



5. Tätigkeitsbericht
Berichtszeitraum 2023 und 2024



Evangelische Kirche
in Deutschland

DER BEAUFTRAGTE FÜR DEN
DATENSCHUTZ DER EKD

**Der Beauftragte für den Datenschutz
der Evangelischen Kirche in Deutschland**

Lange Laube 20
30159 Hannover

Telefon: +49 (0) 511 768128-0

Telefax: +49 (0) 511 768128-20

E-Mail: info@datenschutz.ekd.de

Diesen Tätigkeitsbericht können Sie auch auf unserer Website abrufen unter
<https://datenschutz.ekd.de/ueber-uns/unsere-taetigkeitsberichte>

5. Tätigkeitsbericht

des Beauftragten für den Datenschutz
der Evangelischen Kirche in Deutschland

für die Jahre 2023 und 2024

vorgelegt im Juni 2025

Redaktionsschluss 31. Mai 2025

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Vorwort	4
<hr/>	
Über die Entwicklungen im Datenschutz	7
In der evangelischen Kirche	8
In der römisch-katholischen Kirche	9
In der Bundesrepublik Deutschland	9
Datenschutzrecht des Bundes und der Länder	9
Datenschutzaufsicht des Bundes und der Länder	10
Datenschutzrechtsprechung staatlicher Gerichte	10
In der Europäischen Union	12
Europäisches Datenschutzrecht	12
Datenschutzaufsicht der Europäischen Union	12
Datenschutzrechtsprechung des Europäischen Gerichtshofs	12
<hr/>	
Über den Beauftragten für den Datenschutz der EKD	17
Überblick zur Datenschutzaufsicht in der EKD	18
Struktur und Arbeit des BfD EKD	18
Die Behörde	20
Aufgaben und Tätigkeiten	23
Öffentlichkeitsarbeit	30
Vernetzung	31
<hr/>	
Über die Themen bei Aufsicht und Beratung	35
Datenverarbeitung und Auskunftsrecht	36
Freiwilligkeit einer Einwilligungserklärung	36
Bearbeitung eines Auskunftsanspruchs	37
Kommunikation mit Betroffenen von sexualisierter Gewalt	37
Ungewollte Berechtigungsänderung	37
Scannen von Dokumenten	37
Erstellung einer Datenschutz-Folgenabschätzung mithilfe des KDM	38
Fragen im gemeindlichen Alltag	38
Private E-Mail-Adressen in der Seelsorge	38
Streaming von Gottesdiensten	39
Geburtstagsgratulation im Gemeindebrief	39
Online-Wahlen in Kirchengemeinden	40
Besonderheiten im diakonischen Bereich	40
Versendung von Entlassberichten trotz fehlender Einwilligung	40
Exkurs: Schwerpunktprüfung in evangelischen Krankenhäusern	41
Zweckentfremdung von Patientendaten	41
Zusendung von Informationsmaterial	42
Schnittstelle Schulsozialarbeit	42
Das Gesundheitsdatennutzungsgesetz zwischen Digitalisierung und Datenschutz	43

Aufbewahrung und Löschung	44
Vernichtung von Corona-Testnachweisen auf Wertstoffhof	44
Sicherheitsstandards bei der Vernichtung von (Papier-)Akten	44
Geltendmachung eines Löschanpruchs für Taufbucheinträge	45
Anfertigung eines Löschkonzepts	45
Verarbeitung von Beschäftigendaten	46
Umgang mit erweiterten Führungszeugnissen	46
Zugriff auf das persönliche Laufwerk	46
Betrieblicher Aushang mit sensiblen Informationen	47
Nachweis der Kinderanzahl durch Vorlage von Geburtsurkunden	47
Einsatz von Videokameras	48
Videoüberwachung in Kirchen	48
Videoüberwachung im Pflegeheim	48
Einsatz von Kamera-Attrappen	49
Digitale Kommunikation	49
Phishing-E-Mails	49
Überprüfung von Websites	50
Datenschutzerklärungen häufig falsch	50
Datensicherheit und Verschlüsselung	51
Verschlüsselung mobiler Datenträger	51
Diebstahl mobiler Endgeräte	51
Beschlagnahme von IT-Geräten	51
Privater Erwerb einer gebrauchten Festplatte	52
Multi-Faktor-Authentifizierung als Stand der Technik?!	52
Auslagerung der IT-Infrastruktur in die Azure-Cloud	52
Durchführung von Backups mithilfe von Cloud-Diensten	53
Nutzung von Social Media und Software	54
Veröffentlichungen auf Social Media	54
Einbindung von Social Media - Angeboten	54
Social Media auf privaten Endgeräten am Arbeitsplatz	55
Gleiche Inhalte auf mehreren Social Media - Plattformen	55
Einsatz von Programmen zur Fremdsprachenübersetzung	55
Nutzung von Kita-Apps	56
Datenpanne in Kita-App	56
Örtlich Beauftragte für den Datenschutz	57
Gemeinsame Bestellung von örtlich Beauftragten für den Datenschutz	57
Datenschutzniveau in kleinen kirchlichen Einrichtungen	57
Haftung von örtlich Beauftragten für den Datenschutz	58
<hr/>	
Ausblick	59

Vorwort

Weiterentwicklung des kirchlichen Datenschutzes in herausfordernden Zeiten



In diesen herausfordernden Zeiten krisenhafter Zuspitzungen in Staat, Gesellschaft und Kirche gerät auch der (kirchliche) Datenschutz immer mehr unter Druck!

Da war es zur Wahrung eines kräftigen Grundrechtsschutzes in Staat und Kirche

wichtig, dass in der evangelischen Kirche im Berichtszeitraum ein breit angelegter Prozess zur Evaluierung des EKD-Datenschutzgesetzes stattgefunden hat. Im November 2024 hat die EKD-Synode das evaluierte Gesetz einstimmig beschlossen und verabschiedet. Es ist zum 1. Mai 2025 in Kraft getreten. Der Gesetzgeber verfolgte dabei zwei Zielrichtungen: Einerseits wurde das EKD-Datenschutzgesetz näher an die Datenschutzgrundverordnung (DSGVO) herangeführt, um den nach Art. 91 DSGVO erforderlichen Einklang zwischen den beiden Gesetzen noch besser darzustellen. Andererseits wurden kirchliche Spezifika klarer herausgestellt und geregelt.

Auch grundsätzlich wurde im Rahmen des Gesetzgebungsverfahrens diskutiert, ob an den beiden Rechten aus Art. 91 DSGVO für Religionsgemeinschaften festgehalten werden sollte. Dabei ergab die Diskussion, dass man in der evangelischen Kirche auch weiterhin eigenes Datenschutzrecht (Art. 91 Abs. 1 DSGVO) setzen und dessen Durchsetzung mit eigenen Aufsichtsbehörden (Art. 91 Abs. 2 DSGVO) sicherstellen möchte.

Diesem gesetzgeberischen Auftrag sind wir als unabhängige Datenschutzaufsichtsbehörde in der EKD für Kirche und Diakonie in besonderer Weise verpflichtet. Seit Anfang des Jahres 2025 nehmen wir unsere Aufgaben nun ekd-weit umfassend wahr, nachdem die noch verbliebenen zwei Landeskirchen und diakonischen Landesverbände, die die Datenschutzaufsicht bisher eigenständig wahrgenommen hatten, diese auf die EKD übertragen haben. Vor dem Hintergrund unseres kirchlichen Auftrags gilt für uns auch weiterhin, bei all

unserem Tätigwerden den Grundrechtsschutz für betroffene Personen und die Interessen von kirchlichen und diakonischen verantwortlichen Stellen in einen grundrechtskonformen Ausgleich zu bringen.

Im Berichtszeitraum haben wir neben regelmäßig wiederkehrenden rechtlichen und technischen Datenschutzthemen auch kirchlich-spezifische und innovativ-technische Datenschutzthemen bearbeitet. Dabei sind zwei Themenbereiche in besonderer Weise hervorzuheben:

- Kirchlich-spezifisch ist der Umgang mit personenbezogenen Daten beim Thema sexualisierte Gewalt
- Innovativ-technisch ist das Thema Künstliche Intelligenz und insbesondere der datenschutzkonforme Umgang mit Large Language Modellen

Beiden Themen werden wir uns auch zukünftig umfassend widmen.

Dieser 5. Tätigkeitsbericht versteht sich als Weiterentwicklung der bisher von mir vorgelegten Tätigkeitsberichte für die Berichtszeiträume 2015/2016, 2017/2018, 2019/2020 und 2021/2022. Dabei wurden das Kapitel I „Über die Entwicklungen im Datenschutz“ und das Kapitel II „Über den Beauftragten für den Datenschutz der EKD“ weiter konzentriert. Das Kapitel III „Über die Themen bei Aufsicht und Beratung“ enthält wieder viele unterschiedliche konkrete Beispiele aus dem rechtlichen und technischen Datenschutz und versucht nochmal praxisbezogener und technischer zu sein als im letzten Tätigkeitsbericht. Alle konkret zitierten Paragraphen aus dem EKD-Datenschutzgesetz beziehen sich auf die im Berichtszeitraum geltende Fassung, soweit nicht ausdrücklich etwas anderes gekennzeichnet ist.

Und so ist auch zukünftig die gesetzliche Aufforderung im EKD-Datenschutzgesetz, jede einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird, ein besonderer Auftrag an alle kirchlichen und diakonischen Stellen und die kirchliche Datenschutzaufsicht!

Allen Mitarbeitenden, die an der Erstellung dieses Tätigkeitsberichts beteiligt waren, gilt mein herzlicher Dank!

Den Leserinnen und Lesern wünsche ich bei der Lektüre dieses Tätigkeitsberichts nunmehr viele interessante und hilfreiche Erkenntnisse im Bereich des (kirchlichen) Datenschutzes!

Hannover, im Juni 2025

A handwritten signature in blue ink that reads "Michael Jacob". The signature is written in a cursive, flowing style.

Michael Jacob
Der Beauftragte für den Datenschutz
der Evangelischen Kirche in Deutschland



Über die Entwicklungen im Datenschutz

Der Datenschutz in seiner heutigen Form hat eine fünfzigjährige Entwicklung hinter sich. Doch seine Ursprünge im kirchlichen Bereich sind mit dem Beicht- und Seelsorgegeheimnis viel älter. Vor diesem Hintergrund wird in diesem Kapitel über die aktuellen Entwicklungen des Datenschutzes im kirchlichen und staatlichen Bereich informiert. Beim Blick nach vorne stehen heute sowohl der staatliche als auch der kirchliche Datenschutz vor großen Herausforderungen.

In der evangelischen Kirche

Am 24. Mai 2018 trat das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz, – DSG-EKD) in einer neuen Fassung in Kraft. Die Neufassung stand in engem Zusammenhang mit der europäischen Datenschutzgrundverordnung (DSGVO), die seit dem 25. Mai 2018 in allen Mitgliedsstaaten der Europäischen Union gilt. Die beiden großen Kirchen in Deutschland hatten sich zuvor entschieden dafür eingesetzt, dass das kirchliche Datenschutzrecht in Deutschland – welches in Europa in dieser Form singulär ist – weiterhin Bestand hat und die Kirchen eigene unabhängige Aufsichtsbehörden errichten können. Diese Bemühungen waren erfolgreich und fanden Ausdruck in Art. 91 DSGVO.

In § 54 Abs. 4 DSG-EKD war eine Überprüfung des Gesetzes innerhalb von fünf Jahren vorgesehen. Diese Überprüfung hat im Berichtszeitraum stattgefunden. Dieser Evaluationsprozess wurde durch das Kirchenamt der EKD gesteuert. Das zuständige Referat hat im Jahr 2022 eine Arbeitsgruppe eingerichtet, die das EKD-Datenschutzgesetz überprüft und dann konkrete Gesetzesänderungen vorgeschlagen hat. Parallel wurde zur weiteren Abstimmung eine Resonanzgruppe gebildet, die über die Ergebnisse der Arbeitsgruppe beraten hat. In beiden Arbeitsgruppen waren Vertreterinnen und Vertreter der Landeskirchen und der evangelischen Datenschutzaufsichtsbehörden vertreten. In der Resonanzgruppe wirkten der Beauftragte für den Datenschutz der EKD Michael Jacob und die stellvertretende Behördenleitung Sandra Coors mit. Zwischen März und Juni 2024 wurde in den Landeskirchen und Diakonischen Landesverbänden ein breit angelegtes Stellungnahmeverfahren durchgeführt. Die Synode der EKD hat dann im November 2024 das evaluierte EKD-Datenschutzgesetz verabschiedet, das zum 1. Mai 2025 in Kraft getreten ist.

Die Evaluierung war geprägt von einer „Doppelbewegung“. Zum einen galt es in einigen Regelungen, in denen es erforderlich war, dichter an die Regelungen der DSGVO heranzurücken um den Einklagbereich zu plausibilisieren, zum anderen wurden kirchliche

Spezifika – auch durch neue Regelungen – gestärkt. So wurde beispielsweise die Frist aus § 16 Abs. 3 DSG-EKD insgesamt verkürzt. Auskunftersuchen betroffener Personen müssen daher künftig unverzüglich, in jedem Fall aber innerhalb von drei Monaten nach Eingang des Antrags beantwortet werden. Außerdem müssen die Informationspflichten gemäß § 17 DSG-EKD nunmehr aktiver als bisher und nicht erst auf Verlangen erfüllt werden. Dafür muss der betroffenen Person zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten in geeigneter und angemessener Weise Zugang zu den in § 17 DSG-EKD genannten Informationen gewährt werden. Praxistaugliche Lösungen können laut der nichtamtlichen Begründung zum EKD-Datenschutzgesetz dadurch gefunden werden, dass es zentrale Datenschutzinformationen auf der Website gibt. Außerdem wurde das Recht auf Kopie normiert. Auch das Widerspruchsrecht wurde überarbeitet und ein neuer Paragraph zu automatisierten Entscheidungen einschließlich Profiling aufgenommen. Mit den neuen §§ 30a und 50b DSG-EKD werden kirchliche Spezifika geregelt. Mit § 30a DSG-EKD wird ein neuer Paragraph zu zentralen Verfahren eingefügt. Es wird die Datenverarbeitung in Aufsichtskonstellationen geregelt und die Einführung von zentral beschaffter Software vereinfacht. Mit § 50b DSG-EKD wurde ein Paragraph zur Mitgliederkommunikation aufgenommen. Die Verarbeitung von Kontaktdaten der Kirchenmitglieder ist notwendig, um eine effektive Kommunikation zwischen der Kirche und ihren Mitgliedern zu gewährleisten. Dies ist eine originäre kirchliche Aufgabe. Die sogenannte Unterwerfung von nicht-kirchlichen Auftragsverarbeitern unter die kirchliche Aufsicht in § 30 Abs. 5 DSG-EKD wurde gestrichen.

Gemäß Art. 91 Abs. 2 DSGVO können Kirchen, die umfassende Datenschutzregeln anwenden, eine unabhängige Aufsichtsbehörde spezifischer Art errichten. Im Bereich der evangelischen Kirche gab es im Berichtszeitraum neben dem Beauftragten für den Datenschutz der EKD (BfD EKD) und der von ihm geleiteten Aufsichtsbehörde eine weitere Aufsichtsbehörde für zwei ostdeutsche Landeskirchen und zwei diakonische Landesverbände mit ihren Mitgliedseinrichtungen und bis zum 30. September 2023 eine weitere Aufsichtsbehörde für die Nord-

kirche. Seit dem 1. Januar 2025 ist der BfD EKD die einheitliche Datenschutzaufsichtsbehörde im gesamten Bereich der evangelischen Kirche und ihrer Diakonie. Der BfD EKD übte im Berichtszeitraum die Datenschutzaufsicht in der evangelischen Kirche über weite Bereiche von Kirche und Diakonie aus. Über die Aufgabenerledigung des BfD EKD wird in Kapitel II und III dieses Tätigkeitsberichts ausführlich berichtet.

Im Berichtszeitraum ist der BfD EKD Beklagter in insgesamt vier beendeten Verfahren vor dem Kirchengericht der EKD gewesen. Davon wurden drei Klagen von der klagenden Partei im laufenden Verfahren zurückgenommen. Eine Klage wurde als unzulässig abgewiesen.

Im Ganzen hat das Thema Datenschutz in den letzten Jahren auch in der evangelischen Kirche weiter an Bedeutung gewonnen. Im Mittelpunkt steht dabei gerade auch beim kirchlichen Datenschutz immer der Schutz des einzelnen Menschen mit seinen personenbezogenen Daten, um so das aus dem Grundgesetz abgeleitete Grundrecht auf informationelle Selbstbestimmung für jeden Einzelnen zu garantieren. Für die Kirchen hat der Schutz von personenbezogenen Daten vor dem Hintergrund des kirchlichen Auftrags und des christlichen Menschenbildes auch im Hinblick auf das Beicht- und Seelsorgegeheimnis von jeher eine besondere Bedeutung.

In der römisch-katholischen Kirche

Wie die evangelische Kirche fällt auch die römisch-katholische Kirche unter die Vorgaben in Art. 91 Abs. 1 DSGVO und hat mit dem Gesetz über den Kirchlichen Datenschutz (KDG), das am 24. Mai 2018 in Kraft getreten ist, ein eigenes Datenschutzgesetz. Gemäß § 58 Abs. 2 KDG soll das Gesetz über den kirchlichen Datenschutz (KDG) innerhalb der ersten Jahre seines Bestehens überprüft werden. Der Evaluationsprozess dauert an und wird demnächst abgeschlossen.

Mit Blick auf Art. 91 Abs. 2 DSGVO sind in der römisch-katholischen Kirche die Diözesanbischöfe aufgrund

ihrer Gesetzgebungsgewalt für ihren Zuständigkeitsbereich befugt Diözesandatenschutzbeauftragte zu ernennen. Die Datenschutzaufsicht im Bereich der römisch-katholischen Kirche gliedert sich deutschlandweit in fünf Regionen. In jeder Region wird die Datenschutzaufsicht durch eine Diözesandatenschutzbeauftragte oder einen Diözesandatenschutzbeauftragten wahrgenommen. Die Diözesandatenschutzbeauftragten bilden die Konferenz der Datenschutzbeauftragten im Bereich der römisch-katholischen Kirche in Deutschland. Die Konferenz trifft sich regelmäßig zur Erarbeitung gemeinsamer Entschlüsse und Empfehlungen und zum Austausch über Datenschutzfragen. Der Vorsitz der Konferenz wechselt jährlich.

In der Bundesrepublik Deutschland

In der Bundesrepublik Deutschland wurde der Datenschutz im Berichtszeitraum durch das Inkrafttreten neuer Gesetze sowie durch neue Rechtsprechung weiterentwickelt.

Datenschutzrecht des Bundes und der Länder

Das Datenschutzrecht wurde im Berichtszeitraum insbesondere durch die beabsichtigte Novellierung des Bundesdatenschutzgesetzes (BDSG) weiterentwickelt.

Novellierung des Bundesdatenschutzgesetzes

Die Bundesregierung hat im Februar 2024 einen Entwurf für eine Novellierung des Bundesdatenschutzgesetzes (BDSG) vorgelegt. Der Gesetzentwurf wurde in der Legislaturperiode nicht verabschiedet. Er sah folgende neue Regelungen vor:

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wird im BDSG institutionalisiert. Die DSK soll die Datenschutzgrundrechte schützen sowie eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts ermöglichen und gemeinsam für seine Fortentwicklung eintreten. Unternehmen sowie Einrichtungen, die Daten für wissenschaftliche, historische oder statistische Zwecke verarbeiten, können bei länderübergreifenden Vorhaben, wenn eine gemeinsame datenschutzrechtliche Verantwort-

tung bei mehreren Aufsichtsbehörden bestehen würde, nur eine Aufsichtsbehörde als Ansprechpartner haben.

Darüber hinaus wurde im Gesetzentwurf klar gestellt, dass sich die Aufsichtsbehörden des Bundes und der Länder im Rahmen der europäischen Zusammenarbeit frühzeitig innerstaatlich abstimmen müssen. Damit wird auch in EU-Angelegenheiten die Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder gestärkt.

Zudem wurden die rechtlichen Grundlagen für das Scoring neu geregelt. Hintergrund ist eine Entscheidung des Europäischen Gerichtshofs (EuGH) aus Dezember 2023. Danach folgt aus Art. 22 DSGVO das Verbot, Personen einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung zu unterwerfen, die ihnen gegenüber rechtliche Wirkung entfaltet. Nach dieser Rechtsprechung kann bereits die Bildung eines Score-Wertes durch eine Auskunft eine solche automatisierte Entscheidung sein, wenn von diesem Score-Wert die Entscheidung eines Dritten maßgeblich abhängt. Von der in der DSGVO vorgesehenen Möglichkeit für nationale Ausnahmen von diesem Verbot wird Gebrauch gemacht.

Gesetz zur Umsetzung der NIS-2-RL

Die Bundesregierung hat im Juli 2024 einen Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie vorgelegt. Der Gesetzgebungsprozess zu diesem Gesetz war damit eingeleitet. Der Gesetzentwurf wurde in der Legislaturperiode nicht verabschiedet. Das Gesetz sollte die rechtlichen IT-Sicherheitsanforderungen, die sich bisher aus dem BSI-Grundschutz ergeben, auf eine Vielzahl weiterer Unternehmen und Sektoren ausdehnen.

Datenschutzaufsicht des Bundes und der Länder

Seit September 2024 ist Prof. Dr. Louisa Specht-Riemenschneider Bundesbeauftragte für den Datenschutz und die Informationssicherheit. Sie ist die Nachfolgerin von Prof. Ulrich Kelber.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist eine unabhängige eigenständige oberste Bundesbehörde für den

Datenschutz und die Informationsfreiheit. In dieser Funktion überwacht sie im föderalen System Deutschlands gemäß § 9 BDSG die Einhaltung des Datenschutzrechts in öffentlichen Stellen des Bundes sowie in Unternehmen, die Telekommunikations- und Postdienstleistungen erbringen.

