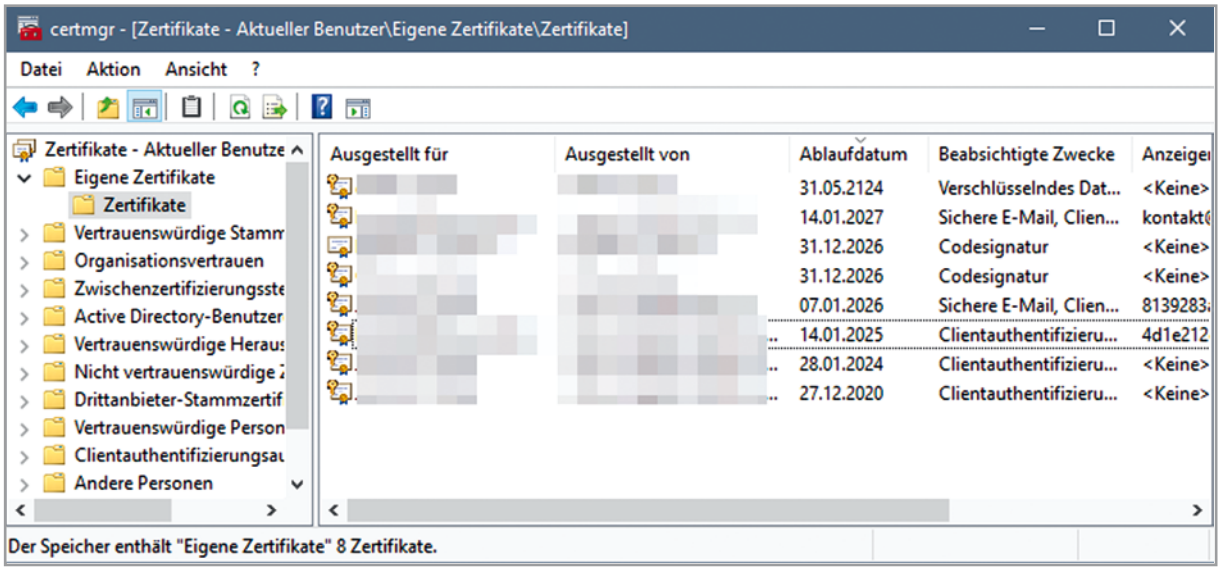
- Schwierigkeiten bei der Entschlüsselung: Nutzer, die versuchen, auf archivierte E-Mails zuzugreifen, bekommen Probleme, diese zu entschlüsseln, sofern das verwendete abgelaufene Zertifikat mit seinem privaten Schlüssel nicht mehr verfügbar ist. Ab diesem Zeitpunkt ist ein Zugriff auf die Inhalte nicht mehr möglich.

7.5.2 Risiken der Zertifikatsverwaltung

Die Verwaltung von S/MIME-Zertifikaten erfordert ständiges Monitoring und administrativen Aufwand. Dies umfasst:

- Regelmäßige Erneuerung: Um die Gültigkeit der Signaturen und deren Entschlüsselungsmöglichkeiten sicherzustellen, müssen die Zertifikate regelmäßig erneuert werden. Dies kann zusätzliche Kosten und Aufwand verursachen.
- Verwaltung mehrerer Zertifikate: In Organisationen, in denen viele Mitarbeiter E-Mails signieren und verschlüsseln, muss der Verantwortliche sicherstellen, dass alle Benutzer rechtzeitig neue Zertifikate erhalten und diese korrekt installieren.
- Probleme mit neuen Systemen: Werden neue Geräte angeschafft oder Geräte neu eingerichtet, fehlen in der Regel alle älteren Daten. Das betrifft u.a. auch alle historischen Zertifikate im Zertifikats-

speicher des Systems. Auf Nachrichten, die mit den älteren Zertifikaten verschlüsselt wurden, ist dann kein Zugriff mehr möglich. Eine Ende-zu-Ende Beziehung durch das Fehlen der Zertifikatskette ist dann nicht mehr vorhanden.