Die Aufsichtsbehörden der Länder überwachen nach dem jeweiligen Landesrecht bei den öffentlichen Stellen des Landes sowie den nichtöffentlichen Stellen die Anwendung der Vorschriften über den Datenschutz und beraten die Stellen in Fragen des Datenschutzes. Im Rahmen dieser Aufgabenerfüllung sind sie unabhängig, weisungsfrei und nur dem Gesetz unterworfen. Die Rechtsstellung und die Befugnisse der Landesdatenschutzbeauftragten sind in den jeweiligen Landesdatenschutzgesetzen geregelt.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beschäftigt sich mit aktuellen Fragen des Datenschutzes in Deutschland und nimmt zu ihnen Stellung. Die DSK besteht aus der Bundesdatenschutzbeauftragten, den Landesdatenschutzbeauftragten der 16 Bundesländer und dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht. Die DSK ist in verschiedene Arbeitskreise untergliedert. Sie veröffentlicht auf ihrer Website (<https://www.datenschutzkonferenz-online.de/>) regelmäßig Entschlüsse zu wichtigen Entwicklungen und Themen im Bereich Datenschutz.

Datenschutzrechtsprechung staatlicher Gerichte

Im Berichtszeitraum sind einige Urteile staatlicher Gerichte zum Datenschutz ergangen. Von besonderer Bedeutung sind mehrere Urteile des Bundesarbeitsgerichts (BAG). Ein Urteil beschäftigt sich mit dem Sonderkündigungsschutz für Datenschutzbeauftragte. Ein anderes Urteil des BAG stellt fest, dass die Pflichten eines Betriebsratsvorsitzenden mit den Pflichten eines Datenschutzbeauftragten nicht vereinbar sind. Ein drittes Urteil des BAG befasst sich auch mit dem kirchlichen Datenschutzrecht.

Sonderkündigungsschutz für Datenschutzbeauftragte

Das BAG hat mit Urteil vom 6. Juni 2023 (Az.: 9 AZR 621/19) eine wichtige Entscheidung zum Sonderkündigungsschutz für Datenschutzbeauftragte getro-

fen. Danach hat landesspezifisches Datenschutzrecht Vorrang vor dem BDSG. Soweit für öffentliche Stellen der Länder besondere landesdatenschutzrechtliche Bestimmungen gelten, sind diese, auch wenn sie Bundesrecht ausführen, von den Bestimmungen des BDSG ausgenommen. Das BDSG hat damit den Charakter eines Auffanggesetzes. § 38 Abs. 1 Satz 1 und Abs. 1 in Verbindung mit § 6 Abs. 4 Satz 1 BDSG stehen im Einklang mit dem Unionsrecht und sind verfassungsmäßig bestätigt. Die Bestimmungen beeinträchtigen die Verwirklichung der Ziele der DSGVO nicht. Nach dem Urteil wird die Rechtsstellung eines auf Grund des BDSG (alte Fassung) bestellten Datenschutzbeauftragten nicht automatisch durch das Inkrafttreten der DSGVO beendet. Aufgrund der Verweisung in § 6 Abs. 4 Satz 1 BDSG muss für die Abberufung ein wichtiger Grund nach § 626 Abs. 1 BGB vorliegen, der es dem Verantwortlichen auf Grund von Tatsachen und unter Berücksichtigung der Gegebenheiten des Einzelfalls sowie unter Abwägung der Interessen beider Vertragspartner unzumutbar macht, die betreffende Person als betrieblichen Datenschutzbeauftragten auch nur bis zum Ablauf der ordentlichen Kündigungsfrist weiterhin einzusetzen. Eine Abberufung kann durch Gründe gerechtfertigt sein, die mit der Funktion und der Tätigkeit des Datenschutzbeauftragten zusammenhängen. Dies kann z. B. der Fall sein, wenn der zum betrieblichen Datenschutzbeauftragten bestellte Arbeitnehmer die für die Aufgabenerfüllung erforderliche Fachkunde oder Zuverlässigkeit nicht (mehr) besitzt. Die Zuverlässigkeit eines betrieblichen Datenschutzbeauftragten kann auch in Frage stehen, wenn Interessenkonflikte drohen. Der nach § 6 Abs. 4 Satz 1 BDSG normierte besondere Schutz des betrieblichen Datenschutzbeauftragten vor einer Abberufung ist mit dem Unionsrecht vereinbar.

Datenschutzbeauftragter und Betriebsratsvorsitzender

Mit Urteil vom 6. Juni 2023 (Az.: 9 AZR 383/19) hat das BAG eine weitere wichtige Entscheidung getroffen, die die Datenschutzbeauftragten betreffen. Es stellte fest, dass die Pflichten eines Datenschutzbeauftragten mit denen eines Betriebsratsvorsitzenden nicht zu vereinbaren sind. Der bei gleichzeitiger Wahrnehmung beider Funktionen bestehende Interessenkonflikt rechtfertigt es, die Bestellung des Betriebsratsvorsitzenden zum Datenschutzbeauftragten zu widerrufen.

Einsicht ins Protokoll eines kirchlichen Leitungsorgans

Bei dem Urteil des BAG vom 17. Oktober 2024 (Az.: 8 AZR 42/24) klagte eine Organistin und Chorleiterin, die ehemals bei der beklagten evangelischen Kirchengemeinde beschäftigt war. Sie begehrte Einsicht in das Protokoll einer nichtöffentlichen Sitzung des Kirchengemeinderats. In dieser Sitzung wurden arbeitsrechtliche Maßnahmen gegen sie beschlossen, deren Inhalt ihr nicht mitgeteilt wurde. Nach mehreren erfolglosen Versuchen, das Protokoll einzusehen – darunter zwei Klagen vor dem Verwaltungsgericht der Landeskirche –, klagte sie erneut unter Berufung auf die DSGVO und die kirchliche Anstellungsordnung (KAO). Das Arbeitsgericht Stuttgart (Az.: 15 Ca 3910/22) und das Landesarbeitsgericht Baden-Württemberg (Az.: 7 Sa 35/23) wiesen die Klage als unbegründet ab. Die Klägerin legte Revision beim BAG ein. Das BAG hob die Urteile der Vorinstanzen teilweise auf und gab der Klägerin Recht. Es entschied, dass die Beklagte verpflichtet ist, der Klägerin eine Kopie des Protokolls auszuhändigen. Die Beklagte argumentierte, dass ausschließlich die kirchliche Verwaltungsgerichtsbarkeit zuständig sei. Das BAG stellte klar, dass der Anspruch auf Herausgabe der Protokollkopie eine bürgerliche Rechtsstreitigkeit darstellt, die in den Anwendungsbereich staatlicher Gerichte fällt. Art. 140 Grundgesetz in Verbindung mit Art. 137 Abs. 3 Weimarer Reichsverfassung schließt staatliche Gerichte nicht generell aus, wenn es um individuelle arbeitsrechtliche Ansprüche geht. § 3 Abs. 5 KAO gewährt Beschäftigten das Recht auf Einsicht in ihre Personalakte und Kopien daraus. Das BAG folgte dem weiten Personalaktenbegriff: Dokumente, die dienstliche Verhältnisse betreffen, gehören unabhängig von ihrer äußeren Zuordnung zur Personalakte. Das Protokoll behandelte ausschließlich arbeitsrechtliche Maßnahmen gegen die Klägerin und war daher Teil ihrer materiellen Personalakte. Die Beklagte berief sich auf die Verschwiegenheitspflicht aus der Kirchengemeindeordnung, da es sich um eine nichtöffentliche Sitzung handelte. Das BAG stellte fest, dass die Verschwiegenheitspflicht vorrangig dem Schutz der betroffenen Person dient, nicht aber, um dieser selbst Informationen vorzuenthalten. Ein freier Meinungsbildungsprozess innerhalb des Kirchengemeinderats sei auch ohne vollständige Geheimhaltung gegenüber der Klägerin gewährleistet. Die Urteile des Verwal-

tungsgerichts der Landeskirche von 2012 und 2018 entfalten keine Rechtskraftwirkung für den vorliegenden Fall, da sie nicht die Herausgabe einer Kopie, sondern nur allgemeine Auskunftsansprüche betrafen. Zwischenzeitlich hat die Beklagte gegen das Urteil des BAG Verfassungsbeschwerde beim Bundesverfassungsgericht eingelegt.

In der Europäischen Union

In der Europäischen Union waren im Berichtszeitraum neben digitalen Rechtsetzungsakten insbesondere die Wahrung der Betroffenenrechte und die Bedeutung von Transparenz wichtige Themen.

Europäisches Datenschutzrecht

In der Europäischen Union wurden im Berichtszeitraum zwei bedeutende Regelungen verabschiedet, die die Anwendung des Datenschutzrechts betreffen: Die KI-Verordnung (Artificial Intelligence Act – AI Act) und der Europäische Gesundheitsdatenraum (The European Health Data Space – EHDS).

Im August 2024 trat die europäische Verordnung über künstliche Intelligenz (KI-Verordnung) in Kraft. Sie regelt die verantwortungsvolle Entwicklung und Nutzung von KI in der Europäischen Union und setzt klare Standards, die von minimalen Transparenzpflichten bis hin zu strengen Anforderungen für hochriskante Anwendungen reichen. Ziel ist es Innovationen zu fördern, Risiken zu minimieren und die Grundrechte der Bürgerinnen und Bürger zu schützen. Dabei stellt die Verordnung klar, dass KI-Systeme im Einklang mit den geltenden Vorschriften zum Schutz der Privatsphäre und zum Datenschutz entwickelt und verwendet werden müssen.

Der EHDS, auf den sich die Europäische Union im März 2024 einigte, soll den datenschutzkonformen Zugang zu Gesundheitsdaten für Patientinnen und Patienten und Fachkräfte erleichtern. Nach Auffassung der Kommission der Europäischen Union sollen der EHDS und die DSGVO nebeneinanderstehen. Dabei soll der EHDS ausweislich seiner Erwägungsgründe auf der DSGVO aufbauen und einen hohen Sicherheitsstandard bei der Verarbeitung im europäischen Gesundheitsdatenraum sicherstellen. Zusätzlich wird

eine einheitliche Sekundärnutzung der Daten für Forschung und Innovation ermöglicht, wobei Bürger ein Widerspruchsrecht (Opt-Out) haben. Dies schafft die Grundlage für eine effizientere und innovativere Gesundheitsversorgung als bisher in der Europäischen Union.

Datenschutzaufsicht der Europäischen Union

Der Europäische Datenschutzbeauftragte (EDSB) ist die zuständige Datenschutzkontrollbehörde für alle Organe und Einrichtungen der Europäischen Union. Den EDSB gibt es seit dem Jahr 2004. Er hat seinen Sitz in Brüssel.

Mit Inkrafttreten der DSGVO wurde der Europäische Datenschutzausschuss (EDSA) mit Sitz in Brüssel geschaffen. Der EDSA setzt sich aus Vertretern der nationalen Datenschutzbehörden und dem EDSB zusammen. Für Angelegenheiten in Verbindung mit der DSGVO sind auch die Aufsichtsbehörden der Staaten des Europäischen Wirtschaftsraums sowie die der Europäischen Freihandelsassoziation (EWR-/EFTA-Staaten) Mitglieder. Sie haben aber nur eingeschränkte Rechte und z. B. kein Stimmrecht. Aufgabe des EDSA ist es, die einheitliche Anwendung des Datenschutzrechts in den Mitgliedsstaaten der Europäischen Union sicherzustellen und den Austausch und die Zusammenarbeit zwischen den verschiedenen Aufsichtsbehörden zu fördern. Er verfasst Leitlinien zu Fragen der Auslegung der DSGVO und führt öffentliche Konsultationen durch, um die Ansichten und Anliegen aller Interessenträger und Bürger zu hören. Im Rahmen der Konsultationen können in einem festgelegten Zeitraum Interessierte ihre Meinung zu den Richtlinien des EDSA äußern. Diese werden anschließend gegebenenfalls durch diesen veröffentlicht. In Kapitel 7 der DSGVO finden sich in den Artikeln 60 bis 76 die Regelungen zur Zusammenarbeit und Kohärenz der Aufsichtsbehörden der Mitgliedsstaaten und des Europäischen Datenschutzbeauftragten (EDSB).

Datenschutzrechtsprechung des Europäischen Gerichtshofs

Die Rechtsprechung des EuGH hat in den Jahren 2023 und 2024 die Auslegung der DSGVO entscheidend geprägt. Die Urteile betonen die Bedeutung von Transparenz und der Wahrung der Betroffenenrechte.

Schadensersatzansprüche

Der EuGH hat im Mai 2023 (Az.: C-300/21) entschieden, dass für Schadensersatzansprüche nach Art. 82 DSGVO ein individueller Schaden nachgewiesen werden muss. Ein bloßer Verstoß gegen die DSGVO reicht nicht aus. Materielle oder immaterielle Schäden müssen konkret vorliegen, wobei es keine Erheblichkeitsschwelle für immaterielle Schäden gibt. Diese Entscheidung erleichtert es Betroffenen, Ansprüche geltend zu machen und könnte eine Zunahme von Klagen bewirken. Nationale Gerichte haben nun zu klären, wie solche Schäden definiert und bewiesen werden können.

Empfänger benennen

Im selben Urteil (Az.: C-300/21) entschied der EuGH, dass eine Verpflichtung zur Benennung von konkreten Datenempfängern besteht. Nur durch umfassende Transparenz hinsichtlich der Empfänger verarbeiteter Daten können Betroffene ihre Rechte, z. B. wie das Recht auf Berichtigung oder Löschung, effektiv geltend machen. Verantwortliche Stellen müssen sicherstellen, dass alle relevanten Informationen bereitgestellt werden, um rechtliche Konsequenzen zu vermeiden.

Recht auf Kopie

Der EuGH hat im Oktober 2023 (Az.: C-307/22) klargestellt, dass betroffene Personen Anspruch auf eine originalgetreue und verständliche Kopie der verarbeiteten personenbezogenen Daten haben. Dazu können Dokumente, Datenbankauszüge oder ähnliche Informationen gehören, sofern diese notwendig sind, um die Rechtmäßigkeit der Verarbeitung zu überprüfen. Verantwortliche Stellen müssen dabei nicht nur die Daten selbst, sondern auch deren Verarbeitungskontext in verständlicher Weise darstellen. Gleichzeitig sind Ausnahmen zu beachten, insbesondere wenn Rechte Dritter betroffen sind.

Kopie der Patientenakte

Ebenfalls im Oktober 2023 entschied der EuGH (Az.: C-307/22), dass die erste vollständige Kopie einer Patientenakte – im Einklang mit dem datenschutzrechtlichen Auskunftsanspruch – unentgeltlich zur Verfügung gestellt werden muss. Diese Entscheidung löst die bisherige deutsche Sonderregelung

nach dem Patientenrechtegesetz (§ 630 g BGB) ab, wonach den Behandelnden die entstandenen Kosten für die Kopie der Patientenakte zu erstatten waren. Der Anspruch gilt unabhängig vom Zweck des Auskunftsersuchens und umfasst eine vollständige und verständliche Bereitstellung der relevanten Daten. Für weitere zusätzliche Kopien dürfen jedoch weiterhin entsprechende Kosten durch die verantwortlichen Stellen berechnet werden. Diese Entscheidung stellt damit sicher, dass Patientinnen und Patienten ihre grundlegenden Betroffenenrechte aus dem Datenschutzrecht effektiv wahrnehmen können, ohne dass sie durch zusätzliche Kosten belastet werden.

Personenbezug der FIN

Im November 2023 entschied der EuGH (Az.: C-319/22), dass die Fahrzeugidentifikationsnummer (FIN) als solche grundsätzlich kein personenbezogenes Datum darstellt, da sie primär der Identifikation von Fahrzeugen dient. Gleichzeitig wurde aber klargestellt, dass die FIN unter bestimmten Umständen zu einem personenbezogenen Datum werden kann. Dies ist der Fall, wenn ein Verarbeiter selbst über die Mittel verfügt, die es ihm erlauben, die FIN einer bestimmten Person zuzuordnen. Entscheidend ist dabei die Perspektive des jeweiligen Verarbeiters und nicht die theoretische Möglichkeit, dass ein Dritter einen Personenbezug herstellen könnte. Der EuGH betonte, dass die konkrete Beurteilung der Identifizierbarkeit auf vernünftig einsetzbaren Mitteln basieren muss. Damit bestätigt der EuGH seine bisherige Tendenz hinsichtlich des relativen Personenbezugs. Insoweit genügt für die Personenbeziehbarkeit – anders als nach dem absoluten Personenbezug – nicht das Zusatzwissen Dritter, das eine Identifikation theoretisch ermöglichen würde, sondern nur die tatsächliche Möglichkeit. Darüber hinaus stellte der EuGH fest, dass Fahrzeughersteller unabhängigen Wirtschaftsakteuren die FIN bereitstellen müssen, da dies eine rechtliche Verpflichtung nach der EU-Fahrzeuggenehmigungsverordnung darstellt. Dies gilt unabhängig davon, ob die FIN als personenbezogenes Datum anzusehen ist. Die Entscheidung hat erhebliche Auswirkungen auf die Praxis und könnte auf andere technische Kennnummern übertragen werden, deren Personenbezug stets im Einzelfall zu prüfen ist.

Datenschutzaufsichtsbehörden und Abhilfemaßnahmen

Des Weiteren hat der EuGH im November 2023 (Az.: C-333/22) entschieden, dass Datenschutzaufsichtsbehörden nicht verpflichtet sind, Abhilfemaßnahmen zu ergreifen, wenn diese nicht erforderlich sind, um die festgestellte Unzulänglichkeit abzustellen und die Einhaltung der DSGVO sicherzustellen. Die Entscheidung beruht auf einem Vorabentscheidungsersuchen des Verwaltungsgerichts Wiesbaden. Im zugrundeliegenden Fall hatte eine betroffene Person beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit Beschwerde gegen eine Sparkasse eingereicht. Der EuGH stellte klar, dass die Datenschutzaufsichtsbehörden bei der Auswahl von Maßnahmen ein Ermessen haben, das durch die Vorgaben der DSGVO begrenzt wird. Dieses Ermessen ermöglicht es den Behörden, die Besonderheiten des Einzelfalls zu berücksichtigen. Ein Beispiel ist der Fall, in dem der Verantwortliche nach Kenntnis der Verletzung bereits ausreichende Maßnahmen ergriffen hat, um die Verletzung abzustellen und eine Wiederholung zu verhindern. Die Entscheidung unterstreicht, dass Datenschutzaufsichtsbehörden flexibel auf Verstöße reagieren können, um ein hohes und gleichmäßiges Schutzniveau für personenbezogene Daten sicherzustellen. Ähnlich entschied der EuGH mit Urteil vom 26. September 2024 (Az.: C-768/21), dass ein Anspruch auf Verhängung eines Bußgeldes nicht besteht, sondern Aufsichtsbehörden individuelle Abhilfemaßnahmen zu bestimmen haben, die geeignet, erforderlich und verhältnismäßig sind.

Verstoß gegen Informationspflichten

Im Juli 2024 entschied der EuGH (Az.: C-757/22), dass ein Verstoß gegen die Informationspflichten aus Art. 13 und 14 DSGVO eine rechtswidrige Datenverarbeitung darstellt. Datenschutzinformationen müssen rechtzeitig, korrekt und vollständig bereitgestellt werden. Werden diese Vorgaben nicht eingehalten, können sich verantwortliche Stellen nicht auf die Rechtmäßigkeit der Verarbeitung berufen. Wenn – wie im vorliegenden Fall – die Datenverarbeitung auf die Rechtsgrundlage der Einwilligung gestützt wird, dann gehöre bereits die transparente Information der Betroffenen zur Voraussetzung einer rechtmäßigen Verarbeitung. Dieses Urteil hebt

die Bedeutung von Transparenz und korrekter Information für die Rechtmäßigkeit der Datenverarbeitung hervor.



Über den Beauftragten für den Datenschutz der EKD

Zur Wahrnehmung der Datenschutzaufsicht existiert für die EKD sowie für alle Gliedkirchen, gliedkirchlichen Zusammenschlüsse und Diakonischen Werke seit Anfang 2014 die unabhängige und eigenständige Aufsichtsbehörde „Der Beauftragte für den Datenschutz der EKD (BfD EKD)“. Seit Errichtung dieser Behörde wird die Datenschutzaufsicht innerhalb der evangelischen Kirche einheitlicher als in der Vergangenheit und in größeren Strukturen wahrgenommen. Am Ende des Berichtszeitraums haben die zwei noch verbliebenen Gliedkirchen und die zwei diakonischen Landesverbände, die die Datenschutzaufsicht bis dahin eigenständig wahrgenommen hatten, diese auf den BfD EKD übertragen.

Überblick zur Datenschutzaufsicht in der EKD

Vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofs (EuGH) zur Unabhängigkeit von Datenschutzaufsichtsbehörden wurden mit der Novellierung des EKD-Datenschutzgesetzes bereits im Jahr 2013 die rechtlichen Grundlagen zur Neustrukturierung der Datenschutzaufsicht innerhalb der EKD geschaffen. Seitdem entspricht es einem kirchen- und diakoniepolitischen Ziel, diese Aufgabe einheitlicher als in der Vergangenheit und in größeren Strukturen wahrzunehmen.

Mit Wirkung zum 1. Januar 2022 hat der Rat der Evangelischen Kirche in Deutschland Herrn Michael Jacob als Beauftragten für den Datenschutz der EKD wiedergewählt und für weitere acht Jahre berufen. Er leitet bereits seit Januar 2014 die gleichnamige, unabhängige und eigenständige Behörde (BfD EKD) und übt seitdem für große Bereiche der evangelischen Kirche die Datenschutzaufsicht in Kirche und Diakonie aus. Die IT-Leitung liegt bei Herrn Michael Tolk, der zugleich der stellvertretende Beauftragte für den Datenschutz ist. Die stellvertretende Behördenleitung beim BfD EKD wird von Frau Sandra Coors wahrgenommen.

Im Berichtszeitraum ist die Datenschutzaufsicht der Nordkirche auf den BfD EKD übertragen worden. Zwei Gliedkirchen und zwei diakonische Landesverbände nahmen im Berichtszeitraum die Datenschutzaufsicht weiterhin eigenständig wahr. Am Ende des Berichtszeitraums haben auch diese Gliedkirchen und diakonischen Landesverbände die Datenschutzaufsicht auf den BfD EKD übertragen.

Die Hauptaufgaben des BfD EKD sind Aufsicht, Beratung und Weiterbildung in den Bereichen des rechtlichen und technischen Datenschutzes sowie im Bereich der Organisation des Datenschutzes. Zu den Kernaufgaben des BfD EKD gehört die Einhaltung des Datenschutzes zu kontrollieren und zu überwachen. Im Rahmen der Beratung ist der BfD EKD bestrebt, das Thema Datenschutz in Kirche und Diakonie, insbesondere durch Informationsmaterialien, noch stärker ins Bewusstsein zu rücken. Der BfD EKD bietet des Weiteren ein umfangreiches einheitliches Weiterbildungsprogramm für örtlich Beauftragte für den Datenschutz

an. Das Programm beinhaltet einerseits Schulungsmaßnahmen, andererseits aber auch Aspekte des Erfahrungsaustausches. Überdies hat der BfD EKD im Berichtszeitraum seine zweite Schwerpunktprüfung – dieses Mal im Bereich evangelischer Krankenhäuser – durchgeführt.

Struktur und Arbeit des BfD EKD

Der BfD EKD nimmt die im EKD-Datenschutzgesetz normierte Datenschutzaufsicht für die EKD, für das Evangelische Werk für Diakonie und Entwicklung und für gesamtkirchliche Werke und Einrichtungen sowie nach Übertragung seit dem 1. Januar 2025 für alle 20 Gliedkirchen, die gliedkirchlichen Zusammenschlüsse und für alle 15 diakonischen Landesverbände wahr. Seit dem 1. Januar 2014 haben sukzessive die nachfolgenden Gliedkirchen und gliedkirchlichen Zusammenschlüsse sowie diakonischen Landesverbände die Datenschutzaufsicht auf die EKD übertragen:

- Evangelische Landeskirche Anhalts (ab 1. Januar 2025)
- Evangelische Landeskirche in Baden
- Evangelisch-Lutherische Kirche in Bayern
- Evangelische Kirche Berlin-Brandenburg-schlesische Oberlausitz
- Evangelisch-lutherische Landeskirche in Braunschweig
- Bremische Evangelische Kirche
- Evangelisch-lutherische Landeskirche Hannovers
- Evangelische Kirche in Hessen und Nassau
- Evangelische Kirche von Kurhessen-Waldeck
- Lippische Landeskirche
- Evangelische Kirche in Mitteldeutschland
- Evangelisch-Lutherische Kirche in Norddeutschland (Nordkirche)
- Evangelisch-Lutherische Kirche in Oldenburg
- Evangelische Kirche der Pfalz
- Evangelisch-reformierte Kirche
- Evangelische Kirche im Rheinland
- Evangelisch-Lutherische Landeskirche Sachsens (ab 1. Januar 2025)
- Evangelisch-Lutherische Landeskirche Schaumburg-Lippe
- Evangelische Kirche von Westfalen
- Evangelische Landeskirche in Württemberg

- Union Evangelischer Kirchen in der EKD (UEK)
- Vereinigte Evangelisch-Lutherische Kirche Deutschlands (VELKD)
- Konföderation evangelischer Kirchen in Niedersachsen
- Herrnhuter Brüdergemeine
- Deutsches Nationalkomitee des Lutherischen Weltbundes (DNK / LWB)
- Reformierter Bund in Deutschland
- Diakonisches Werk Rheinland-Westfalen-Lippe e. V.
- Diakonisches Werk Mecklenburg-Vorpommern e. V.
- Diakonisches Werk Schleswig-Holstein e. V.
- Diakonisches Werk Bremen e. V.
- Diakonisches Werk Hamburg e. V.
- Diakonisches Werk evangelischer Kirchen in Niedersachsen e. V.
- Diakonisches Werk der Ev. Landeskirche in Baden e. V.
- Diakonisches Werk der Evangelisch-Lutherischen Kirche in Bayern e. V.
- Diakonisches Werk der evangelischen Kirche in Württemberg e. V.
- Diakonisches Werk Berlin-Brandenburg-schlesische Oberlausitz e. V.
- Diakonisches Werk der Evangelischen Kirche der Pfalz
- Diakonisches Werk in Hessen und Nassau und Kurhessen-Waldeck e. V.
- Diakonisches Werk der Ev.-Luth. Kirche in Oldenburg e. V.
- Diakonisches Werk Evangelischer Kirchen in Mitteldeutschland e. V. (ab 1. Januar 2025)
- Diakonisches Werk der Ev.-Luth. Landeskirche Sachsens e. V. (ab 1. Januar 2025)

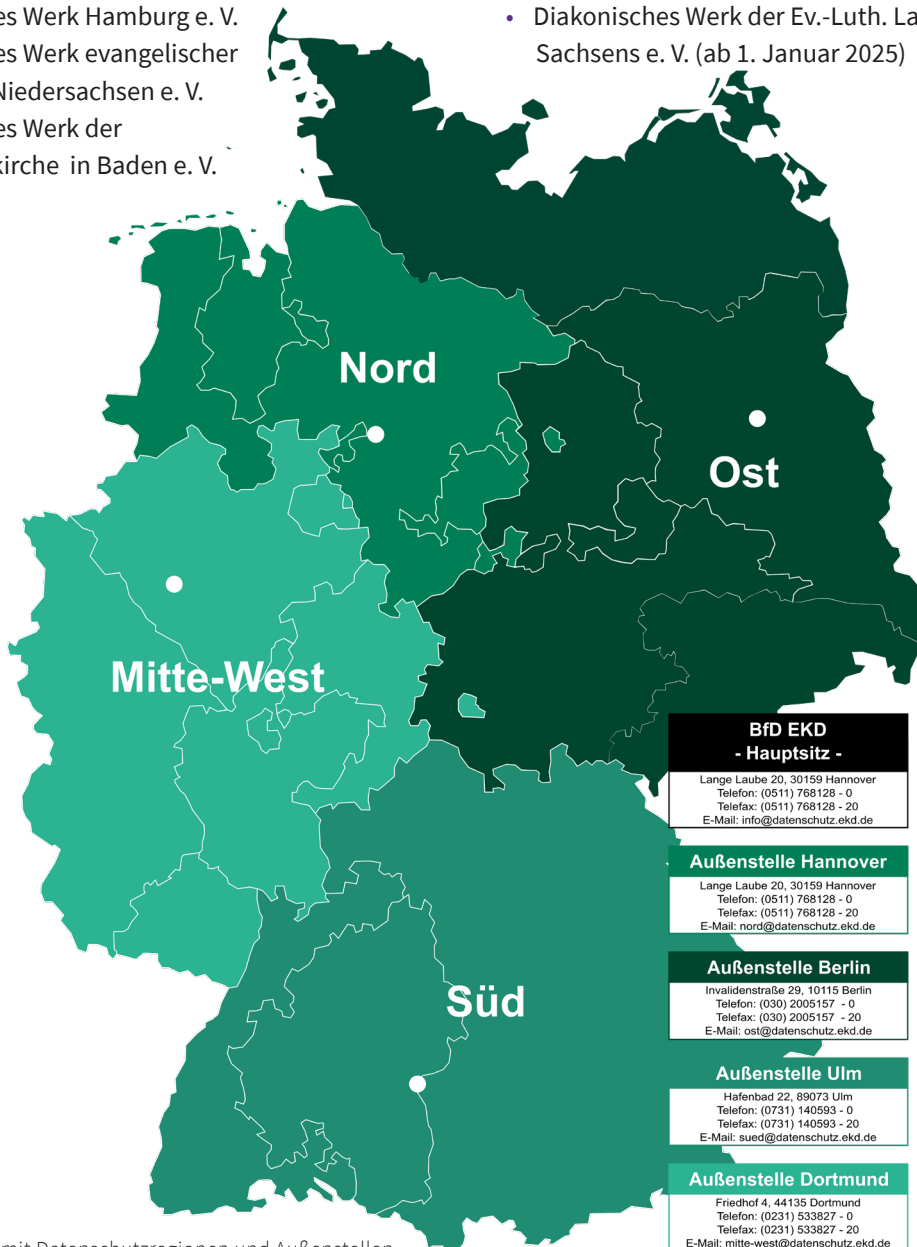


Abbildung 1: Karte mit Datenschutzregionen und Außenstellen

(Die Evangelische Landeskirche Anhalts sowie die Evangelisch-Lutherische Landeskirche Sachsens und ihre diakonischen Landesverbände haben zum 1. Januar 2025 die Datenschutzaufsicht auf den BfD EKD übertragen.)

Zur regionalen Gliederung der auf die EKD übertragenen Datenschutzaufsicht in den Gliedkirchen und diakonischen Landesverbänden wurden die vier Datenschutzregionen Nord, Ost, Süd und Mitte-West gebildet. In jeder Datenschutzregion befindet sich eine Außenstelle (Nord: Hannover; Ost: Berlin; Süd: Ulm; Mitte-West: Dortmund). Die regionale Zuordnung ist der Abbildung 1 auf Seite 19 zu entnehmen.

Die Behörde

Zur Wahrnehmung der gesetzlich normierten sowie der übertragenen Aufgaben der Datenschutzaufsicht existiert seit Anfang 2014 – in der Rechtsform einer unselbstständigen Einrichtung der EKD – die unabhängige und eigenständige Behörde „Der Beauftragte für den Datenschutz der EKD (BfD EKD)“.

Organisation

Die Behörde wird vom Beauftragten für den Datenschutz der EKD Herrn Michael Jacob geleitet und hat ihren Hauptsitz in Hannover. Die Standorte der vier Außenstellen sind der Abbildung 1 auf Seite 19 zu entnehmen. Im Rahmen der Errichtung der Behörde wurde seit dem Jahr 2014 eine komplette Behördenstruktur aufgebaut. Der personelle Aufbau erfolgte sukzessive entsprechend der tatsächlichen Aufgaben und der finanziellen Ausstattung der Behörde.

Die Behörde hatte im Berichtszeitraum insgesamt 23 (Plan-) Stellen. Alle Stellen waren besetzt. Die vier Außenstellen waren mit mindestens einer oder einem Regionalverantwortlichen (juristische Kompetenz), einer IT-Sachbearbeitung und einer Teamassistenz besetzt. Im Berichtszeitraum konnten die vakante Regionalverantwortlichen-Stelle in der Außenstelle Berlin, die vakante Stelle der IT-Sachbearbeitung am Hauptsitz sowie die Stellen der Teamassistenzen am Hauptsitz und in der Außenstelle Hannover erfolgreich wiederbesetzt werden. Die Auswahl von Mitarbeitenden erfolgte stets potenzial- und genderorientiert. Die Aufbauorganisation des BfD EKD zum 31. Dezember 2024 ist dem Organigramm auf Seite 21 zu entnehmen.

Die Teams der Außenstellen organisieren sich bei der Aufgabenerledigung unter Berücksichtigung des Geschäftsverteilungsplanes und der Geschäftsordnung des BfD EKD selbständig, ohne dass Mitarbeitende vor Ort Leitungsverantwortung haben. Somit unterstehen

alle Mitarbeitenden der Fach- und Dienstaufsicht der Behördenleitung.

In Ausgestaltung von grundlegenden organisatorischen Festlegungen wurden in der Vergangenheit folgende interne Regelungen erarbeitet, für verbindlich erklärt und im Berichtszeitraum ständig auf dem aktuellen Stand gehalten:

- Geschäftsordnung
- Leitlinien zur Informationssicherheit und zum Datenschutz
- Richtlinie zum Umgang mit der IT
- IT-Sicherheitskonzept nach dem Grundsatz des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Dienstvereinbarungen (z. B. zur privaten Nutzung von Internet und E-Mail etc.)
- Geschäftsverteilungsplan
- Aktenplan
- Verzeichnis von Verarbeitungstätigkeiten nach § 31 DSGVO (sog. „Verfahrensverzeichnis“)
- Diverse Hausverfügungen (z. B. zu Vertretungsregelungen, Zeichnungsbefugnissen, Beschaffungsentscheidungen etc.)
- Diverse Prozessbeschreibungen (zur Etablierung eines Qualitätsmanagementsystems)
- Styleguide

Zu Beginn der Corona-Pandemie wurde am Hauptsitz der Behörde in Hannover ein Studio mit Videokonferenztechnik eingerichtet. So wurde gewährleistet, dass alle Weiterbildungen und Veranstaltungen des BfD EKD auch in Pandemiezeiten weiter angeboten und online durchgeführt werden konnten. Im Berichtszeitraum wurde deutlich, dass auch nach Ende der Corona-Pandemie ein großer Bedarf besteht, Weiterbildungen und sonstige Veranstaltungen nicht nur präsentisch, sondern auch im Online-Format anzubieten.

Im Berichtszeitraum hat der BfD EKD außerdem das Programm „Zukunftsstrategie des BfD EKD“ initiiert. Ziel dieses Programms ist es, die Effizienz der Aufgabenerledigung weiter zu steigern und den Mehrwert der Behörde für die Gliedkirchen, gliedkirchlichen Zusammenschlüsse und diakonischen Landesverbände nachhaltig zu erhöhen und transparent darzustellen. Dabei werden sowohl der pandemiebedingte Digitali-



Abbildung 2: Organigramm des BfD EKD

sierungsschub als auch die fortschreitende allgemeine Digitalisierung berücksichtigt. Ein wesentlicher Bestandteil des Programms war die „Zukunftswerkstatt des BfD EKD“, zu der der BfD EKD im Mai 2023 Vertreterinnen und Vertreter aus Arbeitsbereichen der verfassten Kirche und der Diakonie eingeladen hatte. Ziel der Zukunftswerkstatt war es, Anforderungen an die Aufgabenerfüllung und die Dienstleistungsangebote des BfD EKD zu identifizieren. Die Veranstaltung diente als Plattform für einen konstruktiven Austausch und die Entwicklung gemeinsamer Perspektiven. Im Rahmen des Zukunftsstrategie-Programms wurden die internen Prozesse des BfD EKD analysiert und Optimierungspotenziale identifiziert. Diese wurden im Berichtszeitraum schrittweise durch konkrete Maßnahmen umgesetzt. Eine detaillierte Darstellung dieser Maßnahmen ist in diesem Kapitel den Bereichen Beratung und Weiterbildung zu entnehmen.

Personal

Mit dem Ziel, den Aufgabenbereich Personal stärker selbst wahrzunehmen, sind seit einigen Jahren die Abläufe und Zuständigkeiten für die Durchführung von Stellenbesetzungsverfahren neu geregelt und umgesetzt worden. In diesem Zusammenhang wurde zusammen mit dem Referat für Chancengerechtigkeit im Kirchenamt der EKD auch das Auswahlverfahren

stärker standardisiert. Auf Basis von funktionsbezogenen, standardisierten Fragenkatalogen soll die Chancengerechtigkeit bei der Personalauswahl erhöht und sichergestellt werden, dass die am besten geeignete Person für die jeweilige Stelle ausgewählt wird.

Die Vereinbarkeit von Beruf und Familie ist für den BfD EKD ebenfalls ein wichtiges Thema. Mit dem Ziel, die Mitarbeitendenzufriedenheit und damit auch die Qualität der Arbeitsergebnisse zu steigern, nimmt der BfD EKD seit 2020 am Auditprozess „berufundfamilie“ teil und wurde in das Zertifikat für die EKD aufgenommen. Darüber hinaus ist der BfD EKD seit der erfolgreichen Auditierung in der Arbeitsgruppe Vereinbarkeit von Beruf und Familie der EKD vertreten. Durch die Teilnahme in der Arbeitsgruppe wird sichergestellt, dass der BfD EKD seine Erfahrungen zum Thema Beruf und Familie in den weiteren Prozess einbringen kann und an den zukünftigen Entwicklungen in der EKD beteiligt ist. Alle drei Jahre ist das Zertifikat zur Sicherung der Qualität in einem sogenannten Dialogverfahren zu bestätigen, was im Berichtszeitraum erfolgreich gelang.

Im Sinne einer kontinuierlichen Personalentwicklung nehmen alle Mitarbeitenden regelmäßig und bedarfsgerecht an fachlichen sowie persönlichen Weiterbil-

dungsmaßnahmen teil. Mit dem Ziel, Fortbildungen als zentrales Instrument der Personalentwicklung zu fördern und die Abläufe und Inhalte von Fortbildungsmaßnahmen transparent zu regeln, hat der BfD EKD im Berichtszeitraum ein Fortbildungskonzept für die eigene Behörde entwickelt. Um die Arbeitsorganisation weiter zu flexibilisieren, wurde im Berichtszeitraum – gemeinsam mit der Mitarbeitervertretung und weiteren Dienststellen – eine Dienstvereinbarung über mobile Arbeit abgeschlossen. Im Bereich der Personalverwaltung wird der BfD EKD auch bei vermehrt eigenständiger Aufgabenwahrnehmung weiterhin von der Personalabteilung im Kirchenamt der EKD unterstützt.

Finanzen

Die Finanz- und Budgethoheit liegt vollständig beim BfD EKD. In Finanz- und Haushaltsangelegenheiten wurde der BfD EKD im Berichtszeitraum – wie bereits in der Vergangenheit – von der Abteilung Finanzen im Kirchenamt der EKD unterstützt. Die praktische Umsetzung und Abwicklung dieser Aufgaben erfolgte überwiegend direkt durch die Behörde des BfD EKD. Die Personal- und Sachkosten des BfD EKD werden über Beiträge von denjenigen finanziert, die die Datenschutzaufsicht entweder auf vertraglicher oder gesetzlicher Grundlage auf den BfD EKD übertragen haben. Diese Beiträge werden seit einer entsprechenden Gesetzesänderung im Jahr 2023 gemäß § 39 Abs. 3 Satz 3 DSG-EKD vom Rat der EKD auf Vorschlag des Finanzbeirats der EKD festgelegt.

Der Finanzbedarf des BfD EKD für Personal- und Sachkosten und die Beiträge wurden für das Jahr 2023 vom Finanzbeirat der EKD und – nach der entsprechenden Gesetzesänderung – für das Jahr 2024 vom Rat der EKD auf Vorschlag des Finanzbeirats neu festgelegt. Grundlage des Finanzbedarfs ist die mittelfristige Finanzplanung 2030 des BfD EKD, die in den Prozess zur Neuausrichtung der Finanzstrategie der EKD eingeordnet ist und kontinuierlich fortgeschrieben und aktualisiert wird. Der festgestellte Finanzbedarf des BfD EKD wurde im Berichtszeitraum zu zwei Dritteln auf den Bereich der verfassten Kirche und zu einem Drittel auf den Bereich der Diakonie umgelegt. Die Höhe der Beiträge errechnete sich im Bereich der verfassten Kirche neben einem Sockelbetrag jeweils zur Hälfte auf der Grundlage des Schlüssels Gemeindegli-

derzahlen und des Schlüssels Beschäftigtenzahlen. Im Bereich der Diakonie wurden die Beiträge nur auf Grundlage der Beschäftigtenzahlen ermittelt. Diese nach verschiedenen Berechnungsschlüsseln ermittelten Beiträge sind erst ab dem Zeitpunkt der tatsächlichen Übertragung der Datenschutzaufsicht auf den BfD EKD zu entrichten.

Um die Transparenz und Nachvollziehbarkeit der Finanzmittelverwendung im Rahmen des Prozesses zur Neuausrichtung der Finanzstrategie der EKD zu erhöhen, professionalisiert die Behörde kontinuierlich ihr Handeln in Finanz- und Haushaltsangelegenheiten. Eine Neustrukturierung ermöglicht eine präzisere Darstellung aller Erträge und Aufwendungen des BfD EKD im Haushaltsplan der EKD. Weitere Einzelheiten sind den Haushaltsplänen und Haushaltsabschlüssen der EKD zu entnehmen.

IT-Infrastruktur und Kommunikation

Im Bereich der vorhandenen technischen Infrastruktur ermöglichen das eigenständige IT-Konzept des BfD EKD, die damit verbundene zentrale Terminalserverlösung sowie die Ausstattung der Mitarbeitenden mit mobilen Endgeräten ein ortsunabhängiges Arbeiten im (digitalen) Aktenplan. Nicht nur analoge, sondern auch digitale Informationen können so zentral abgelegt und durch ein Rollenkonzept gesichert werden.

Zur Absicherung der digitalen Kommunikation verfügt der BfD EKD über verschiedene Möglichkeiten der Ende-zu-Ende-Verschlüsselung wie die Nutzung asymmetrischer Verschlüsselung (PGP) und die Verschlüsselung über den Dienst FTAPI.

Die Sicherstellung einer funktionierenden internen Kommunikation ist ein weiterer wichtiger Schlüssel zur Professionalisierung der Arbeit des BfD EKD. Grundsätzlich finden alle zwei Monate hierarchieübergreifende Dienstbesprechungen per Videokonferenz sowie im Frühjahr und im Herbst jeweils zweitägige Klausurtagungen in Präsenz statt. Zum fachlichen Austausch unter den Mitarbeitenden mit der gleichen Funktion innerhalb der Behörde (Regionalverantwortliche, IT-Sachbearbeitende und Teamassistenzen) werden zwischen den einzelnen Dienstbesprechungen regelmäßig Videokonferenzen und präsentische Treffen

durchgeführt. Davon unabhängig organisieren sich die Mitarbeitenden in den Außenstellen und am Hauptsitz der Behörde eigenständig zum weiteren fachlichen und organisatorischen Austausch.

Der BfD EKD hat im Berichtszeitraum zur weiteren Digitalisierung der Behörde und zur Stärkung der standortübergreifenden Zusammenarbeit das Projekt „Digitalisierung“ weiter vorangetrieben. Im Rahmen dieses Projektes hat der BfD EKD ein softwarebasiertes Adress- und Veranstaltungsmanagement eingeführt und plant in einer zweiten Phase die Einführung eines Dokumentenmanagementsystems. Zudem wurde im Berichtszeitraum die Telefonanlage ausgebaut, um die vorhandene Technologie Voice over IP (VoIP) vollumfänglich nutzen zu können und die Kommunikation im Rahmen der mobilen Arbeit bestmöglich zu unterstützen.

Aufgaben und Tätigkeiten

In Erfüllung des gesetzlichen Auftrags wacht der BfD EKD über die Einhaltung des Datenschutzes. Dabei will er vor

allem beraten und unterstützen. Zu den Aufgaben des BfD EKD gehört aber auch, die Einhaltung des Datenschutzes zu kontrollieren und zu überwachen. Über allem Handeln steht dabei der Zweck jedes modernen Datenschutzes: Jede einzelne Person ist davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird.