7.5.3 Technische Herausforderungen

Die Implementierung von S/MIME für die Langzeitarchivierung bringt auch technische Herausforderungen mit sich. Dazu gehören:

- **Kompatibilität mit Archivierungslösungen:** Nicht alle E-Mail-Archivierungssysteme unterstützen S/MIME in vollem Umfang. Das kann dazu führen, dass bestimmte E-Mails nicht ordnungsgemäß archiviert oder wiederhergestellt werden können.
- **Archivierungsformate:** E-Mails müssen in einem geeigneten Format gespeichert werden, das sowohl die Signaturen als auch die Verschlüsselungen bewahrt, wodurch die Auswahl der richtigen Archivierungstechnologie einschränkt wird.

Fazit:

Die Langzeitarchivierung von E-Mails, die mit S/MIME gesichert sind, stellt erhebliche Herausforderungen dar, vor allem aufgrund der begrenzten Laufzeit von Zertifikaten.

Es ist notwendig, dass Verantwortliche eine umfassende Strategie entwickeln müssen (durchgängigen Zertifikatsverwaltung), um eine langfristige Verfügbarkeit von E-Mail-Inhalten, u.a. auf Grund längerer gesetzlich vorgeschriebener Aufbewahrungspflichten, zu gewährleisten.

Es ist ratsam, alternative Methoden der E-Mail-Archivierung oder ergänzende Technologien in Betracht zu ziehen, um diese Schwierigkeiten zu überwinden und den rechtlichen Anforderungen gerecht zu werden. Beispielsweise den Inhalt der Nachricht als PDF archivieren oder die E-Mail an ein zentrales Archivierungssystem ohne S/MIME Verschlüsselung weiterleiten.

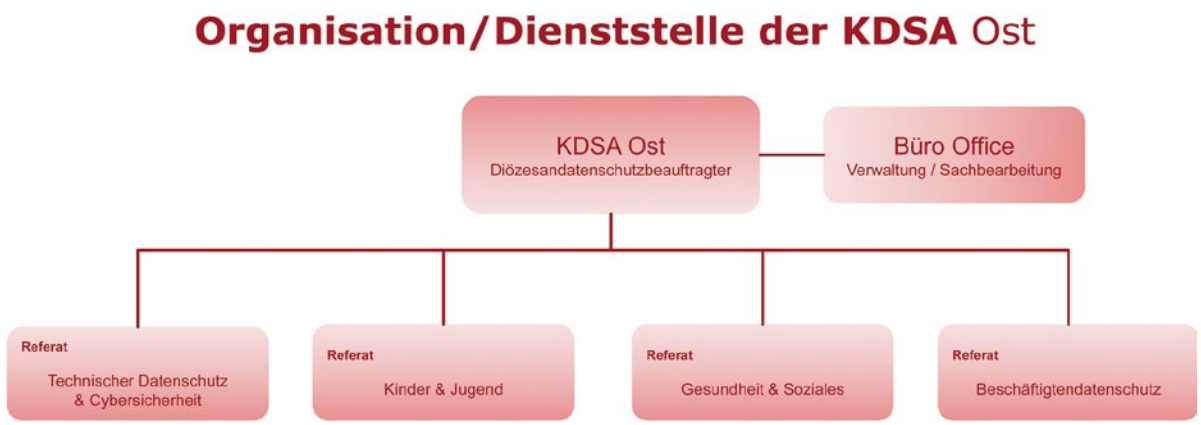
Zu prüfen sind auch datenschutzrechtliche Auswirkungen, z.B. beim Auskunftsanspruch, denn Zertifikate beinhalten in der Regel personenbezogene Daten.

Die Kirchliche Datenschutzaufsicht Ost

KDSA Ost als Dienststelle

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

Organigramm



Unsere Aufgaben und Befugnisse

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

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

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

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

Öffentlichkeitsarbeit

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

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

Auszug aus unseren Veranstaltungen 2025

TOMtalk?! Supportende von Windows 10 (mehrere Termine im Jahr)

Im Oktober 2025 wurde laufzeitbedingt der Support für Windows 10 von Microsoft eingestellt.