Der BfD EKD ist inhaltlich in den Bereichen rechtlicher Datenschutz, technischer Datenschutz und Organisation des Datenschutzes tätig. Sämtliche Tätigkeiten des BfD EKD sind den drei Aufgaben Aufsicht, Beratung und Weiterbildung zugeordnet. Eine grobe Übersicht über die Aufgaben und Tätigkeiten des BfD EKD ist der Tabelle 1 auf Seite 23 zu entnehmen. Über die Anzahl der in den Jahren 2023 und 2024 bearbeiteten Vorgänge in den einzelnen Aufgabenbereichen geben die Tabellen 2 und 3 auf Seite 24 Auskunft.

Aufsicht

Im Bereich seines aufsichtlichen Handelns verzeichnet

Tabelle 1: Aufgaben-Tätigkeitsmatrix des BfD EKD (Die Aufgaben sind jeweils gegliedert in die Bereiche rechtlicher Datenschutz (R), technischer Datenschutz (T) und Organisation des Datenschutzes (O)).

Aufgabe \ Tätigkeit	Aufsicht			Beratung			Weiterbildung		
	R	T	O	R	T	O	R	T	O
Bearbeitung von Beschwerden	✓	✓	✓						
Etablieren einer proaktiven Datenschutzaufsicht	✓	✓	✓						
Materialdienst (standardisierte Beratung)				✓	✓	✓			
einzelfallbezogen	✓	✓	✓	✓	✓	✓			
einheitliches und aufeinander abgestimmtes (modulares) Weiterbildungsangebot für örtlich Beauftragte für den Datenschutz							✓	✓	✓
individuelles Angebot für weitere Zielgruppen							✓	✓	✓
schwerpunktsetzend	✓	✓	✓	✓	✓	✓	✓	✓	✓

Tabelle 2: Statistik über die Anzahl der Tätigkeiten im Jahr 2023

	Aufsicht	Beratung	Weiterbildung	Gesamt
Hauptsitz	18	4	1	23
AS Hannover	77	66	1	144
AS Berlin	110	88	6	204
AS Ulm	202	180	2	384
AS Dortmund	202	124	4	330
Summe	609	462	14	1085

Tabelle 3: Statistik über die Anzahl der Tätigkeiten im Jahr 2024

	Aufsicht	Beratung	Weiterbildung	Gesamt
Hauptsitz	10	19	2	31
AS Hannover	165	72	2	239
AS Berlin	177	93	4	274
AS Ulm	334	154	2	490
AS Dortmund	221	75	2	298
Summe	907	413	12	1332

Tabelle 4: Statistik über die Anzahl der gemeldeten Datenpannen und eingegangenen Beschwerden in den Jahren 2023 und 2024

	2023	2024
Datenpannen	450	754
Beschwerden	159	153
Summe	609	907

der BfD EKD seit Inkrafttreten des neuen EKD-Datenschutzgesetzes ständig wachsende Zahlen von Beschwerden und Datenpannenmeldungen. Näheres ist der Tabelle 4 auf Seite 24 zu entnehmen. Dabei verfestigt sich der Eindruck, dass den Datenpannen häufig ähnlich gelagerte Verstöße – insbesondere Diebstahl und Verlust von dienstlichen mobilen Endgeräten sowie falsch adressierte E-Mails oder Faxe – zu Grunde liegen. Diese Erkenntnis hat der BfD EKD bei seinem Handeln bereits stärker berücksichtigt als in der Vergangenheit. Das erhöhte Aufkommen von Datenpannenmeldungen im Jahr 2024 ist vor allem auf die beim Anbieter der Kita-App „Stay Informed“ aufgetretene Fehlkonfiguration eines freizugänglichen Webservers zurückzuführen. Infolgedessen kam es in einer Vielzahl von kirchlichen und diakonischen Einrichtungen zu Datenpannen, die dem BfD EKD gemeldet wurden. Sämtliche eingegangenen Beschwerden, Datenpannenmeldungen und Eingaben wurden im Berichtszeitraum ordnungsgemäß bearbeitet.

Schwerpunktprüfungen

Aufgrund der gesetzlichen Anforderungen in § 43 und § 44 DSGVO-EKD sowie der Vorgaben aus der Rechtsprechung des EuGH besteht für den BfD EKD die Verpflichtung, verantwortliche Stellen zu prüfen, ohne dass ein konkreter Anlass (z. B. Beschwerde oder Hinweis) vorliegt. Daher hat der BfD EKD ein Verfahren zur Durchführung von sogenannten Schwerpunktprüfungen erarbeitet. Im Sommer 2023 initiierte der BfD EKD die zweite Schwerpunktprüfung, die in 20 zufällig ausgewählten evangelischen Krankenhäusern durchgeführt wurde. Die Datenerhebung erfolgte primär über einen Online-Fragebogen, ergänzt durch Einreichung von Unterlagen und Vor-Ort-Prüfungen. Nach Ablauf der Abgabefrist konnte eine sehr hohe Rücklaufquote verzeichnet werden. Die Auswertung der eingereichten Dokumente sowie die abschließenden Prüfungen wurden in den zuständigen Außenstellen durchgeführt. Es wurde für jedes geprüfte Krankenhaus ein individuelles Abschluss schreiben erstellt. Eine Beanstandung musste ausgesprochen werden. Mit der Veröffentlichung des Abschlussberichts auf der Website des BfD EKD wurde die zweite Schwerpunktprüfung abgeschlossen. (<https://datenschutz.ekd.de/ueber-uns/schwerpunktpruefungen/>) Die Ergebnisse dieser Prüfung sind in Kapitel III des Tätigkeitsberichts dokumentiert. Die nächste

Schwerpunktprüfung findet im Bereich der kirchlichen Verwaltung statt mit dem Schwerpunkt Umgang mit Meldedaten.

KDM

Im Berichtszeitraum hat der BfD EKD im Rahmen einer ökumenischen Projektgruppe die Entwicklung des Kirchlichen Datenschutzmodells (KDM) abgeschlossen. Die Projektgruppe empfiehlt das KDM als Werkzeug zur Auswahl und Bewertung technischer und organisatorischer Maßnahmen bei den beteiligten Aufsichtsbehörden anzuwenden, um so die praktische Umsetzung von gesetzlichen Anforderungen zu ermöglichen. Das KDM bietet sowohl der Aufsichtsbehörde als auch den verantwortlichen Stellen und den örtlich Beauftragten für den Datenschutz in kirchlichen und diakonischen Einrichtungen ein Verfahren, das auf systematische und reproduzierbare Weise die Umsetzung der kirchlichen Datenschutzvorgaben in konkrete technische und organisatorische Maßnahmen beschreibt. Im Berichtszeitraum erfolgte die Finalisierung eines Fallbeispiels zum KDM und dessen Veröffentlichung auf der Internetseite <https://kirchliches-datenschutzmodell.de>. Auf dem ökumenischen Datenschutztag im März 2023 ist die ökumenische Projektgruppe KDM aufgelöst worden. Zur Weiterentwicklung des KDM und der Rezeption künftiger SDM-Versionen ist eine neue Projektgruppe „KDM-Werkstatt“ gebildet worden. Ihre Kernaufgaben werden von je einer Koordinatorin oder einem Koordinator von evangelischer und von katholischer Seite wahrgenommen. Das KDM basiert auf dem Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK).

Beratung

Die Bearbeitung sämtlicher Beratungsanfragen ist ein Hauptbestandteil der Arbeit aller Mitarbeitenden des BfD EKD. Dabei ist erkennbar, dass die Anfragen den folgenden Themenbereichen zugeordnet werden können:

- Datenverarbeitung und Auskunftsrecht
- Fragen im gemeindlichen Alltag
- Besonderheiten im diakonischen Bereich
- Aufbewahrung und Löschung
- Verarbeitung von Beschäftigtendaten
- Einsatz von Videokameras

- Digitale Kommunikation
- Datensicherheit und Verschlüsselung
- Nutzung von Social Media und Software
- Örtlich Beauftragte für den Datenschutz

Auch beim aufsichtlichen Handeln des BfD EKD geht es häufig um diese Themen. Fachliche Erläuterungen zu den Themen sind daher in ausführlicher Form in Kapitel III „Themen bei Aufsicht und Beratung“ dieses Tätigkeitsberichts zu finden.

Materialien

In Ergänzung zu einzelfallbezogenen Beratungen in mündlicher Form (vor allem im persönlichen Gespräch oder telefonisch) und schriftlicher Form (per E-Mail oder als Brief) sind – auch mit dem Ziel der stetigen Standardisierung und Professionalisierung der Beratung – zu vielen datenschutzrechtlich und -technisch relevanten Fragestellungen Materialien erarbeitet worden. Die Materialien sind den acht unterschiedlichen Formaten Entschlüsselung, Häufig gestellte Fragen (FAQ), Handreichung, Kurzinformation, Kurzpapiere, Muster, Sensibilisierung und Stellungnahme zugeordnet. Die Bereitstellung dieser Materialien erfolgt insbesondere über die Rubrik Infothek auf der Website des BfD EKD unter <https://datenschutz.ekd.de/infothek/> und in Papierform.

Telefonsprechstunde

Im Rahmen des Programms „Zukunftsstrategie des BfD EKD“ hat der BfD EKD im April 2023 eine offene Telefonsprechstunde eingeführt, die seitdem wöchentlich donnerstags von 14:00 Uhr bis 15:00 Uhr angeboten wird. Während dieser Sprechzeiten stehen den Anrufern juristische und technische Mitarbeitende des BfD EKD beratend zur Verfügung. Dieses niederschwellige Angebot dient dazu, auf Fragen rund ums Thema Datenschutz eine erste Einschätzung zu geben und den Austausch zu intensivieren. Um die Telefonsprechstunde bekannt zu machen, hat sie der BfD EKD gezielt auf verschiedenen Informations- und Weiterbildungsveranstaltungen vorgestellt und weist auch auf seiner Website darauf hin. Die Resonanz ist positiv und gleichbleibend stabil.

Schulungsfolien

Zu den Aufgaben von örtlich Beauftragten für den Datenschutz gehört auch die Sensibilisierung und

Schulung der Mitarbeitenden im Bereich Datenschutz. Um die örtlich Beauftragten für den Datenschutz bei dieser Aufgabe zu unterstützen, hat der BfD EKD im Rahmen des Programms „Zukunftsstrategie des BfD EKD“ Musterfolien zur Schulung von Mitarbeitenden entwickelt und stellt diese über seine Homepage zur Verfügung. Die Musterfolien vermitteln grundlegendes Wissen über gesetzliche und technische Aspekte des Datenschutzes sowie dessen Anwendung im beruflichen Alltag. Sie sind so gestaltet, dass sie flexibel eingesetzt werden können. Die örtlich Beauftragten für den Datenschutz haben die Möglichkeit, die Inhalte individuell anzupassen oder lediglich einzelne Abschnitte zu nutzen, je nach den spezifischen Anforderungen. Der BfD EKD bietet die Folien in verschiedenen digitalen Formaten an, die eine einfache Integration in Schulungsmaßnahmen ermöglichen. Dieses Angebot unterstreicht das Engagement des BfD EKD, die örtlich Beauftragten in ihrer wichtigen Rolle zu stärken, die Einhaltung gesetzlicher Datenschutzerfordernisse zu fördern und das Bewusstsein für Datenschutz in kirchlichen und diakonischen Einrichtungen nachhaltig zu verankern.

Weiterbildung

Der BfD EKD setzt neben den Aufgaben Aufsicht und Beratung einen weiteren Schwerpunkt seiner Arbeit im Bereich Weiterbildung. Dies ergibt sich aus den in § 43 DSGVO gesetzlich festgelegten Aufgaben der Aufsichtsbehörden. Demnach ist es Aufgabe des BfD EKD zu sensibilisieren, zu informieren und die örtlich Beauftragten für den Datenschutz zu schulen und weiterzubilden.

Für den BfD EKD sind die örtlich Beauftragten für den Datenschutz als strategische Partner eine wichtige Zielgruppe im Bereich Weiterbildung. Der BfD EKD vermittelt den örtlich Beauftragten für den Datenschutz die erforderliche Fachkunde und informiert über aktuelle rechtliche und technische Entwicklungen. Auch für andere Zielgruppen bietet der BfD EKD Veranstaltungen an. Weitere Informationen sind auf der Website des BfD EKD unter <https://datenschutz.ekd.de/veranstaltungen/> zu finden.

Grund- und Aufbauseminare

Die jeweils dreitägigen Grund- bzw. Aufbauseminare richten sich an (künftige) örtlich Beauftragte für den

Datenschutz in kirchlichen und diakonischen Einrichtungen aus Landeskirchen und diakonischen Landesverbänden. Mit der Teilnahme am Grundseminar wird die Voraussetzung für die Teilnahme am Aufbauseminar erlangt. Die Durchführungsverantwortung für die Grundseminare liegt bei den jeweiligen Außenstellen des BfD EKD. In dem dreitägigen Grundseminar für örtlich Beauftragte für den Datenschutz wird eine Basisqualifikation zum Datenschutz vermittelt. In drei Modulen wird eine Einführung in den rechtlichen und technischen Datenschutz sowie in die Organisation des Datenschutzes gegeben.

Die dreitägigen Aufbauseminare, die inhaltlich auf den Basisqualifikationen des Grundseminars aufbauen, werden vom Hauptsitz des BfD EKD durchgeführt. Das Aufbauseminar richtet sich an örtlich Beauftragte für den Datenschutz in kirchlichen und diakonischen Einrichtungen, die bereits am Grundseminar des BfD EKD teilgenommen haben. Die Aufbauseminare werden getrennt für örtlich Beauftragte für den Datenschutz im Bereich der sog. verfassten Kirche und im Bereich der Diakonie angeboten und durchgeführt. Die inhaltlichen Themen zum Datenschutz werden entsprechend gewichtet. In zwei Modulen werden rechtliche und technische Datenschutzthemen vertiefend behandelt.

Das Aufbauseminar schließt mit einer häuslichen Abschlussarbeit zur Erlangung der Fachkunde ab.

Im Rahmen des Programms „Zukunftsstrategie des BfD EKD“ wurde entschieden und umgesetzt, die Seminarunterlagen nur noch digital per E-Mail zu versenden. Dies ist sowohl kosteneffizienter als auch nachhaltiger im Vergleich zur bisherigen Praxis, bei der gedruckte Unterlagen zur Verfügung gestellt wurden.

Die Anzahl der in den Jahren 2023 und 2024 durchgeführten Grund- und Aufbauseminare können den Tabellen 5 und 6 entnommen werden. An jedem Grund- und Aufbauseminar nahmen maximal 25 Personen teil.

Datenschutz-Infotage

Mit den vier Regionalkonferenzen pro Jahr, den sog. Datenschutz-Infotagen, wird eine Plattform angeboten, auf der sich einmal jährlich in jeder Datenschutzregion örtlich Beauftragte für den Datenschutz fachlich und persönlich mit dem BfD EKD austauschen können. Bei dieser Tagesveranstaltung wird ein aktuelles Datenschutzthema ausführlich in mehreren Fachvorträgen aus rechtlicher, technischer und praktischer Sicht behandelt. Die Datenschutz-Infotage werden inhaltsgleich in jeder Datenschutzregion veranstaltet.

Tabelle 5: Statistik über die Anzahl der durchgeführten Grund- und Aufbauseminare im Jahr 2023

	AS Berlin	AS Dortmund	AS Hannover	AS Ulm	Hauptsitz	Summe
Grundseminare 2023	1	1	1			3
Aufbaueminare 2023					4	4
Gesamt	1	1	1	1	4	7

Tabelle 6: Statistik über die Anzahl der durchgeführten Grund- und Aufbauseminare im Jahr 2024

	AS Berlin	AS Dortmund	AS Hannover	AS Ulm	Haupt-sitz	Summe
Grundseminare 2024	1	1		1		3
Aufbaueminare 2024					3	3
Gesamt	1	1		1	3	6

Tabelle 7: Statistik über die Anzahl der durchgeführten Erfa-Kreise in den Jahren 2023 und 2024

	AS Berlin	AS Dortmund	AS Hannover	AS Ulm	Summe
Erfa-Kreise 2023	2	4	2	4	12
Erfa-Kreise 2024	2	4	2	4	12
Gesamt	4	8	4	8	24

Die Datenschutz-Infotage richten sich an (künftige) örtlich Beauftragte für den Datenschutz in kirchlichen und diakonischen Einrichtungen aus Landeskirchen und Diakonischen Landesverbänden. Die Datenschutz-Infotage für örtlich Beauftragte für den Datenschutz werden vom Hauptsitz des BfD EKD sowie von den Mitarbeitenden der jeweiligen Außenstellen des BfD EKD geleitet und durchgeführt. Im Jahr 2023 wurden vier Datenschutz-Infotage und im Jahr 2024 insgesamt sechs Veranstaltungen durchgeführt. Im Jahr 2023 waren die Hauptthemen der Umgang mit sensiblen Daten in der Diakonie, die Verarbeitung von Meldewesendaten sowie ein Fallbeispiel zur Erstellung eines Löschkonzepts am Beispiel von Meldewesendaten. Im Jahr 2024 standen die Nutzung Künstlicher Intelligenz und die damit verbundenen Herausforderungen und Risiken für Kirche und Diakonie im Vordergrund. Seit der Corona-Pandemie werden die Datenschutz-Infotage sowohl in Präsenz als auch online durchgeführt. An den Datenschutz-Infotagen nahmen in den Jahren 2023 und 2024 jeweils etwa 300 Personen teil.

Erfahrungsaustauschkreise

Erfahrungsaustausch und Vernetzung sind wichtige Instrumente zur Unterstützung der örtlich Beauftragten für den Datenschutz in ihrer täglichen Arbeit. Um diesen Austausch zu fördern, organisiert der BfD EKD regelmäßig Erfahrungsaustauschkreise (Erfa-Kreise). Diese bieten den (zukünftigen) örtlich Beauftragten für den Datenschutz aus kirchlichen und diakonischen Einrichtungen die Gelegenheit, sich intensiv mit datenschutzrechtlichen und technischen Fragestellungen auseinanderzusetzen und sich dazu fachlich auszutauschen. Darüber hinaus ermöglichen die Erfa-Kreise eine Vernetzung der Teilnehmenden untereinander, auch wenn diese bei Online-Veranstaltungen nur eingeschränkt möglich ist. Außerdem soll genug Raum für die Besprechung aktueller Probleme und konkreter

Fragen bleiben. Die Erfa-Kreise werden in unregelmäßigen Abständen von den Außenstellen des BfD EKD in Präsenz und online angeboten und von den Regionalverantwortlichen und IT-Sachbearbeitenden moderiert. Die Termine werden auf der Website des BfD EKD bekanntgegeben. Die Anzahl der durchgeführten Erfa-Kreise kann der Tabelle 7 entnommen werden.

E-Learning-Plattform

Ein wesentlicher Teil des Programms „Zukunftsstrategie des BfD EKD“ ist das im Berichtszeitraum realisierte Angebot einer E-Learning-Plattform. Das Angebot zielt darauf ab, Mitarbeitenden in Kirche und Diakonie ein flexibles und leicht zugängliches Schulungsformat anzubieten. Der BfD EKD hat im Jahr 2023 ein leistungsfähiges E-Learning-System installiert und den Kurs „Basisschulung Datenschutz“, der die wesentlichen Grundkenntnisse für den sicheren Umgang mit personenbezogenen Daten vermittelt, erstellt. Seit dem Start des Kurses im April 2024 absolvieren durchschnittlich rund 400 Mitarbeitende den Kurs monatlich. Der E-Learning-Kurs soll kontinuierlich weiterentwickelt werden.

Sensibilisierung

Daneben widmet sich der BfD EKD auch der Sensibilisierung von anderen Beschäftigten und (Leistungs-)Gremien zu datenschutzrechtlichen und -technischen Themen mit individuellen Vorträgen. Im Berichtszeitraum hat der BfD EKD ungefähr 20 Vorträge in unterschiedlichen kirchlichen und diakonischen Einrichtungen sowie Gremien gehalten. Die Vorträge vermittelten adressatengerechte Inhalte und hatten das Ziel, die Teilnehmenden gleichzeitig für das Thema Datenschutz zu sensibilisieren und praktische Hinweise zu geben. Die Vorträge werden individuell von den Regionalverantwortlichen und IT-Sachbearbeitenden in den jeweiligen Außenstellen des BfD EKD sowie vom Beauftragten für den Datenschutz der EKD gestaltet.

Schwerpunkthemen

Neben den regulären Aufgaben (Aufsicht, Beratung, Weiterbildung) beschäftigt sich der BfD EKD mit dem Thema Datenschutz auch unter Berücksichtigung von vier Schwerpunkthemen (Kinder, Jugendliche und junge Erwachsene – Diakonie (Gesundheitsdatenschutz) – Ehrenamtliche – Mitarbeitende (Beschäftigtendatenschutz)). Jede Außenstelle bearbeitet ein Schwerpunkthema. Um der kirchlichen Datenschutzaufsicht somit auch zielgruppenorientiert gerecht zu werden, wurden im Berichtszeitraum mit diesen vier Schwerpunkthemen folgende Akzente gesetzt.

Kinder, Jugendliche und junge Erwachsene

In Kirche und Diakonie werden eine Vielzahl von Kindertageseinrichtungen, Jugendhilfeeinrichtungen und Schulen betrieben. In diesen Einrichtungen gibt es viele Berührungspunkte zwischen der Zielgruppe Kinder, Jugendliche und junge Erwachsene und dem Thema Datenschutz. Im Berichtszeitraum wurde zur Sensibilisierung von Schülerinnen und Schülern das vom BfD EKD erstellte PosterMagazin mit dem Titel „Du siehst mich?!“ veröffentlicht. Darin werden Datenschutzthemen aus dem Alltag von Kindern und Jugendlichen aufgegriffen und altersgerecht illustriert. Daneben gibt es Tipps zu datenschutzfreundlichen Einstellungen für mobile Endgeräte. Das PosterMagazin enthält ebenfalls Hintergrundtexte, die sich eher an die Lehrkräfte wenden und diesen einen Einstieg im Unterricht in das Thema Datenschutz bieten oder auch an Pfarrerinnen und Pfarrer, um als Diskussionsgrundlage im (Konfirmanden-)Unterricht eingesetzt zu werden. Geplant ist zudem eine Handreichung, die das Thema Datenschutz in Kindertageseinrichtungen aufgreift und erläutert. Im Berichtszeitraum hat der BfD EKD außerdem mehrere Vorträge zum Schwerpunkthema gehalten. Zur Vernetzung mit den evangelischen Schulen nimmt der BfD EKD regelmäßig an der Wirtschaftskonferenz der Evangelischen Schulbünde teil. Die Vernetzung mit den staatlichen Aufsichtsbehörden im Arbeitskreis Schulen und Bildungseinrichtungen der DSK hat sich im Berichtszeitraum weiter etabliert.

Gesundheitsdatenschutz

Im Berichtszeitraum stellten sich in kirchlichen und diakonischen Einrichtungen zahlreiche Fragen im

Bereich des Gesundheitsdatenschutzes. Auch in evangelischen Krankenhäusern werden eine Vielzahl sensibler Gesundheitsdaten verarbeitet. Daher wählte der BfD EKD diesen Bereich für seine zweite Schwerpunktprüfung aus, die zum Beginn des Berichtszeitraums gestartet ist und an dessen Ende abgeschlossen wurde. Für eine noch bessere und intensivere Zusammenarbeit innerhalb der evangelischen Kirche organisiert der BfD EKD die Fachgruppe Diakonie, um bereichsspezifische Fragen des Datenschutzes unter Beteiligung von örtlich Beauftragten für den Datenschutz gemeinsam zu beantworten und einheitliche Standards zu entwickeln. Zur Vernetzung mit den staatlichen Aufsichtsbehörden und zur einheitlichen Rechtsanwendung nimmt der BfD EKD seit einigen Jahren am Arbeitskreis Gesundheit und Soziales der DSK teil.

Ehrenamtliche

Datenschutz spielt auch beim ehrenamtlichen Engagement in Kirche und Diakonie eine wichtige Rolle. Von der einfachen Mitgliederverwaltung über die Nutzung von Cloud-Diensten, die Öffentlichkeitsarbeit mittels Website und Social Media bis hin zu Online-Veranstaltungen gehört der Umgang mit personenbezogenen Daten zum Ehrenamt. Ehrenamtliche suchen im Rahmen ihres Engagements praxisnahe Hilfen zur Umsetzung datenschutzrechtlicher Vorgaben. Das vorhandene Wissen zum Datenschutz ist dabei unterschiedlich ausgeprägt. Im Berichtszeitraum wurde darum individuell sensibilisiert, um die Ehrenamtlichen in ihrer Tätigkeit bestmöglich zu unterstützen.

Beschäftigtendatenschutz

Das Thema Beschäftigtendatenschutz betrifft alle Bereiche von Kirche und Diakonie, sobald personenbezogene Daten von Mitarbeitenden verarbeitet werden. Auch personenbezogene Daten von Bewerberinnen und Bewerbern sowie personenbezogene Daten von ausgeschiedenen Mitarbeitenden fallen unter den gesetzlichen Schutz gemäß § 49 DSGVO. Im Berichtszeitraum wurden regelmäßig Themen aus dem Bereich des Beschäftigtendatenschutzes im Rahmen von Veranstaltungen und Sensibilisierungen aufgegriffen. Dabei hatte im Berichtszeitraum die Digitalisierung von Personalakten besondere Relevanz. Zur Wahrnehmung des Schwerpunkthemas gehört auch die Teilnahme des BfD EKD am Arbeitskreis Beschäftigtendatenschutz der DSK.

Öffentlichkeitsarbeit

Der BfD EKD verfolgt – auch im Hinblick auf eine standardisierte Beratung, mit gezielten Aktionen, Produkten und Plattformen – das Ziel, das Thema kirchlicher Datenschutz modern, attraktiv und leicht in die (kirchliche) Öffentlichkeit und den Menschen nahe zu bringen.

Der wichtigste Kommunikationskanal des BfD EKD ist dessen Internetauftritt. Der BfD EKD nutzt diese Plattform, um fortwährend aktuelle Nachrichten und Informationen, Pressemitteilungen sowie Materialien zur Verfügung zu stellen. Interessierte können so stets auf dem Laufenden bleiben und die aktuellen Entwicklungen im Bereich des kirchlichen Datenschutzes nachvollziehen. Im Bereich Infothek können interessierte Personen die vom BfD EKD erstellten Materialien herunterladen. Einige Materialien, die in den acht Kategorien Entschließung, Häufig gestellte Fragen (FAQ), Handreichung, Kurzinformation, Kurzpapiere, Muster, Sensibilisierung und Stellungnahme veröffentlicht werden, stellt der BfD EKD auch als Printprodukte bereit. Interessierte haben die Möglichkeit Printprodukte zum Selbstkostenpreis zu erwerben. Folgende Materialien wurden vom BfD EKD im Berichtszeitraum erarbeitet und veröffentlicht:

- Häufig gestellte Fragen (FAQ)
 - Häufig gestellte Fragen zum Auskunftsanspruch nach § 19 DSGVO-EKD
 - Häufig gestellte Fragen zum EU-US Data Privacy Framework
- Handreichung
 - Schulungsfolien zur Sensibilisierung von Mitarbeitenden
 - PosterMagazin zum Datenschutz für Kinder und Jugendliche
- Sensibilisierung
 - Vertrag zur Auftragsverarbeitung und Zusatzklärung

Zudem veröffentlicht der BfD EKD seit 2017 in regelmäßigen Abständen eigene Pressemitteilungen. Im Berichtszeitraum wurden folgende eigene Pressemitteilungen veröffentlicht:

- Diakonie lebt Datenschutz – BfD EKD äußert sich zum Europäischen Datenschutztag 2023, veröffentlicht am 28. Januar 2023

- BfD EKD legt 4. Tätigkeitsbericht vor, veröffentlicht am 23. Juni 2023

Außerdem wurden auf der Internetseite des BfD EKD unter anderem fachliche Beiträge zu folgenden Themen veröffentlicht:

- Örtlich Beauftragte für den Datenschutz dürfen auch Mitarbeitervertretungen kontrollieren
- Das neue EU-U.S. Data Privacy Framework – Was gilt nun?
- EU einigt sich auf die weltweit erste Verordnung zur Regulierung von Künstlicher Intelligenz
- 40 Jahre Volkszählungsurteil und Grundrecht auf informationelle Selbstbestimmung
- Sprachmodelle – Künstliche Intelligenz – Datenschutz
- „Kirchen-App“ Churchpool
- EU-Parlament beschließt KI-Verordnung
- Sicherheitslücke bei der KiTa-App Stay Informed aufgedeckt
- Kritische Sicherheitslücke in Palo Alto Network Firewalls ermöglicht Root-Zugriff
- Umgang mit erweiterten Führungszeugnissen
- Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder veröffentlicht Orientierungshilfe zu Künstlicher Intelligenz und Datenschutz
- Das TMG wird zum DDG und das TTDSG zum TDDDG – Handlungsbedarf für Webseitenbetreiber
- EKD-Synode evaluiert Datenschutzgesetz
- Häufig auftretende Fehler bei der Erstellung einer DSFA

Um auch über andere Kommunikationskanäle die Sensibilisierung weiter voranzutreiben, verfasst der BfD EKD regelmäßig Artikel für kirchliche und diakonische Zeitschriften und gibt Interviews. Im Berichtszeitraum wurde folgendes Interview veröffentlicht:

- Fünf Jahre DSGVO-EKD – Interview mit BfD EKD Michael Jacob auf <https://artikel91.eu>

Seit 2019 arbeitet der BfD EKD gemeinsam mit den katholischen Diözesandatenschutzbeauftragten in der katholischen Kirche kontinuierlich an der Weiterentwicklung des Kirchlichen Datenschutzmodells (KDM). Im März 2023 ist das Fallbeispiel zum KDM, zur Dokumentation in Kindertageseinrichtungen, online

gestellt worden. Auf der Internetseite <https://kirchliches-datenschutzmodell.de> können Interessierte neben dem Fallbeispiel auch weitere Materialien herunterladen.

Vernetzung

Der BfD EKD baute auch im Berichtszeitraum seine Kontakte im kirchlichen und staatlichen Umfeld weiter aus, um sich als Datenschutzaufsichtsbehörde nachhaltig zu etablieren. Hierfür knüpfte der BfD EKD beispielsweise in Gremien, Arbeitsgruppen und auf Veranstaltungen Kontakte, die zukünftig weiter ausgebaut werden. Bestehende Kontakte wurden gepflegt.

In der evangelischen Kirche

Der BfD EKD tauscht sich einmal im Jahr im persönlichen Gespräch mit der Ratsvorsitzenden der EKD zu strategischen und konzeptionellen Aspekten des kirchlichen Datenschutzes aus. Daneben steht der BfD EKD in regelmäßigem Kontakt zum Präsidenten des Kirchenamtes der EKD, zu den Abteilungsleitungen Recht und Finanzen sowie zu dem für Datenschutzrecht zuständigen Referenten und dem Leiter der Stabstelle Digitalisierung im Kirchenamt der EKD.

Darüber hinaus steht der BfD EKD in regelmäßigem Kontakt zur Leitungsebene (insbesondere leitende Juristinnen und Juristen sowie diakonische Vorstände) und zur operativen Ebene (insbesondere Datenschutzreferentinnen und Datenschutzreferenten, Finanzreferentinnen und Finanzreferenten sowie IT-Referentinnen und IT-Referenten) der Landeskirchen und diakonischen Landesverbände. Seit 2018 werden in jeder Datenschutzregion jährliche Treffen mit den Datenschutzreferentinnen und Datenschutzreferenten organisiert. Diese Treffen dienen dem fachlichen Austausch und wurden im Berichtszeitraum überwiegend online durchgeführt. In den Jahren 2023 und 2024 nutzte der BfD EKD diese Treffen, um sich mit den Datenschutzreferentinnen und Datenschutzreferenten über das Thema Künstliche Intelligenz auszutauschen sowie über die Evaluation des EKD-Datenschutzgesetzes und das vom BfD EKD initiierte Programm „Zukunftsstrategie des BfD EKD“ zu informieren. Im Zusammenhang mit seinem aufsichtlichen Handeln informierte der BfD EKD über den Stand der Schwerpunktprüfung in evangelischen Krankenhäusern sowie

über aktuelle Klagen gegen den BfD EKD.

Der BfD EKD stand im Berichtszeitraum auch in Erfüllung des gesetzlichen Auftrags zur Zusammenarbeit in regelmäßigem Kontakt zu den anderen Beauftragten für den Datenschutz innerhalb der EKD. Einmal im Jahr wurde zu Fragen des kirchlichen Datenschutzes die Tagung der Konferenz der Beauftragten für den Datenschutz in der EKD unter Vorsitz des BfD EKD durchgeführt. Im Jahr 2023 hat die Konferenz in Essen und im Jahr 2024 in Erfurt stattgefunden.

Darüber hinaus ist der BfD EKD in mehreren Gremien, Konferenzen und (temporären) Arbeitsgruppen der EKD (als Gast) vertreten (z. B. Synode der EKD (mit Gaststatus), Sitzung der leitenden Juristinnen und Juristen in den zentralen Verwaltungen der Gliedkirchen der EKD, Referentenkonferenz für Datenschutz, IT-Referentenkonferenz der EKD und andere). Zudem trägt der BfD EKD seine Anliegen nach Bedarf eigenständig dem Rat der EKD, gegebenenfalls auch der Kirchenkonferenz, dem Finanzbeirat der EKD und dem Haushaltsausschuss der Synode der EKD vor.

Zur römisch-katholischen Kirche

Der BfD EKD steht in regelmäßigem Kontakt zu den Diözesandatenschutzbeauftragten in der römisch-katholischen Kirche. Neben persönlichen Gesprächen trafen sich im Berichtszeitraum die Konferenz der Beauftragten für den Datenschutz in der EKD und die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands einmal im Jahr zum Ökumenischen Datenschutztag. Die Organisation erfolgt abwechselnd durch die römisch-katholische und die evangelische Seite. Im Berichtszeitraum lag ein Schwerpunkt der Zusammenarbeit auf dem erfolgreichen Abschluss des gemeinsamen ökumenischen Projekts Kirchliches Datenschutzmodell. Auf einer abschließenden Sondersitzung zum Ende des Berichtszeitraums wurde die Ergänzung des KDM mit neuen Beispielen und die Übernahme des sogenannten Datenschutzwürfels aus dem SDM beschlossen. Die Weiterentwicklung des Modells und die Rezeption künftiger SDM-Versionen wird seitdem durch die neue Arbeitsgemeinschaft „KDM Werkstatt“ sichergestellt.

Zu Bund und Ländern

Der BfD EKD stand auch in diesem Berichtszeitraum in regelmäßigem Kontakt zum Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und seiner Behörde. Dieser Kontakt soll weiterhin auch zur neuen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ökumenisch, intensiv fortgeführt werden. Zudem pflegt der BfD EKD direkte Kontakte zu den Landesbeauftragten für den Datenschutz und die Informationsfreiheit und zu deren Behörden.

Daneben nimmt der BfD EKD am regelmäßigen Austausch der Datenschutzkonferenz des Bundes und der Länder mit den spezifischen Aufsichtsbehörden teil. Zudem ist der BfD EKD zwischenzeitlich Mitglied in den folgenden acht Arbeitskreisen der Datenschutzkonferenz:

- Arbeitskreis Grundsatz
- Arbeitskreis Technik (inkl. Mitwirkung in der Unterarbeitsgruppe Standard-Datenschutzmodell)
- Arbeitskreis Beschäftigtendatenschutz
- Arbeitskreis Gesundheit und Soziales
- Arbeitskreis Schulen und Bildungseinrichtungen
- Arbeitskreis Zertifizierung
- Arbeitskreis Medienkompetenz
- Arbeitskreis Künstliche Intelligenz

Eine konkrete Mitwirkung in der Datenschutzkonferenz selbst konnte bislang nicht erreicht werden.

Zu sonstigen Akteuren

Darüber hinaus steht der BfD EKD mit Akteuren im Bereich Datenschutz und IT-Sicherheit im Umfeld von Politik, Gesellschaft und Wissenschaft (z. B. Stiftung Datenschutz) in gutem Kontakt. Auch zu den eigenständigen Datenschutzaufsichten im Bereich der öffentlich-rechtlichen Rundfunk- und Fernsehanstalten werden regelmäßige Kontakte gepflegt. Der BfD EKD ist außerdem Mitglied in mehreren Interessenvertretungen im Bereich Datenschutz und IT (z. B. Gesellschaft für Datenschutz und Datensicherheit (GDD) e. V., Gesellschaft für Informatik (GI) e. V., Allianz für Cybersicherheit und Virtuelles Datenschutzbüro).



Über die Themen bei Aufsicht und Beratung

Die Themen bei Aufsicht und Beratung sind vielfältig! In Erfüllung des gesetzlichen Auftrags wacht der BfD EKD über die Einhaltung des Datenschutzes. Dabei will er vor allem beraten und unterstützen. Zu den Aufgaben des BfD EKD gehört aber auch, die Einhaltung des Datenschutzes zu kontrollieren und zu überwachen. Über allem Handeln steht dabei der Zweck jedes modernen Datenschutzes. Jede einzelne Person ist davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird. In diesem Kapitel wird umfassend über die Themen bei Aufsicht und Beratung informiert.

Datenverarbeitung und Auskunftsrecht

Viele kirchliche und diakonische Einrichtungen stehen bei der Datenverarbeitung und bei der Erfüllung von Auskunftsrechten vor Herausforderungen. Der BfD EKD beschäftigte sich im Berichtszeitraum mit diesem Themenkomplex sowohl im Rahmen von Datenschutzbeschwerden und Datenpannenmeldungen als auch im Zusammenhang mit verschiedenen Beratungsanfragen.

Freiwilligkeit einer Einwilligungserklärung

Oftmals werden in Kindertageseinrichtungen vorformulierte Einwilligungserklärungen zur Anfertigung und Veröffentlichung von Fotos der Kinder verwendet und im Zuge des Abschlusses des Betreuungsvertrages von den Erziehungsberechtigten unterzeichnet.

In den Formularen wird in der Regel bereits angegeben, dass der Widerruf jederzeit möglich ist und die Nichterteilung der Einwilligung zu keinem Nachteil für das Kind führen wird. In der Praxis wird jedoch gerade dieser Aspekt der Freiwilligkeit nicht richtig umgesetzt. So erreichen uns Mitteilungen von Erziehungsberechtigten, dass die Kinder – sofern in die Anfertigung von Fotos nicht eingewilligt wird – nicht an Aktionen oder Ausflügen teilnehmen dürfen. Dies wird von den Kindertageseinrichtungen mit der Einhaltung des Datenschutzes begründet. Nicht nur, dass die Nichtteilnahme des Kindes an einer Aktion einen erheblichen Nachteil für das Kind darstellt und damit die Freiwilligkeit zur Unterzeichnung der Einwilligungserklärung deutlich in Frage stellt. Diese Vorgehensweise widerspricht zudem dem Grundsatz der Verhältnismäßigkeit. Wenn es Kindertageseinrichtungen nicht möglich ist, darauf zu achten, dass bestimmte Kinder nicht fotografiert oder im Nachhinein auf den Fotos unkenntlich gemacht werden, so wäre es naheliegend, von einer Anfertigung der Bilder abzusehen, nicht jedoch dem Kind die Teilnahme an dem Ausflug oder der Aktion zu verwehren.

Fazit: Eine Einwilligung kann nicht wirksam erteilt werden, wenn diese unter eine Bedingung gestellt wird oder das Nichtunterzeichnen einen Nachteil mit sich bringt.

Bearbeitung eines Auskunftsanspruchs

Bei der Bearbeitung eines Auskunftsanspruchs stellt sich der verantwortlichen Stelle häufig die Frage, wie detailliert die Auskunft erteilt werden muss. Müssen nur die Datenkategorien aufgeführt werden, die verarbeitet wurden? Oder muss genau mitgeteilt werden, welche konkreten personenbezogenen Daten verarbeitet wurden?

Diese Fragen waren Teil eines Beschwerdeverfahrens, das der BfD EKD im Berichtszeitraum zu bearbeiten hatte. In diesem Beschwerdeverfahren beanstandete der BfD EKD letztendlich einen Datenschutzverstoß gegen § 19 Abs. 1 DSGVO-EKD.

Mit Urteil vom 4. Mai 2023 (Az.: C-487/21) hatte sich der Europäische Gerichtshof (EuGH) in Bezug auf Umfang und Inhalt einer datenschutzrechtlichen Auskunft geäußert. Das Recht, eine „Kopie“ der personenbezogenen Daten nach Art. 15 DSGVO zu erhalten, bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion oder Abschrift aller dieser Daten ausgehändigt werden muss. Die Auskunft muss aber nicht zwingend in Form einer „Fotokopie“ erteilt werden. Die Kopie muss alle personenbezogenen Daten umfassen, die verarbeitet werden. Mit den mitgeteilten Daten muss es der anfragenden Person möglich sein, die Richtigkeit ihrer personenbezogenen Daten zu überprüfen, um gegebenenfalls weitere Betroffenenrechte geltend zu machen. Es besteht die Pflicht des Verantwortlichen, der betroffenen Person alle Informationen in transparenter und leicht verständlicher und zugänglicher Sprache zu übermitteln.

Die in diesem Urteil aufgestellten Grundsätze zu Art. 15 DSGVO sollten bereits im Berichtszeitraum entsprechend auf § 19 Abs. 1 DSGVO-EKD angewendet werden. Eine Auskunft nach § 19 DSGVO-EKD sollte daher eine originalgetreue und verständliche Reproduktion oder Abschrift der Daten der betroffenen Person enthalten, auch wenn das Recht auf Kopie bisher nicht explizit in § 19 DSGVO-EKD geregelt war. Die Auskunft sollte demnach auch alle personenbezogenen Daten umfassen, die verarbeitet werden.

Beachte: Im evaluierten EKD-Datenschutzgesetz, das zum 1. Mai 2025 in Kraft getreten ist, wurde das Recht auf Kopie in § 19 Abs. 4 DSGVO-EKD (neu) aufgenommen.

Kommunikation mit Betroffenen von sexualisierter Gewalt

Im Berichtszeitraum erreichte den BfD EKD eine Beschwerde, die die schriftliche Kommunikation der Fachstelle Prävention, Intervention und Aufarbeitung sexualisierter Gewalt einer Landeskirche mit einer betroffenen Person zum Inhalt hatte.

Durch eine problematische Faltung des Anschreibens der Fachstelle an die betroffene Person und Versendung in einem Sichtfensterumschlag waren Teile der Betreffzeile schon durch das Sichtfenster erkennbar. Im Zusammenspiel mit dem aufgebrachten Absenderstempel, der nicht allgemein gehalten war, sondern explizit die Fachstelle aufführte, ließ dies Rückschlüsse auf den Inhalt des Briefes zu. Dies stellt eine unberechtigte Offenlegung personenbezogener Daten dar. Es ist anzuraten, angesichts der Sensibilität der Thematik besondere Sorgfalt auf die Kommunikationswege zu verwenden. Insbesondere sollte geprüft werden, ob die Nennung der Fachstelle in den Absenderangaben tatsächlich erforderlich ist. Vielfach dürfte die Angabe der übergeordneten Organisationseinheit, also im Regelfall der Landeskirche bzw. des Landeskirchenamts, ausreichen. Besondere Sorgfalt ist bei der Verwendung von Sichtfensterumschlägen erforderlich: Hier sollte der sichtbare Teil der kuvertierten Sendung nochmals sorgfältig geprüft werden, bevor sie aufgegeben wird. Es kann sich auch anbieten, von vornherein auf Sichtfensterumschläge zur Risikominimierung zu verzichten.

Fazit: Wenden sich Betroffene an solche Fachstellen, ist ein besonderes Maß an Sensibilität erforderlich, um die Vertraulichkeit zu schaffen, die der Umgang mit dem Thema voraussetzt.

Ungewollte Berechtigungsänderung

Im Berichtszeitraum erreichte uns, wie schon häufiger, eine Datenpannenmeldung wegen zu weit gehender Berechtigungen auf einem Ordner im Filesystem des Betriebssystems Windows.