Um bei Fragen rund um dieses Thema, gerade bei kleineren Einrichtungen, zu helfen, bieten wir einen speziellen „TOMtalk“ im Rahmen einer Videosprechstunde an.
Die Veranstaltung wurde an mehreren Terminen angeboten.

Veranstaltung Auskunftsverlangen im Datenschutz, Datenverkehr - aber gesichert (Leipzig)

Nachgefragt?! Unsere regelmäßigen Videosprechstunden

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

Veranstaltung „Datenschutz macht Schule“

Gefahrenpotential

Offene Netze (Wlan, etc)

- Spionage bei offenen Funkverbindungen
- Hacker ahmen Websiten nach
- Besser: eigenes Datenvolumen nutzen. Ggf. erhöhen
- Automatisches WLAN deaktivieren

Phishing

- Unterschiedliche Ausprägungen (E-Mail, SMS, QR-Code, u.ä.)

Quishing

- Methoden beim QR-Code
- Gefälschte Codes locken auf präparierte Webseiten
- Verleiten zum Herunterladen von Schadsoftware
- Keine fremden Codes Scannen, ggf. phy-sische Überprüfung (z.B. überklebte QR-Codes)
- Ziel des QR-Codes überprüfen
- Vorsicht bei der Eingabe von persönlichen Daten

KDSA - Kirchliche Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs

Anhang

Auskunftsersuchen gem. § 17 KDG / Art. 15 DS-GVO Handlungsleitfaden

Schritt-für-Schritt-Anleitung zur Beantwortung der Auskunft

Die Beantwortung einer Auskunftsanfrage nach § 17 KDG / Art. 15 DS-GVO erfordert präzise Schritte, um sicherzustellen, dass die Anfrage korrekt und vollständig bearbeitet wird. Hier ist eine strukturierte Anleitung:

1. Eingang der Anfrage

Erfassung der Anfrage: Eingang der Anfrage dokumentieren (Datum, Uhrzeit, Eingangskanal). Bestätigung des Erhalts der Anfrage an den Antragsteller senden.

Identitätsprüfung: Verifikation der Identität des Antragstellers (Kopie des Personalausweises oder andere geeignete Identifikationsdokumente anfordern).

2. Analyse der Anfrage

Anfrageinhalte prüfen / Umfang der Anfrage erfassen: Welche Datenkategorien, welche Verarbeitungstätigkeiten, welche Zeiträume sind betroffen? Prüfung, ob die Anfrage präzisiert werden muss.

3. Sichtung der Daten

Datenerfassung: Ermittlung aller personenbezogenen Daten des Antragstellers in allen relevanten Systemen und Datenbanken. Identifizierung der Datenquellen (intern/extern).

Datenzusammenstellung: Zusammenführung der Daten in einer strukturierten Form. Dokumentation der Datenkategorien, Zwecke der Verarbeitung, Empfänger der Daten, geplante Speicherfristen.

4. Erstellung der Antwort

Inhalt der Auskunft:

- Kopie der verarbeiteten personenbezogenen Daten,

- Informationen über Verarbeitungszwecke,
- Kategorien der personenbezogenen Daten,
- Empfänger oder Kategorien von Empfängern,
- geplante Speicherdauer oder Kriterien für die Festlegung dieser Dauer,
- Informationen über die Herkunft der Daten, falls sie nicht beim Betroffenen erhoben wurden,
- Informationen über das Bestehen eines Rechts auf Berichtigung oder Löschung der Daten,
- Einschränkung der Verarbeitung oder Widerspruch gegen die Verarbeitung; Informationen über das Beschwerderecht bei einer Aufsichtsbehörde,
- Informationen über das Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling, und aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer solchen Verarbeitung.
- Form und Format der Auskunft: Die Auskunft muss in einer klaren und verständlichen Sprache erfolgen; Die Daten sollten in einem gängigen elektronischen Format bereitgestellt werden, sofern die Anfrage elektronisch einging und nichts anderes gewünscht ist.

5. Versand der Auskunft

Übermittlung: unverzüglicher Versand der Auskunft spätestens innerhalb eines Monats nach Eingang der Anfrage; Falls eine Verlängerung notwendig ist (bis zu zwei weitere Monate bei komplexen Anfragen), den Antragsteller innerhalb der ersten Monatsfrist informieren und Gründe für die Verzögerung angeben.