Mehrere Personen einer verantwortlichen Stelle hatten in unzulässiger Weise die Berechtigung zum Lesen und Ändern von Dateien, die personenbezogene Daten enthielten. Durch das Verschieben von Dateien können

sich unbeabsichtigte Seiteneffekte ergeben. Bei dieser Handhabung gehen die ursprünglichen Zugriffsberechtigungen verloren und es greifen die Dateiberechtigungen aus dem Zielordner, in den die Dateien verschoben wurden, da in der Regel mit Vererbung bei den Dateiberechtigungen gearbeitet wird.

Es gilt also: Beim Verschieben von Dateien muss sorgsam auf die Zugriffsberechtigungen geachtet werden. Dies kann in der Regel bei den Eigenschaften der Dateien über die Registerlasche „Sicherheit“ überprüft werden. Unterschiedliche Einstellungen, ob mit oder ohne Vererbung von Dateizugriffsberechtigungen gearbeitet wird, können beim Verschieben von Dateien zu ungewollten Zugriffsberechtigungen führen.

Fazit: Beim Verschieben von Dateien müssen die Zugriffsberechtigungen überprüft werden.

Scannen von Dokumenten

Immer wieder erreichen den BfD EKD Datenpannenmeldungen im Zusammenhang mit dem Scannen von Dokumenten. In der Praxis ist es üblich, dass Papierdokumente mit einem Multifunktionsgerät digitalisiert und die erstellten Dateien mit automatisch erzeugten Dateinamen in einem festgelegten Verzeichnis im internen Netzwerk abgelegt werden oder per E-Mail an eine ausgewählte E-Mail-Adresse gesendet werden. Als problematisch erweist sich hier vor allem der automatisch erzeugte Dateiname, aus dem kein Bezug zum Inhalt des jeweiligen Dokumentes herstellbar ist. Eine weitere Problematik ergibt sich, wenn das Ablageverzeichnis mit Zugriffsberechtigungen für mehrere Personen ausgestattet ist. Im Berichtszeitraum kam es mehrfach vor, dass eingescannte Dateien aus dem Scan-Verzeichnis oder aus der Mailbox falsch ausgewählt wurden, um sie an Dritte zu versenden. Darunter befanden sich auch sensible Informationen wie z. B. zu Arbeitsverhältnissen oder Patientenunterlagen. Der BfD EKD gab Hinweise zur Verbesserung der jeweiligen Scanprozesse.

Die Ablage von gescannten Dateien sollte so konfiguriert sein, dass Beschäftigte nur auf ihre eigenen Scan-Ergebnisse Zugriff erhalten können. In Handlungsanweisungen sollten Schritte zur sinnhaften Umbenennung von Scan-Ergebnissen und dem Einsor-

tieren der umbenannten Dateien in die zugehörigen digitalen Akten oder thematischen Verzeichnisse sowie das anschließende Löschen der ursprünglichen Scans aus den Mailboxen und Scan-Verzeichnissen festgelegt werden. Die Mitarbeitenden sind regelmäßig zu sensibilisieren, dass sie die Anhänge beim E-Mail-Versand sorgfältig auf ihre Richtigkeit überprüfen.

Erstellung einer Datenschutz-Folgenabschätzung mithilfe des KDM

Die Datenschutz-Folgenabschätzung (DSFA) stellt ein Verfahren zur risikobasierten datenschutzrechtlichen Bewertung von risikobehafteten geplanten Verarbeitungen im Rahmen der Rechenschaftspflicht gemäß § 5 Abs. 2 DSGVO dar und ergänzt die in jedem Fall bestehende Pflicht gemäß § 27 DSGVO, geeignete technische und organisatorische Maßnahmen (TOMs) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Vorgehensweise beruht darauf, dass auf der Grundlage der Verarbeitungstätigkeiten Risiken für die Rechte und Freiheiten bewertet werden und ein angemessenes Schutzniveau ermittelt wird. Um die erkannten Risiken auf ein vertretbares Maß zu reduzieren und hierdurch das angemessene Schutzniveau sicherzustellen, müssen konkret nachzuweisende Schutzmaßnahmen ergriffen werden.

An dieser Stelle hilft das KDM bei der konkreten Umsetzung, indem für die jeweiligen Prüfschritte Bausteine das konkrete Vorgehen beschreiben. Bei der Darstellung der Verarbeitung helfen die Bausteine 41 (Planen und Spezifizieren) und 42 (Dokumentieren), die die Ausführungen im KDM unter D2.3 Komponenten einer Verarbeitung bzw. Verarbeitungstätigkeit in Form ergänzender Anleitungen mit Checklisten konkretisieren. In gleicher Weise wird für die unter Risikobeurteilung zu D3 Risiken und Schutzbedarf beschriebenen Anforderungen mit der Anlage zum KDM ‚Richtlinie zur Risikoanalyse‘ ein hilfreiches Werkzeug an die Hand gegeben. Auf der Grundlage der zuvor dargestellten Verarbeitung und der erkannten Risiken können zur praktischen Umsetzung aus dem unter D1 Generische Maßnahmen dargestellten Katalog generische, technische und organisatorische Maßnahmen abgeleitet und zur Gewährleistung des angemessenen Schutzniveaus verwendet werden. Im Übrigen führt

der Baustein 41 vor Augen, dass das mindestens zweimalige Durchlaufen des PDCA-Zyklus bei einer DSFA charakteristisch für den Aufbau eines wirksamen Datenschutzmanagementsystems ist.

Fazit: Das KDM kann helfen, eine DSFA strukturiert zu erstellen.

Fragen im gemeindlichen Alltag

Als eigenständige verantwortliche Stellen sind Kirchengemeinden dazu verpflichtet, den Datenschutz einzuhalten und umzusetzen. Insbesondere durch gesetzliche Änderungen und veränderte Rahmenbedingungen haben sich in der praktischen Arbeit immer wieder spezielle datenschutzrechtliche Fragestellungen ergeben.

Private E-Mail-Adressen in der Seelsorge

Zu den Kernaufgaben von Pfarrpersonen gehört die Seelsorge. Seelsorge findet in der Regel in einem geschützten Rahmen statt. Aber auch hierbei gibt es immer mehr Kommunikation über E-Mails. Beim Einsatz von E-Mails in der Seelsorge müssen Besonderheiten der vertraulichen Kommunikation und des Datenschutzes angemessen berücksichtigt werden.

In einem Aufsichtsfall musste – im Spannungsfeld der zeitgemäßen niederschweligen Kontaktaufnahmemöglichkeiten mit einer E-Mail – die Nutzung des privaten Freemailers durch einen Pfarrer datenschutzrechtlich bewertet werden, weil der Pfarrer seine dienstlich-personalisierte E-Mail-Adresse nicht nutzte. Trotz Nachfrage und Hilfestellungen konnte der Pfarrer den Nachweis der datenschutzkonformen Nutzung der E-Mail-Adresse des Freemailers nicht führen. Es lag weder ein Vertrag über die Verarbeitung personenbezogener Daten im Auftrag vor. Aber auch ein angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten durch die Dokumentation geeigneter technischer und organisatorischer Maßnahmen auf der Grundlage einer zuvor durchgeführten DSFA konnte nicht nachgewiesen werden.

Aufgrund der fehlenden Nachweise war zu befürchten, dass die personenbezogenen Daten der Seelsorgesu-

chenden nicht ausreichend vor dem unberechtigten Zugriff Dritter geschützt waren und damit neben dem Datenschutz auch das Seelsorgegeheimnis verletzt wurde. Die datenschutzwidrige Nutzung der E-Mail-Adresse des Freemailers wurde dem Pfarrer durch Anordnung bis zum Nachweis einer datenschutzkonformen Nutzung untersagt.

Fazit: Die dienstlich zur Verfügung gestellten E-Mail-Adressen sind stets zu nutzen.

Streaming von Gottesdiensten

Während der Corona-Pandemie wurden Gottesdienste vermehrt im Internet gestreamt, um auch Menschen zu erreichen, die den Gottesdienst nicht besuchen konnten. Auch nach der Corona-Pandemie hat sich in vielen Kirchengemeinden etabliert, weiterhin solche Angebote vorzuhalten, um einem größeren Personenkreis die Teilnahme an den Gottesdiensten zu ermöglichen. § 53 DSGVO bietet dafür die einschlägige datenschutzrechtliche Grundlage. Allerdings ist darauf zu achten, dass die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden müssen. Den BfD EKD erreichten im Berichtszeitraum Beschwerden, in denen die Veröffentlichung von Gottesdienstvideos auf YouTube kritisiert wurde, weil eine ausreichende Information der Gottesdienstteilnehmenden nicht erfolgt sei.

Eine betroffene Kirchengemeinde erläuterte auf Nachfrage, dass entsprechende Hinweisschilder zur Videoaufzeichnung angebracht worden seien und nur der Altarraum und die handelnden Akteure gefilmt würden.

Bei Prüfung der veröffentlichten Videos konnte allerdings festgestellt werden, dass in einigen Videos auch andere Personen erkennbar gefilmt wurden, z. B. Konfirmandinnen und Konfirmanden und Mitglieder der Kirchengemeinde im Rahmen spezieller Projekte. Sofern die Gottesdienstteilnehmenden jedoch auf einem Video zu erkennen sind, müssen neben § 53 DSGVO noch weitere Rechtsgrundlagen für die Veröffentlichung geprüft werden. Hier käme als Rechtsgrundlage eine Einwilligung der betroffenen Personen in Betracht. Entsprechende Einwilligungen konnten seitens der Kirchengemeinde nicht vorgelegt werden. In einem Beratungsgespräch vor Ort wurden die datenschutz-

rechtlichen Rahmenbedingungen erläutert, vor allem hinsichtlich der Einhaltung der allgemeinen Datenschutzgrundsätze nach § 5 DSGVO und zum Erfordernis einer Rechtsgrundlage sowie zur Auftragsverarbeitung und Datenübermittlung in ein Drittland.

Fazit: Als mögliche Alternative zu digital abgespeicherten Gottesdiensten in einem Videoportal kann eine Echtzeitübertragung mit einem Videokonferenztool in Betracht gezogen werden.

Geburtstagsgratulation im Gemeindebrief

Auch in diesem Berichtszeitraum erreichten den BfD EKD wieder Beschwerden über Veröffentlichungen in Gemeindebriefen. Eine der Beschwerden betraf die Veröffentlichung eines Glückwunsches zu einem runden Geburtstag.

Gemeindebriefe bilden das Gemeindeleben ab. Sie informieren über Neuigkeiten, anstehende Termine und veröffentlichen Amtshandlungen, wie Taufen, Konfirmationen, Trauungen und Bestattungen. Einige Landeskirchen haben eigene Rechtsgrundlagen für die Veröffentlichung bestimmter weiterer Inhalte geschaffen: So dürfen vielfach Alters- und Ehejubiläen von Gemeindegliedern in Gemeindebriefen mit Namen, Tag und Ort des Ereignisses veröffentlicht werden, soweit auf das Widerspruchsrecht hingewiesen wurde, ein Widerspruch jedoch nicht vorliegt.

Ist hingegen keine eigene landeskirchliche Rechtsgrundlage vorhanden, richtet sich die Zulässigkeit der Veröffentlichung von Geburtstagswünschen und somit die Offenlegung des Namens und des Geburtsdatums nach § 9 Abs. 1 Nr. 3 DSGVO. Danach ist die Offenlegung von personenbezogenen Daten an sonstige Stellen oder Personen zulässig, wenn die Empfänger ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft darlegen und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Offenlegung hat. Da das Interesse des Einzelnen am Schutz seiner personenbezogenen Daten höher zu gewichten ist als das Interesse der übrigen Gemeindeglieder an der Kenntnis dieses Geburtstags, kann die Offenlegung dieser personenbezogenen Daten im Gemeindebrief nicht auf § 9 Abs. 1 Nr. 3 DSGVO gestützt werden. In diesen Fällen muss vor Veröffentlichung stets eine Einwilligung eingeholt werden.

Beachte: Im evaluierten Datenschutzgesetz wurde in § 50b Abs. 2 DSGVO (neu) eine entsprechende Rechtsgrundlage geschaffen.

Online-Wahlen in Kirchengemeinden

In regelmäßigen Abständen finden in Kirchengemeinden Wahlen zur Besetzung des gemeindlichen Leitungsorgans statt.

Dabei fällt es den Kirchengemeinden immer schwerer, die Wahlberechtigten zur Teilnahme an den Wahlen zu motivieren. Traditionell werden die wahlberechtigten Gemeindeglieder per Brief benachrichtigt und die Wahl wird an einem einheitlich festgelegten Sonntag mit Wählerverzeichnis, Stimmzetteln und Wahlurne durchgeführt. Eine Briefwahl ist auch möglich.

Seit mehreren Jahren gehen einige Landeskirchen bei diesen Wahlen einen neuen Weg, der im Mittelpunkt mehrerer Beratungsanfragen von örtlich Beauftragten für den Datenschutz an den BfD EKD stand.

Dabei wird den Kirchengemeinden als zusätzliche oder alternative Option die Durchführung der Wahl per Online-Abstimmung angeboten. Hinter der Online-Wahl stehen unterschiedliche Anbieter, die solche Wahlen und Abstimmungen auch bereits für andere öffentliche und private Einrichtungen durchgeführt haben. Mit diesem Anbieter schließt die jeweilige Landeskirche einen Dienstleistungs- und Auftragsverarbeitungsvertrag.

Solche Online-Wahlen sind nach Bewertung des BfD EKD datenschutzkonform erfolgt. Ausschlaggebend dafür ist – neben der Erfahrung des Anbieters der Online-Plattform – die intensive und detaillierte Planung und Vorbereitung in den Landeskirchen durch entsprechende Arbeitsgruppen mit Mitarbeitenden aus den Bereichen IT und Meldewesen. Wichtig ist aus Sicht des BfD EKD die Wahrung des Wahlgeheimnisses (z. B. durch Pseudonymisierung der Wählerinnen und Wähler gegenüber dem Dienstleister) und die Sicherstellung der Einmaligkeit der Stimmabgabe (z. B. durch wirkungsvolle Synchronisierung des Online-Stimmabgabevermerks mit dem Wählerverzeichnis). Auch sollte immer für die Wählerinnen und Wähler neben der Online-Stimmabgabe mindestens eine klassische Option – Präsenz- oder Briefwahl – verbleiben.

Besonderheiten im diakonischen Bereich

Diakonische Einrichtungen verarbeiten häufig Gesundheitsdaten und somit besondere Kategorien personenbezogener Daten. Auch sind sie bei der Erfüllung ihrer Aufgaben immer öfter auf die Zusammenarbeit mit anderen Einrichtungen angewiesen. Daraus ergeben sich in der Praxis immer wieder bereichsspezifische Datenschutzfragen.

Versendung von Entlassberichten trotz fehlender Einwilligung

Mehrfach wurden Datenschutzverletzungen in Einrichtungen des Gesundheitswesens festgestellt, die im Kern darin bestanden, dass eine unberechtigte Offenlegung von Gesundheitsdaten erfolgte, indem entgegen dem Willen der Patienten sogenannte Entlassberichte oder Arztbriefe z. B. an den Hausarzt oder andere medizinische Stellen versendet wurden.

Im Zuge der Digitalisierung setzen Krankenhäuser überwiegend Krankenhaus-Informationssysteme (KIS) ein, in denen auch der Behandlungsvertrag und die in der Regel gleichzeitig eingeholten Einwilligungen der Patienten abgelegt sind. Eine typische Einwilligung wird für die Übermittlung von Entlassberichten an die ärztliche Nachversorgung abgefragt. Die Erteilung oder Verweigerung der Einwilligung wird elektronisch vermerkt. Der Vermerk im KIS ist für alle Berechtigten sichtbar, hat aber meistens keine technisch steuernde Konsequenz.

In den gemeldeten Datenschutzverletzungen wurde vorgetragen, dass die Ursache in menschlichem Versagen oder dem bewussten oder unbewussten Ignorieren von Dienstanweisungen läge, indem der im KIS hinterlegte Vermerk nicht beachtet wurde.

Auch bei sonstigen aufsichtlichen Tätigkeiten in Krankenhäusern wurde immer wieder festgestellt, dass die gängigen KIS in den Grundeinstellungen keine technischen Funktionen enthalten, die bei fehlender Einwilligung eine Druckausgabe verhindern. Es wird häufig systemseitig nicht verhindert, dass ein Entlassbericht erstellt und gedruckt wird, obwohl keine Einwilligung vorliegt oder sogar ein Widerruf der Einwilligung erfasst wurde. Es hängt alleine an

organisatorischen Maßnahmen (z. B. Anweisungen) und der Aufmerksamkeit der Mitarbeitenden, ob es in solchen Fällen zu Datenschutzverstößen kommt.

Fazit: Beim Einsatz eines KIS wird empfohlen, vom Hersteller eine Weiterentwicklung einzufordern, mit der solche Datenübermittlungen ohne Rechtsgrundlage wirksam technisch unterbunden werden können.

Exkurs: Schwerpunktprüfung in evangelischen Krankenhäusern

In Erfüllung der Aufgabe einer Datenschutzaufsichtsbehörde und der Vorgaben des Europäischen Gerichtshofs führte der BfD EKD auch in diesem Berichtszeitraum eine Schwerpunktprüfung durch. Eine Schwerpunktprüfung ist eine anlasslose Prüfung in einem kirchlichen oder diakonischen Tätigkeitsfeld mit dem Ziel der kontinuierlichen Verbesserung in den geprüften Einrichtungen.

In diesem Berichtszeitraum hat der BfD EKD evangelische Krankenhäuser geprüft. Dabei wurden 20 evangelische Krankenhäuser nach dem Zufallsprinzip für die Durchführung der Schwerpunktprüfung ausgewählt. Auch diese zweite Schwerpunktprüfung wurde mithilfe eines online-basierten Fragebogens durchgeführt. Zusätzlich sollten ausgewählte Dokumente hochgeladen werden. Der Fragebogen enthielt neben den Fragen zum organisatorischen und rechtlichen Umfeld auch technische Fragen. Dabei stand das KIS besonders im Fokus. Konkret hat der BfD EKD nach dem Rollen- und Berechtigungskonzept sowie der Protokollierung gefragt. Auch die Löschung von Daten spielte eine Rolle. Planmäßig fanden einige Vor-Ort-Prüfungen statt, um auch einen Einblick in die Praxis zu bekommen. Am Ende der Prüfung bekam jedes geprüfte Krankenhaus ein individuelles Abschluss schreiben. Diese Schreiben zeigten die Ergebnisse der Prüfung sowie die erkennbar gewordenen Mängel auf und gaben den Krankenhäusern konkret umzusetzende Anforderungen und Empfehlungen an die Hand. In diesem Zusammenhang wurde eine Beanstandung ausgesprochen. Die Schwerpunktprüfung konnte insgesamt im Frühjahr 2025 abgeschlossen werden. Der BfD EKD veröffentlichte auch nach dieser Schwerpunktprüfung einen Abschlussbericht und den verwendeten Fragebogen auf seiner Homepage.

Erwartungsgemäß erfüllen alle Krankenhäuser die grundsätzlichen Anforderungen an den Datenschutz. So ist die Bestellung von örtlich Beauftragten für den Datenschutz flächendeckend gegeben. Die gesetzlich vorgeschriebene Vertretung hingegen ist nicht überall geregelt. Der Prozess beim Umgang mit Datenpannen sollte in einigen Krankenhäusern noch optimiert werden, insbesondere die interne Dokumentation wird noch nicht überall zufriedenstellend geführt. Nur wenige der geprüften Krankenhäuser verfügten über ein vollständiges Löschkonzept, das auch in der Praxis umgesetzt werden kann.

Patienteninformationen werden überwiegend im KIS erfasst. Das gilt oft auch für die einzuholenden Einwilligungen. Dabei wird das Risiko minimiert, dass Daten ohne die erforderliche Rechtsgrundlage verarbeitet werden und es wird sichergestellt, dass auch erfolgte Widerrufe erfasst und umgesetzt werden können. Dort, wo diese Erklärungen noch in Papier unabhängig von der Patientenakte abgelegt werden, wurde empfohlen, diese Daten im KIS zusammenzuführen. Teilweise war dieser Schritt auch bereits in Planung. Insgesamt macht sich aber der hohe Grad der Digitalisierung positiv bemerkbar und ist hilfreich bei der Erfüllung der Rechenschaftspflichten.

Alle KIS bieten die Möglichkeit, Berechtigungen – entsprechend der fachlichen Aufgaben und der strukturellen Zuordnung der Anwendenden – zu Abteilungen und Stationen zu vergeben. Dabei werden Berechtigungsvergaben gut dokumentiert. Eine Herausforderung bleibt aber der Umgang mit temporären Vertretungen oder Sondersituationen, in denen zusätzliche Berechtigungen vorübergehend und revisions sicher zugewiesen werden müssen.

Die nächste Schwerpunktprüfung im Zeitraum 2025/2026 findet im Bereich der kirchlichen Verwaltung mit einem Schwerpunkt Umgang mit Meldedaten statt.

Zweckentfremdung von Patientendaten

Mehrere Krankenhäuser eines großen diakonischen Trägers haben im Berichtszeitraum ähnliche Datenpannen an den BfD EKD gemeldet. Danach hatte ein Beschäftigter der Trägergesellschaft ein zentrales

Patientenanschriften im Namen der Krankenhäuser angestoßen und hierfür Daten aus dem bestehenden Konzerncontrolling verwendet.

Für den Träger als Konzernzentrale und Muttergesellschaft diverser Gesundheitseinrichtungen existiert für einen begrenzten Personenkreis im Rahmen des Konzerncontrollings Zugriff auf die Daten der Patientinnen und Patienten der Krankenhäuser. Aus datenschutzrechtlicher Sicht besteht allerdings keine Rechtsgrundlage für die Verwendung der Patientendaten durch den Träger zu einem anderen Zweck als dem Konzerncontrolling. Der Sachverhalt wurde mit dem Träger intensiv aufgearbeitet. Es war zwar ein datenschutzkonformer Prozess für Patientenanschriften vorgegeben, dieser konnte aber mangels geeigneter technischer Maßnahmen umgangen werden. Die Datenschutzverletzung erfolgte aufgrund der Nichteinhaltung der festgelegten Prozesse sowie durch individuelles menschliches Versagen. Durch Änderungen im Berechtigungskonzept und in den Prozessabläufen beim Konzerncontrolling sollen derartige Datenschutzverletzungen in Zukunft unterbunden werden.