Dokumentation: Dokumentation der übermittelten Auskunft und der verwendeten Kommunikationswege; Aufbewahrung einer Kopie der gesendeten Auskunft für interne Nachweiszwecke.

Dieser Leitfaden soll eine Hilfestellung geben, damit ein Auskunftsersuchen gemäß § 17 KDG / Art. 15 DS-GVO systematisch und entsprechend den gesetzlichen Anforderungen bearbeitet wird.

Prozessregelung für das Erstellen und Verarbeiten von Fotos

Folgende Punkte sollten in einem Dokument enthalten sein:

- **Zweck der Fotos**
  Beschreibung zu welchen Zwecken Fotos in der Einrichtung angefertigt werden.
- **Vorhandensein der Einwilligungserklärung (Rechtsgrundlage / Erlaubnis)**
  Prüfen, ob von der betroffenen Person bzw. dessen Sorgeberechtigten eine Einwilligungserklärung für den Zweck des Fotos erteilt worden ist.
  Informationen, wo die erteilten Einwilligungserklärungen zu finden sind.
- **Mittel zur Erstellung der Fotos**
  Beschreibung der Geräte, mit welchen die Fotos erstellt werden dürfen.
  Hinweis, dass nur dienstliche und keine privaten Geräte erlaubt sind.
- **Verarbeiten der Fotos - Speicherung**
  Übertragungswege, Speichermedien und Speicherdauer der Fotos festlegen.
  Löschfristen für die Fotos festlegen.
- **Verarbeiten der Fotos - Veröffentlichen**
  Bestimmen, in welcher Art und Weise Fotos ausgedruckt werden (eigener Drucker oder Foto-Dienstleister) und in welcher Form sie veröffentlicht werden (Pinwand, Aushang). Weitere Veröffentlichungen (z.B. Zeitung, Webseite) festlegen.
- **Schutzmaßnahmen für Aufnahmegeräte und Speichermedien** Festlegen, durch welche Maßnahmen (Passwörter, Aufbewahrungsorte, Berechtigungen) die Geräte vor unbefugten Zugriff zu sichern sind.
- **Rechte der Betroffenen (Sorgeberechtigte)**
  Hinweis, dass Sorgeberechtigte im Rahmen von Auskunftsersuchen auch die gespeicherten Fotos von ihrem Kind erhalten müssen. Falls die Einwilligung der Sorgeberechtigten widerrufen wird, müssen alle Fotos gelöscht werden, da die Rechtsgrundlage entfällt.
- **Verantwortlichkeiten und Ansprechpartner festlegen**
  Benennen, wer für die Erstellung, Speicherung und Löschen von

Fotos verantwortlich ist. Ggf. Zuständigkeiten festlegen. Neue Kollegen informieren.

Supportende von Windows 10 und weiteren Microsoft Produkten

Das Jahr im Berichtszeitraum war u.a. geprägt vom Auslauf verschiedener Microsoft-Produkte aus dem Support-Lebenszyklus (LifeCycle), darunter auch Windows 10.

Microsoft hat diese Entscheidung getroffen, um den Fokus auf weiterentwickelte Betriebssysteme (z.B. Windows 11) zu legen. Dies hat weitreichende Folgen für alle Nutzer von Windows 10.

Davon betroffen war auch unsere Dienststelle, mit dem Betriebssystem Windows 10 und Microsoft Office 2019 (Offline-Version). Um nicht sofort eine Überprüfung der vorhandenen Systeme für ein Upgrade auf Windows 11 zu starten, wurden Alternativen zu Microsoft angestrebt.

Überblick über die weiteren Schritte:

1. Bestandsaufnahme aller Anwendungen
2. Betrachtung der Lebens-/Produktzyklen von Microsoft Windows
3. Überlegung Linux Arbeitsplatz und Teststellung

	Version	Start	Erweitertes Enddatum
Windows 10	22H2	Okt. 2022	Okt. 2025
Windows 11	24H2	Okt. 2024	Okt. 2026
MS Office 2019		Sept. 2018	Okt. 2025
MS Office 2021		Okt. 2021	Okt. 2026
MS Office 2024		Okt. 2024	Okt. 2029

Zum Stand der Recherche ist Windows 11 nur ein Jahr länger im Support. Es waren keine offiziellen Informationen zu finden, wie es mit Windows 11 weitergeht oder was danach kommen wird.