Zusendung von Informationsmaterial

In einem Beschwerdefall wurde einem Petenten mehrfach sogenannte Dialogpost von einer diakonischen Einrichtung zugesendet. Die diakonische Einrichtung versendete in regelmäßigen Abständen Dialogpost mit Veranstaltungsangeboten und Spendenbriefe an Personen, die in der Vergangenheit persönlichen Kontakt zur Einrichtung hatten.

Über die Nutzung der personenbezogenen Daten zu diesem Zweck wurden die betroffenen Personen im Vorfeld informiert. Betroffene Personen wurden außerdem darauf hingewiesen, dass sie der Verarbeitung ihrer personenbezogenen Daten nach § 25 Abs. 1 DSGVO-EKD widersprechen können. Sofern eine Person der Verwendung ihrer Daten widersprochen hat, muss dieser Widerspruch gut dokumentiert werden. In dem Beschwerdefall widersprach der Petent der weiteren Nutzung seiner Daten zu Werbezwecken bereits nach der ersten Dialogpost. Da die Einrichtung ihm trotz des Widerspruchs weiterhin Dialogpost zusendete, wurde ein Verstoß gegen die Vorschriften des EKD-Datenschutzgesetzes festgestellt.

Darüber hinaus stellt sich in solchen Fällen häufig auch die Frage nach der richtigen Rechtsgrundlage der Datenverarbeitung der personenbezogenen Daten. Insoweit hat sich die Einrichtung auf das berechtigte Interesse nach § 6 Nr. 8, 4 DSGVO-EKD berufen. Wenn Einrichtungen die Verarbeitung von personenbezogenen Daten auf das Vorliegen eines berechtigten Interesses stützen, müssen sie im Vorfeld eine Interessenabwägung zwischen den berechtigten Interessen der Einrichtung und den schutzwürdigen Interessen der betroffenen Personen durchführen. Diese Interessenabwägungen müssen schriftlich dokumentiert werden und es sollten insbesondere die Interessen der betroffenen Personen nicht zu kurz behandelt werden. Die Aufsichtsbehörde kann diese Dokumentation einer Interessenabwägung im Fall einer Beschwerde anfordern, um das Vorliegen der Voraussetzungen der Rechtsgrundlage zu prüfen.

Schnittstelle Schulsozialarbeit

Schulsozialarbeit ist eine wichtige Schnittstelle zwischen Schule, Familie und dem sozialen Umfeld der Schülerinnen und Schüler. Sie verfolgt das Ziel, Kinder und Jugendliche in ihrer persönlichen Entwicklung zu unterstützen, soziale Kompetenzen zu fördern und bei der Bewältigung von Herausforderungen in Schule und Alltag zu helfen. Durch ihre Arbeit tragen Mitarbeitende in der Schulsozialarbeit dazu bei, das Lernklima zu verbessern und Chancengleichheit zu fördern.

Dabei sind sie in die schulische Organisation eingebunden, jedoch rechtlich und organisatorisch unabhängig, da ihre Tätigkeit oft durch freie Träger – z. B. eine diakonische Einrichtung – erbracht wird. Der Einsatz freier Träger hat dabei den Vorteil, dass Schulsozialarbeit unabhängig von den Weisungen der Schulleitungen agieren kann. Dies ermöglicht eine vertrauensvolle Beratungssituation.

Mitarbeitende in der Schulsozialarbeit unterliegen dem Berufsgeheimnis gemäß § 203 Strafgesetzbuch, das die Offenlegung persönlicher Daten ohne ausdrückliche Befugnis untersagt. Diese Schweigepflicht ist ein zentraler Baustein der Arbeit und schützt die Persönlichkeitsrechte der Schülerinnen und Schüler.

Grundsätzlich erfolgt die Verarbeitung personenbezogener Daten im Rahmen der Schulsozialarbeit auf Basis

einer freiwilligen Einwilligung der Schülerinnen und Schüler oder ihrer Personensorgeberechtigten. Diese Einwilligung muss informiert und nachweisbar sein. Die erhobenen Daten sind dabei streng zweckgebunden und dürfen nur für die vereinbarten Aufgaben verwendet werden. Eine Weitergabe an Schulleitungen oder Lehrkräfte ist nur mit ausdrücklicher Einwilligung der Betroffenen möglich. Dies unterstreicht die unabhängige Rolle der Schulsozialarbeit. In Ausnahmefällen können Mitarbeitende in der Schulsozialarbeit jedoch verpflichtet sein, personenbezogene Daten ohne Einwilligung weiterzugeben. Ein typisches Beispiel hierfür ist der Verdacht auf Kindeswohlgefährdung. In diesem Fall dürfen Mitarbeitende in der Schulsozialarbeit das Jugendamt informieren, wenn gewichtige Anhaltspunkte für eine Gefährdung des Kindeswohls vorliegen und andere Maßnahmen, wie die Beratung der Personensorgeberechtigten, nicht ausreichend sind. Dieser Schritt erfolgt stets unter der Abwägung, ob er für den Schutz des Kindes erforderlich ist.

Fazit: Die Schulsozialarbeit ist somit ein sensibler Bereich, in dem der Datenschutz und die Schweigepflicht eine zentrale Rolle spielen. Nur durch die Einhaltung dieser Grundsätze kann das notwendige Vertrauensverhältnis aufgebaut werden, das die Basis für eine erfolgreiche Unterstützung bildet.

Das Gesundheitsdatennutzungsgesetz zwischen Digitalisierung und Datenschutz

Das im März 2024 in Kraft getretene Gesundheitsdatennutzungsgesetz (GDNG) ist Teil eines umfassenden Digitalisierungspakets im Gesundheitswesen. Ziel des Gesetzes ist es, elektronische Gesundheitsdaten für Forschung und gemeinwohlorientierte Zwecke nutzbar zu machen und damit auch die Grundlage für den Anschluss an den Europäischen Gesundheitsdatenraum (EHDS) zu schaffen. Durch das GDNG soll die Nutzung elektronischer Patientenakten (ePA) in Deutschland etabliert und ab 2025 standardmäßig für alle gesetzlich Versicherten eingeführt werden.

Soweit Versicherte ihre Daten nicht für diese Zwecke zur Verfügung stellen wollen, müssen sie aktiv werden und über einen sogenannten Opt-out-Mechanismus ihre Teilnahme ablehnen. Mit diesem Vorgehen wird

eine hohe Teilnahmequote erwartet, so dass eine umfassende Datenbasis für Forschungszwecke geschaffen wird. Das Verfahren zur Nutzung der Gesundheitsdaten sieht eine zentrale Datenzugangs- und Koordinierungsstelle vor. Über diese Stelle werden die in den ePAs gespeicherten Gesundheitsdaten pseudonymisiert und für Forschungsanfragen verfügbar gemacht. Dabei bleibt die tatsächliche Speicherung der Daten weiterhin dezentral in den jeweiligen Gesundheitseinrichtungen, die nur die relevanten Metadaten an die zentrale Stelle übermitteln. Diese Infrastruktur soll sicherstellen, dass Forschungsinstitutionen unter klar definierten Bedingungen auf die Daten zugreifen können. Zudem wird die Möglichkeit einer federführenden Datenschutzaufsicht bei länderübergreifenden Projekten und Forschungsvorhaben geschaffen.

Ein zentraler Aspekt des GDNG ist der Umgang mit Pseudonymisierung. Durch Pseudonymisierung sollen individuelle Gesundheitsdaten von den realen Identitäten der Patientinnen und Patienten entkoppelt werden, um ihre Privatsphäre zu schützen. Trotz dieser Maßnahme gibt es datenschutzrechtliche Bedenken, dass es bei der Verarbeitung und Verknüpfung großer Datenmengen dennoch zur unbeabsichtigten „Re-Identifikation“ von Personen kommen könnte. Das Gesetz betont daher die Notwendigkeit einer DSFA, die speziell für Gesundheitsdaten vorgeschrieben ist.

Außerdem dürfen die Daten nur für eng umrissene Forschungszwecke verwendet werden, wobei der Zugriff durch spezielle Schutzmaßnahmen wie die Geheimhaltungspflicht und Sanktionsmechanismen abgesichert wird.

Für den Umgang mit Abrechnungsdaten der Kranken- und Pflegekassen sind ebenfalls Neuerungen im GDNG vorgesehen. Sie dürfen diese Daten ohne ausdrückliche Zustimmung der Versicherten analysieren, um potenzielle Gesundheitsrisiken zu erkennen. Dieses Verfahren stößt jedoch auf Kritik, da nicht alle Versicherten über die Möglichkeit des Widerspruchs (Opt-out) informiert sein könnten und somit unfreiwillig Teil dieser Analyse werden.

Die Einführung eines zentralen Datenzugriffs soll darüber hinaus die Grundlage für innovative Forschungsan-

sätze legen und Deutschland in der datengetriebenen Medizin wettbewerbsfähiger machen. Schließlich bleibt fraglich, wie der Datenschutz in der Praxis umgesetzt werden kann und ob die Interessen der Versicherten ausreichend berücksichtigt werden. Die Balance zwischen dem Schutz sensibler Gesundheitsdaten und der Öffnung für wissenschaftliche Nutzung bleibt eine Herausforderung.

Aufbewahrung und Löschung

Bei der Datenverarbeitung stellt sich die Frage nach der Aufbewahrung und Löschung von personenbezogenen Daten. Zu diesem Themenkomplex hat der BfD EKD diverse Datenschutzbeschwerden und Beratungsanfragen bearbeitet.

Vernichtung von Corona-Testnachweisen auf Wertstoffhof

Die datenschutzwidrige Entsorgung von Corona-Testnachweisen war Gegenstand der Datenpannenmeldung einer diakonischen Einrichtung. Dem BfD EKD wurde gemeldet, dass, nachdem die Aufbewahrungsfristen aus dem Infektionsschutzgesetz (IfSG) verstrichen waren, sensible Informationen über Beschäftigte auf einem Wertstoffhof im Restmüll entsorgt wurden.

Der verantwortlichen Stelle hätte auffallen müssen, dass diese Art der Löschung datenschutzrechtlich nicht den gesetzlichen Vorgaben entspricht, wenn sie zuvor eine DSFA durchgeführt hätte.

Eine DSFA wäre nach den gesetzlichen Vorgaben durchzuführen gewesen, da im Zuge der damals aufgrund des IfSG geltenden Zutrittskontrollen und Testpflicht für Beschäftigte von bestimmten Einrichtungen eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten in Form von Gesundheitsdaten vorlag.

Dennoch wurde keine DSFA durchgeführt. Die verantwortliche Stelle hat daher im Vorfeld keine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung erstellt. Sie hatte demnach die Risiken für die Rechte und Freiheiten der betroffenen Personen zuvor nicht

bewertet. Zur Bewältigung der erkennbaren Risiken konnten keine Abhilfemaßnahmen geplant werden, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür hätte erbracht werden können, dass die datenschutzrechtlichen Regelungen eingehalten worden wären.

Im Übrigen hätte eine Entsorgung der Test-Nachweise nur abgesichert durch eine Vereinbarung über die Verarbeitung im Auftrag durch einen qualifizierten Auftragsverarbeiter durchgeführt werden dürfen.

Fazit: Die verantwortliche Stelle hätte mit einer DSFA erkennen können, dass von den Corona-Testnachweisen Risiken für die betroffenen Personen ausgehen und die Entsorgung über den Restmüll als datenschutzwidrig nicht hätte erfolgen dürfen.

Sicherheitsstandards bei der Vernichtung von (Papier-) Akten

Auch in Zeiten fortschreitender Digitalisierung werden in kirchlichen und diakonischen Einrichtungen (noch) Papierakten geführt. In manchen Fällen stößt man auch noch auf andere Formen der analogen Langzeit-Ablage, wie etwa Mikrofilme oder Mikrofiche.

Unabhängig von der Art der Speicherung (z. B. Papier, Mikrofilm, physische Datenträger oder in der Cloud) sind personenbezogene Daten unter Einhaltung der Grundsätze aus § 5 Abs. 1 DSGVO – hier Zweckgebundenheit und Datenminimierung – nach Erledigung ihres Zweckes vollständig und irreversibel zu löschen.

In diesem Zusammenhang erreichen uns regelmäßig Anfragen zu Auswahlkriterien an Geräte zur datenschutzkonformen Datenvernichtung.

Das Thema der technischen Löschung/Vernichtung von Datenträgern ist umfassend in der DIN 66399 geregelt. Dort werden drei Schutzklassen für Daten und sieben Sicherheitsstufen für Geräte definiert und einander zugeordnet. Zusätzlich werden die Geräte nach dem Format der Datenrepräsentation unterschieden, wobei z. B. „P“ (Papier) für jede Darstellung in lesbarer Originalgröße und „F“ (Film) für verkleinerte Darstellung stehen. Die Sicherheitsstufen sind unter anderem über die Partikelgröße des geschredderten Materials definiert.

Personenbezogene Daten sind immer mindestens in Schutzklasse 2, personenbezogene Daten besonderer Kategorie (z. B. Gesundheitsdaten) in Schutzklasse 3 einzustufen. Der Schutzklasse 3 werden Vernichtungsgeräte der Sicherheitsstufen 4 bis 7 zugeordnet.

Bei einer notwendigen Investition empfiehlt der BfD EKD daher Geräte mindestens der Sicherheitsstufe 4, also „P4“ für Papierakten bzw. „F4“ für Mikrofilme.

Überall dort, wo eine eigene Investition aufgrund des geringen anfallenden Aktenvolumens nicht sinnvoll ist, kann auch ein entsprechender Entsorgungsvertrag mit einem Dienstleister geschlossen werden, der dem Auftraggeber die Vernichtung nach der spezifizierten Sicherheitsstufe zusichert.

Geltendmachung eines Löschanpruchs für Taufbucheinträge

Die Taufe eines Kindes erfolgt auf Wunsch der Erziehungsberechtigten immer noch oft im Kindesalter. Nicht immer kann sich die getaufte Person jedoch im Erwachsenenalter mit der Religionszugehörigkeit identifizieren. Aufgrund eines Kirchenaustritts kann der Wunsch entstehen, die Taufe „ungeschehen“ zu machen und den Taufbucheintrag löschen zu lassen. Als Rechtsgrundlage für die Durchsetzung eines Löschanpruchs für Taufbucheinträge kommt § 21 DSGVO in Betracht.

Weil die Verarbeitung der personenbezogenen Daten bei einer Taufe nicht auf einer Einwilligung des Kindes beruht, kommt der Widerruf einer etwaigen Einwilligung nach § 21 Abs. 1 Nr. 3 DSGVO nicht in Betracht. Eine Pflicht zur Löschung aufgrund eines Widerspruchs gem. § 21 Abs. 1 Nr. 4 DSGVO setzt voraus, dass keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen. In § 21 Abs. 3 DSGVO werden Ausnahmetatbestände zur Löschpflicht und damit beispielhaft Gründe für ein berechtigtes Interesse an der Verarbeitung aufgezählt. Wenn die Verarbeitung nach den in § 21 Abs. 3 Nr. 1 bis 5 DSGVO genannten Ausnahmetatbeständen erforderlich ist, kann der Anspruch auf die Löschung nicht durchgesetzt werden. Ein solcher Ausnahmetatbestand liegt nach § 21 Abs. 3 Nr. 2 DSGVO beispielsweise vor, wenn die Ausnahme zur Löschpflicht mit der Wahrnehmung

einer Aufgabe, die im kirchlichen Interesse oder in der Ausübung hoheitlicher Gewalt liegt, begründet werden kann.

Für eine dauerhafte Speicherung im Taufbuch spricht aus Sicht des kirchlichen Interesses, dass es sich bei der Taufe um eine Kasualie handelt, die einem unwiderleglich stattgefundenen Ereignis zugeordnet wird. Dieses Ereignis kann auch durch die Löschung des Eintrags in das Taufbuch nicht ungeschehen gemacht werden. Der Eintrag im Taufbuch dokumentiert dieses Ereignis und dient auch konfessionsübergreifend als Nachweis. Die Kenntnis über die Taufe ist ferner bei einem möglichen Wiedereintritt in die Religionsgemeinschaft aus kirchlicher Sicht nötig. Die Interessen der Kirchengemeinde an der Nichtlöschung sind im Rahmen einer Interessenabwägung mit dem Interesse der Einzelperson an der Löschung abzuwägen. Nach herrschender Meinung in Rechtsprechung und Literatur überwiegt das kirchliche Interesse gegenüber dem Interesse einer einzelnen Person. (vgl. Rspr.: VGH Bayern, 16. Februar 2025 – Az.: 7 ZB 14.357).

Im Ergebnis ist daher festzustellen, dass ein nach § 21 Abs. 3 Nr. 2 DSGVO überwiegendes kirchliches Interesse an der Speicherung der Taufdaten besteht und der Löschanpruch in der Regel nicht erfolgreich geltend gemacht werden kann. Um dennoch dem Interesse betroffener Personen gerecht zu werden, welche die Zugehörigkeit zur Religionsgemeinschaft ablehnen und den Löschanpruch geltend machen, sollte aus datenschutzrechtlicher Sicht ein Sperrvermerk im Kirchengemeinderegister eingetragen werden. Ein solcher bewirkt, dass die Verarbeitung der personenbezogenen Daten auf ein Minimum reduziert wird und die Persönlichkeitsrechte gewahrt werden können. Der Eintrag ist damit nur noch für einen sehr geringen Personenkreis einsehbar und es wird die Auskunft und Einsichtnahme durch unbefugte Dritte ausgeschlossen.

Anfertigung eines Löschkonzepts

Es stellt einen elementaren Datenschutzgrundsatz dar, dass personenbezogene Daten nur zu einem klar definierten Zweck verarbeitet werden dürfen und zu löschen sind, wenn dieser Zweck entfällt. Die Daten müssen jedoch verfügbar sein, solange sie recht-

mäßig benötigt werden. Gesetzliche oder betriebliche Anforderungen definieren die (Höchst-)Aufbewahrungsfrist. Bereits bei der Systemkonzeption sind Löschräume vorzusehen. Die DIN 66398 stellt die Leitlinie zur Entwicklung eines Löschkonzepts für personenbezogene Daten dar. Die Norm bietet Vorschläge zur Erstellung von Löschräumen und zur Dokumentation des Konzepts.

Ein Löschkonzept umfasst die folgenden Schritte:

- Datenarten bestimmen: Identifizieren der verschiedenen Arten von personenbezogenen Daten, die in der Organisation verarbeitet werden
- Löschklassen erstellen: Gruppieren der Datenarten in Löschklassen basierend auf ihrer Bedeutung und Verarbeitung
- Löschräume formulieren: Entwickeln von Regeln für die Löschung der Daten in jeder Löschkategorie
- Umsetzungsregeln festlegen: Bestimmen, wie die Löschräume technisch und organisatorisch umgesetzt werden
- Dokumentation: Dokumentieren des gesamten Löschkonzepts und der festgelegten Regeln.

Fazit: Ein Löschkonzept hilft, die gesetzlichen Vorgaben umzusetzen und soll eindeutige Löschräume machen. Es ist für ein umfangreiches Datenschutzmanagement unerlässlich.

Verarbeitung von Beschäftigtendaten

Zur Verarbeitung von Beschäftigtendaten erreichten den BfD EKD im Berichtszeitraum Datenschutzbeschwerden und einige Beratungsanfragen.

Umgang mit erweiterten Führungszeugnissen

Der Umgang mit erweiterten Führungszeugnissen von Mitarbeitenden und Ehrenamtlichen wurde in kirchlichen und diakonischen Einrichtungen in der Vergangenheit unterschiedlich gehandhabt.

Der BfD EKD vertrat bisher die Auffassung, dass verantwortliche Stellen erweiterte Führungszeugnisse von Mitarbeitenden (in einem verschlossenen Umschlag) zur analogen Personalakte nehmen dürfen, ohne dass dies als Datenschutzverstoß angesehen wird. Bei Ehrenamtlichen, für die keine Personal-

akten geführt werden, wurde hingegen in der Vergangenheit nur die Einsichtnahme dokumentiert, ohne das erweiterte Führungszeugnis selbst zu speichern.

Mit der Gesetzesänderung vom 4. Dezember 2022 wurde § 30a in das Bundeszentralregistergesetz (BZRG) eingefügt, der die datenschutzrechtliche Verarbeitung solcher Zeugnisse nun konkreter regelt. Laut § 30a Abs. 3 BZRG dürfen die „Daten aus einem erweiterten Führungszeugnis“ nur verarbeitet werden, soweit dies zur Prüfung der Eignung der betroffenen Person für eine bestimmte Tätigkeit erforderlich ist. Das Führungszeugnis selbst oder eine Kopie davon darf hingegen nicht gespeichert werden. Die Daten müssen zudem vor unbefugtem Zugriff geschützt werden und sind unverzüglich zu löschen, wenn die betreffende Tätigkeit nicht mehr ausgeübt wird.

Nach dieser klarstellenden Regelung bedeutet dies für eine datenschutzkonforme Verarbeitung, dass zukünftig auch bei Mitarbeitenden nur noch ein Sichtvermerk über die Einsichtnahme in das Führungszeugnis erstellt und in den Akten vermerkt werden darf. Die Ablage des Originals oder einer Kopie ist mangels Rechtsgrundlage nicht (mehr) zulässig. In Akten abgelegte Führungszeugnisse sind daher datenschutzkonform zu vernichten. Die datenschutzkonforme Verarbeitung betrifft dabei erweiterte Führungszeugnisse, deren Pflicht zur Einholung sowohl auf kirchlichen Regelungen als auch auf spezialgesetzlichen Rechtsgrundlagen wie etwa § 72a Abs. 1 Sozialgesetzbuch (SGB) VIII oder § 75 Abs. 2 SGB XII basiert.

Fazit: Das erweiterte Führungszeugnis im Original oder in Kopie zur Personalakte zu nehmen, ist nicht (mehr) zulässig. Die Einsichtnahme in das Führungszeugnis ist durch einen Vermerk zu dokumentieren.