Überlegung Linux Arbeitsplatz

Bestandsaufnahme (Windows)

- Büroprogramm: MS Office
- Bürokommunikation: MS Outlook für E-Mail, Kalender, Public Postfach, Kontakte
- Aktenverwaltung
- VPN
- Password Safe
- Drucker/Scanner (MFG)
- DATEV Online
- Ggfs. Div. Tools

Test mit Linux Mint und Wine als Alternative

- Büroprogramm: Libre Office
- E-Mail: Thunderbird, Evolution (keine direkte Exchange-Unterstützung, Komfortverlust)
- Aktenverwaltung, Test hat nicht geklappt (wird vom Hersteller nur unter Windows unterstützt)
- VPN
- Password Safe
- Drucker/Scanner
- DATEN Online
- Div. Tools

Überlegungen zum Büroalltag mit Windows 11:

- Windows 11 hat im Business für den, der „nur ein Betriebssystem" für weitere Büroanwendungen benötigt, nicht die Erwartungen erfüllt (es ist u.a. „überfrachtet" (viel weniger installieren ist schwierig bis nicht möglich).
- Die Systemanforderungen sind unbegründete zu hoch – vs. neue Hardware ohne merklichen Nutzen im Büroalltag.
- Die ständigen Future-Updates sind im Büroalltag kaum von Nutzen, sie bringen aber ständig neue „Ungewöhnlichkeiten" mit sich und setzen ggfs. Einstellungen wieder zurück.
- Durch den kürzeren Lebenszyklus (5J) läuft der erweiterte Support nicht viel länger.

Entscheidung

Auf Grund der Testszenarien und aller weiteren Überlegungen und Abwägungen, fiel die Entscheidung auf Microsoft Betriebssystem mit Microsoft Office. Als Betriebssystem wird aktuell das sehr stabile Windows 10 LTSC 2019 eingesetzt, mit Microsoft Office 202475. Beide Komponenten sind damit bis 2029 im Produkt-Zyklus.

Abkürzungen

AEUV	Vertrags über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
ArbG	Arbeitsgericht
ArbZG	Arbeitszeitgesetz
AU	Arbeitsunfähigkeit
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationssicherheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMG	Bundesmeldegesetz
BT.-Drs	Bundestag-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BZRG	Bundeszentralregistergesetz
DDSB	Diözesandatenschutzbeauftragten
DSK	Datenschutzkonferenz
DSK-DBK	Datenschutzgericht der Deutschen Bischofskonferenz
DS-GVO	Datenschutz-Grundverordnung
ePA	elektronische Patientenakte
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
GewO	Gewerbeordnung
GG	Grundgesetz
GrCH	Grundrechtecharta

HinSchG	Hinweisgeberschutzgesetz
HTML	Hypertext Markup Language (Auszeichnungssprache f. Webseiten)
http	Hypertext Transfer Protokoll (unverschlüsselt)
https	Hypertext Transfer Protokoll Secure (verschlüsselt)
IDSG	Interdiözesane Datenschutzgericht
KDG	Kirchliches Datenschutzgesetz
KDG-DVO	Durchführungsverordnung z. Gesetz über den Kirchlichen Datenschutz
KG	Kammergericht
KI	Künstliche Intelligenz
KSchG	Kündigungsschutzgesetz
LAG	Landesarbeitsgericht
LG	Landgericht
MAV	Mitarbeitervertretung
MAVO	Mitarbeitervertretungsordnung
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PAuswG	Personalausweisgesetz
Seelsorge-PatDSG	Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TOM	Technisch organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutzgesetz
VDD	Verband der Diözesen Deutschlands
VG	Verwaltungsgericht
VVT	Verzeichnis von Verarbeitungstätigkeiten

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