Zugriff auf das persönliche Laufwerk

Im Berichtszeitraum ging beim BfD EKD eine Beschwerde ein, welche den unbefugten Zugriff auf das persönliche Laufwerk (Home-Verzeichnis) einer Beschäftigten zum Gegenstand hatte. Hierbei stand im Raum, dass die Beschäftigte nach einer längeren Vakanz die Einrichtung verlassen würde. Aufgrund

des ungewissen Zustandes und wirtschaftlicher Aspekte entschied die verantwortliche Stelle, die Daten der Beschäftigten zu sperren, anstatt sie zu löschen. Hierbei wurden die Daten aus dem persönlichen Laufwerk auf den Rechner einer anderen Mitarbeiterin kopiert, welche uneingeschränkten Zugang zu den Daten erhielt.

Beschäftigtendaten dürfen nur unter den normierten Voraussetzungen des § 49 DSGVO verarbeitet werden. Allein das „Zur-Verfügung-Stellen“ durch das Ablegen der Daten auf das Laufwerk einer anderen Mitarbeiterin stellt bereits eine Verarbeitung der personenbezogenen Daten dar. Es kommt hierbei nicht darauf an, ob ein tatsächlicher Zugriff stattgefunden hat oder nicht. Es genügt allein die Möglichkeit des Zugriffs.

Sofern dienstliche Daten von Mitarbeitenden an einem anderen Speicherort gespeichert werden, sind gem. § 27 DSGVO geeignete technische und organisatorische Maßnahmen von der verantwortlichen Stelle zu treffen, um ein dem Risiko angemessenes Schutzniveau herzustellen. Dies beinhaltet, dass unbefugte Dritte nicht die Möglichkeit erhalten, auf die Daten zuzugreifen. Entsprechend dem Transparenzgebot müssen Beschäftigte zudem hierüber in Kenntnis gesetzt werden. Im vorliegenden Fall kam erschwerend hinzu, dass die Zugriffsmöglichkeit über einen längeren Zeitraum – auch nach Rückkehr der Beschäftigten – fortbestand, sodass eine Beanstandung durch den BfD EKD ausgesprochen wurde.

Betrieblicher Aushang mit sensiblen Informationen

In der Praxis kommt es in kirchlichen und diakonischen Einrichtungen immer wieder vor, dass bei Weggang von Mitarbeitenden die übrigen Mitarbeitenden darüber informiert werden sollen. Dabei stellt sich die Frage, wie diese Information auch vor dem Hintergrund berechtigter Interessen der betroffenen Person datenschutzkonform erfolgen kann.

In einem Fall informierte der Arbeitgeber die übrigen Mitarbeitenden durch einen Aushang. In diesem Aushang wurde der Name der betroffenen Person benannt und es wurde darauf hingewiesen, dass diese Person gegen datenschutzrechtliche Vorschriften verstoßen habe und dass das Verhalten der Mitarbeite-

rin sogar strafrechtlich relevant sei. Dieser Aushang erfolgte an einer Stelle, die nicht nur Mitarbeitenden, sondern auch Dritten frei zugänglich war.

Vor diesem Hintergrund hat der BfD EKD eine Beanstandung gegenüber der kirchlichen Stelle ausgesprochen. Die berechtigten Interessen der ehemals beschäftigten Person wurden im Vorfeld der Datenverarbeitung nicht ausreichend berücksichtigt. Den Klarnamen dieser Person und die gegen sie erhobenen Vorwürfe für alle Mitarbeitenden sowie für Dritte zugänglich auszuhängen, stellte einen Datenschutzverstoß dar. Vielmehr hätte eine Benachrichtigung der Mitarbeitenden durch eine E-Mail über den Weggang der Person ohne Angabe von Gründen ausgereicht, um die Interessen der verantwortlichen Stelle zu erfüllen.

Nachweis der Kinderanzahl durch Vorlage von Geburtsurkunden

Mit Inkrafttreten des Pflegeunterstützungs- und Entlastungsgesetzes zum 1. Juli 2023 wird der Beitragssatz in der Pflegeversicherung nunmehr nach der Kinderanzahl differenziert. Zur Frage des Nachweises der Elterneigenschaft und der Anzahl der berücksichtigungsfähigen Kinder erhielt der BfD EKD mehrere Anfragen von Mitarbeitenden sowie von kirchlichen und diakonischen Stellen.

Um eine einheitliche Rechtsanwendung sicherzustellen, beabsichtigte der Gesetzgeber, bis zum 31. März 2025 ein digitales Verfahren zur Erhebung und zum Nachweis der Elterneigenschaft und der Anzahl der berücksichtigungsfähigen Kinder zu entwickeln. Der Zeitraum bis dahin schaffte jedoch Unsicherheit. Wenig bekannt ist das sogenannte „vereinfachte Verfahren“, das Arbeitgeber bis längstens 30. Juni 2025 nutzen können. Der Nachweis der Elterneigenschaft gilt danach auch dann als erbracht, wenn Mitarbeitende auf Anforderung der beitragsabführenden Stelle oder der Pflegekasse die erforderlichen Angaben zu den berücksichtigungsfähigen Kindern lediglich mitteilen, § 55 Abs. 3 Satz 2 Sozialgesetzbuch (SGB) XI. Damit ist für eine Vorlagepflicht von Dokumenten wie beispielsweise Geburtsurkunden jedoch kein Platz mehr. Der Zweck der Verarbeitung kann bereits durch die bloße Mitteilung der

Kinderanzahl erreicht werden, da diese Mitteilung als Nachweis im Rechtssinne gilt. Die Verarbeitung der Geburtsurkunden ist damit nicht erforderlich im Sinne von § 49 Abs. 1 DSGVO.

Fazit: Das Einholen von Geburtsurkunden, die über die Elterneigenschaft hinaus weitere personenbezogene Daten zum Kind sowie dem anderen Elternteil enthalten, ist datenschutzrechtlich unverhältnismäßig.

Einsatz von Videokameras

Die Videoüberwachung öffentlicher und nichtöffentlicher Bereiche wird in kirchlichen und diakonischen Einrichtungen immer häufiger eingesetzt. Der Themenkomplex bringt vielseitige Fragen und Probleme mit sich.

Videoüberwachung in Kirchen

Häufig gibt es das Anliegen, Kirchen auch außerhalb von Gottesdienstzeiten oder sonstigen Veranstaltungen zu öffnen. Aber auch Kirchen sind immer öfter von Vandalismus betroffen.

Auch in diesem Berichtszeitraum erreichten den BfD EKD Anfragen zu den Voraussetzungen des datenschutzkonformen Einsatzes der Videoüberwachung von Kircheninnenräumen. Für den Fall eines besonders intensiven Eingriffs in das Persönlichkeitsrecht von Betroffenen durch eine Videoüberwachung im öffentlich zugänglichen Raum sieht das EKD-Datenschutzgesetz in § 52 DSGVO eine spezielle Rechtsgrundlage vor. Zu beachten ist hierbei regelmäßig unter anderem:

Die Beobachtung ist gemäß § 52 Abs. 1 DSGVO nur zulässig, soweit sie in Ausübung des Hausrechts oder zum Schutz von Personen und Sachen erforderlich ist, und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Tatsache, dass eine Videoüberwachung erfolgt, ist gemäß § 52 Abs. 2 DSGVO bekannt zu machen, ebenso der Name und die Kontaktdaten der verantwortlichen Stelle, und zwar zum frühestmöglichsten

Zeitpunkt, z. B. durch gut sichtbare Hinweisschilder am Beginn des überwachten Bereichs.

Die Speicherung oder Verwendung der erhobenen Daten ist gemäß § 52 Abs. 3 DSGVO zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Gemäß § 52 Abs. 5 DSGVO sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Zudem ist die vorherige Durchführung einer DSFA erforderlich. Da bei dieser Art der Überwachung die Möglichkeit zur Verhaltens- und Leistungskontrolle von Mitarbeitenden besteht, ist die Einrichtung der Überwachung gemäß § 40 j MVG-EKD durch die Mitarbeitervertretung auch mitbestimmungspflichtig.

Videoüberwachung im Pflegeheim

Im Berichtszeitraum gingen beim BfD EKD mehrere Beschwerden ein, die die Videoüberwachung sowohl in privaten als auch in Gemeinschaftsräumen von Pflegeheimen zum Gegenstand hatten.

Bei einer bestehenden Selbst- oder Fremdgefährdung kann es aus Sicht des Pflegeheimes in Betracht kommen, Videokameras als notwendiges Mittel zur Beobachtung einzusetzen. Allerdings stellt die Videoüberwachung einen sehr hohen Eingriff in das Persönlichkeitsrecht dar. Die Zulässigkeit des Einsatzes muss vorab gemäß § 52 DSGVO überprüft werden.

Hierbei sind unter anderem folgende Schritte von einer verantwortlichen Stelle zu unternehmen, um den Schutz der personenbezogenen Daten zu gewährleisten: Örtlich Beauftragte für den Datenschutz müssen stets beratend beteiligt werden und es ist eine DSFA nach § 34 DSGVO zu erstellen. Im Übrigen müssen Einwilligungserklärungen von den Personen eingeholt werden, die in den Erfassungsbereich der Videoüberwachung gelangen können. Hierzu gehören nicht nur die Bewohnerinnen und Bewohner, sondern auch Mitarbeitende und Familienangehörige. Auch die Videokameras müssen für den Zweck geeignet sein und den technischen Anforderungen entsprechen. Es darf

sich keinesfalls um ein Gerät handeln, das die Aufnahmen auf private Endgeräte der Mitarbeitenden überträgt. Der Bereich der Videoüberwachung sollte auf das geringste erforderliche Maß bestimmt werden. Das gleiche gilt für den Zeitraum, in dem die Videoüberwachung stattfindet. Hierbei sollte geprüft werden, ob die Beobachtung zu Nachtzeiten genügt. Eine Speicherung der Aufnahmen sollte zum Zweck der Sicherheit der Betreuten in der Regel nicht erfolgen. Darüber hinaus ist mit einer Beschilderung auf den Bereich hinzuweisen, in dem die Videoüberwachung stattfindet. Es muss auch daran gedacht werden, die Überwachungsmaßnahme im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

Fazit: Aufgrund der hohen Eingriffsintensität beim Einsatz von Kameras in diakonischen Einrichtungen sind alle Voraussetzungen für einen datenschutzkonformen Einsatz sorgfältig zu prüfen und zu dokumentieren.

Einsatz von Kamera-Attrappen

Eine weitere Beschwerde hatte – so schien es zunächst – die Videoüberwachung eines öffentlichen Wegs zum Gegenstand. Dabei waren mehrere Kameras an einem Gebäude installiert, das sich auf einem an den Weg angrenzenden Grundstück einer Kirchengemeinde befand.

Bei den am Gebäude angebrachten Kameras handelte es sich aber lediglich um Attrappen. Hintergrund des Anbringens war hier, dass das kirchliche Grundstück mit aufstehendem Gebäude an den örtlichen Marktplatz angrenzte, der aufgrund seiner Kriminalitätsbelastung durch Vandalismus und Kleinkriminalität kommunal als sogenannter „gefährlicher Ort“ geführt wurde.

Der scheinbar überwachte Bereich war wiederum kein öffentliches Straßenland, sondern stand im Eigentum der Kirchengemeinde, die Nutzung durch die Anwohner wurde lediglich geduldet.

Die Kirchengemeinde wurde darauf hingewiesen, dass Kamera-Attrappen zwar nicht unter die Regelungen des Datenschutzrechts fallen, aber einen Eingriff in das allgemeine Persönlichkeitsrecht darstellen können. Auch wenn mit Kameraattrappen keine personenbezo-

genen Daten verarbeitet werden, erzeugt die Attrappe einen Überwachungsdruck. Es wurde geraten, die Attrappen so auszurichten, dass nicht der Eindruck entstehen kann, der Weg werde erfasst.

Digitale Kommunikation

Die digitale Kommunikation beschäftigte den BfD EKD im Berichtszeitraum sowohl im Rahmen von Datenschutzbeschwerden als auch im Rahmen von zahlreichen Beratungsanfragen.

Phishing-E-Mails

Viele Cyber-Angriffe auf kirchliche und diakonische Einrichtung bedienen sich sogenannter Phishing-E-Mails, durch die arglose Mitarbeitende dazu verleitet werden sollen, persönliche oder betriebliche Geheimnisse, etwa Namen und Passwörter zu Anwendungen oder Komponenten der IT-Infrastruktur preiszugeben.

Neben einer wiederholten Schulung der Mitarbeitenden zur Prävention können auch technische Maßnahmen getroffen werden, dass diese schadhafte E-Mails erst gar nicht in den Postfächern der Mitarbeitenden ankommen.

Prinzipiell sind schadhafte E-Mails so aufgebaut, dass auf den ersten Blick durchaus plausible Inhalte von anscheinend legitimen und bekannten Absendern verschickt werden. Oft ist die wirkliche Quelle jedoch eine andere, als auf den ersten Blick aus der Absenderangabe ablesbar ist. Grund dafür ist die Fälschungsanfälligkeit des originalen SMTP (Simple Message Transfer Protocol), der „Bauanleitung“ für jede E-Mail. Nach diesem Protokoll kann – einfach gesagt – die Absenderangabe frei formuliert werden und muss nicht mit den technischen Gegebenheiten, also z. B. der echten Adresse des absendenden Servers übereinstimmen.

Eine Hilfe gegen die Fälschungsanfälligkeit des SMTP bieten die Zusatzdienste SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication, Reporting and Conformance) und DKIM (DomainKeys Identified Mail). Diese drei Dienste haben gemeinsam – auch vereinfacht gesagt –, dass Domäneninhaber bekannt geben, welche Server in ihren Namen E-Mails

verschicken dürfen und wie der Empfänger auf Widersprüchlichkeiten reagieren sollte. Damit die Zusatzdienste nicht auch durch einen Angreifer missbraucht oder gefälscht werden können, werden die Angaben zu den zugelassenen Servern in einer vertrauenswürdigen Stelle hinterlegt.

Jeder E-Mail empfangende Server kann die Zusatzangaben zu jeder eingegangenen E-Mail von der vertrauenswürdigen Stelle abrufen, mit dem Inhalt des SMTP vergleichen und dann entscheiden, ob die E-Mail insgesamt als vertrauenswürdig eingestuft und an das Postfach des Empfängers zugestellt wird oder nicht. Umgekehrt erhöht die versendende Stelle ihre Cyber-Reputation durch die zusätzliche Absicherung der Authentizität der versendeten E-Mail.

Der BfD EKD empfiehlt allen kirchlichen Stellen, die Zusatzdienste zu implementieren, und alle eingehenden E-Mails den entsprechenden Überprüfungen zu unterziehen. Dort, wo die E-Mail-Funktion über einen Dienstleister betrieben wird, sollen die Zusatzdienste Bestandteil des Dienstleistungsvertrags sein. Außerdem sollten alle Mitarbeitenden regelmäßig auf die Gefahren im Umgang mit E-Mails sensibilisiert werden.

Fazit: IT-Sicherheit ist eine wichtige Voraussetzung für wirksamen Datenschutz.

Überprüfung von Websites

Websites können mit speziellen Tools automatisiert überprüft werden, um technische und datenschutzrechtliche Schwachstellen zu identifizieren. Sie prüfen unter anderem, ob SSL-Zertifikate zur sicheren Transportverschlüsselung installiert sind, Analysetools und Cookies eingesetzt werden und ob Daten in unsichere Drittstaaten abfließen, wie es beispielsweise durch das Einbinden von Google Fonts der Fall sein kann.

Einrichtungen, die Websites erstellen oder erstellen lassen, können diese durch solche Tools überprüfen und ihre Datenschutzerklärungen leichter nach den tatsächlichen Gegebenheiten ausrichten. So lassen sich potenzielle Datenschutzverletzungen effizient erkennen und entsprechende Maßnahmen einleiten.

Nicht alle Prüftools können den gesamten Inhalt einer Website analysieren. Kostenlose Tools prüfen oft nur

die Startseite oder wenige Unterseiten und nicht den gesamten Inhalt. Dadurch bleiben beispielsweise der Einsatz von Newsletter-PlugIns oder Kontaktformularen mit Captcha-Funktionalität häufig unbemerkt.

Prüftools können die menschliche Expertise nicht ersetzen. Bei Erstellung einer Datenschutzerklärung sollten die örtlich Beauftragten für den Datenschutz die verantwortliche Stelle unterstützen.

Fazit: Der Einsatz von Prüftools stellt ein wirksames Mittel dar, um die Richtigkeit und Vollständigkeit von Datenschutzerklärungen zu verbessern.

Datenschutzerklärungen häufig falsch

Die Angaben in Datenschutzerklärungen auf Websites entsprechen häufig nicht dem tatsächlichen Umgang mit personenbezogenen Daten bei der Nutzung der Website. Häufig werden zur Erstellung einer Datenschutzerklärung Muster oder Generatoren verwendet, die auf der Datenschutzgrundverordnung (DSGVO) basieren. Die Verwendung von Mustern und Generatoren ohne angepassten Bezug zur Website führt häufig zu einer falschen Datenschutzerklärung. Da wird beispielsweise der Einsatz von Social Media - Funktionalitäten beschrieben, die gar nicht im Einsatz sind. Oder „cookielose“ Websites beschreiben, was Cookies sind. Manchmal befinden sich sogar Einwilligungsbanner für Cookies und Analysetools auf der Website, deren Bestätigung oder Nichtbestätigung zum gleichen Ergebnis führt, dass nämlich kein Cookie gesetzt wird.

Vor dem Hintergrund des in § 5 DSG-EKD normierten Transparenzgebots müssen Datenschutzerklärungen widerspiegeln, wie personenbezogene Daten von Nutzenden der Website tatsächlich verarbeitet werden. Darüber hinaus ist nach § 25 Abs. 1 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDSG) die Speicherung von Cookies und der Zugriff darauf nur zulässig, wenn der Nutzende aufgrund von klaren und umfassenden Informationen eingewilligt hat. Diese notwendigen Informationen sind, sofern tatsächlich Marketing- oder Analysetools eingesetzt werden, nur selten vorhanden.

Fazit: Werden Muster oder Generatoren bei der Erstellung von Datenschutzerklärungen eingesetzt, ist stets eine Anpassung erforderlich.

Datensicherheit und Verschlüsselung

Im Berichtszeitraum hat sich der BfD EKD auch mit unterschiedlichen Beratungsanfragen, Beschwerden und Datenpannenmeldungen im Bereich des technischen Datenschutzes beschäftigt. Regelmäßig dreht es sich dabei um die Themen Datensicherheit und Verschlüsselung.

Verschlüsselung mobiler Datenträger

Eine der effektivsten Maßnahmen zum Schutz der Daten auf mobilen Endgeräten (wie z. B. Notebooks, Tablets, Smartphones und USB-Sticks) ist die vollständige Datenträgerverschlüsselung. Durch eine solche Verschlüsselung werden alle Daten unleserlich gemacht und können nur mit einem entsprechenden Schlüssel entschlüsselt werden. Dies stellt sicher, dass unbefugte Dritte keinen Zugriff auf sensible Informationen erhalten, selbst wenn das Gerät verloren geht oder gestohlen wird.

§ 5 Abs. 1 Nr. 6 DSGVO definiert den Grundsatz der Integrität und Vertraulichkeit, nach dem personenbezogene Daten zu verarbeiten sind. § 27 Abs. 1 DSGVO fordert ein angemessenes Schutzniveau für personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen (TOMs). Darüber hinaus regelt § 27 Abs. 2 DSGVO den Verlust und die unbefugte Offenlegung sowie den unbefugten Zugang zu personenbezogenen Daten.

Ein verschlüsselter Datenträger ist auch nach Abhandenkommen noch sicher, weil selbst beim Zugriff mit einem anderen Betriebssystem die Daten nicht entschlüsselt werden können und somit auch nicht auf die Daten zugegriffen werden kann. Anders verhält es sich, wenn der Schutz der Daten lediglich durch ein Windows-Login im Betriebssystem stattfindet. Dieser Login kann durch den Zugriff über ein alternatives Betriebssystem umgangen werden. Häufig ist der Unterschied zwischen einer Datenträgerverschlüsselung und einem Schutz über den Windows-Login nicht klar. Verschlüsselungen werden selten eingesetzt, obwohl moderne Betriebssysteme oft eingebaute Verschlüsselungsoptionen anbieten, die einfach zu aktivieren und ohne weitere Kosten zu nutzen sind. Ein Beispiel stellt BitLocker in diversen Versionen von Microsoft Windows dar.

Fazit: Mobile Datenträger, auf denen personenbezogene Daten abgelegt werden, sollten stets verschlüsselt werden.

Diebstahl mobiler Endgeräte

Der Diebstahl mobiler Endgeräte ist ein wiederkehrendes Thema, das den BfD EKD bei Datenpannenmeldungen erreicht. Eine Häufung von Diebstählen ist im Bereich von Kindertageseinrichtungen zu beobachten, da aufgrund der fortschreitenden Digitalisierung zunehmend Notebooks, Tablets und Digitalkameras eingesetzt werden. Zur Vermeidung von Datenpannen wird empfohlen, folgende technische und organisatorische Maßnahmen umzusetzen:

Digitale Endgeräte sollten stets verschlüsselt werden. Ein Passwortschutz ist allein nicht ausreichend: Festplatten könnten ausgebaut und dann unter Umgehung des Passwortschutzes ausgelesen werden. In der Praxis werden auch immer noch Passwörter mit einem Klebezettel direkt auf dem Laptop angebracht. Hiervon wird dringend abgeraten.

Bei Digitalkameras besteht die Besonderheit, dass SD-Karten nicht verschlüsselt werden können. Umso wichtiger ist es, Fotos umgehend von der SD-Karte auf ein sichereres Medium zu übertragen.

Darüber hinaus sollten digitale Endgeräte bei Nichtgebrauch stets in einem verschlossenen Schrank aufbewahrt werden. Wünschenswert ist aus datenschutzrechtlicher Sicht auch die Einbindung von Endgeräten in ein Mobile Device Management (MDM) - System.

Beschlagnahme von IT-Geräten

Zur Unterstützung ökumenischer Projekte im Ausland sind Mitarbeitende kirchlicher Einrichtungen weltweit unterwegs und führen dabei IT-Geräte und dienstliche Unterlagen mit. In diesem Zusammenhang wurde dem BfD EKD eine Datenpanne gemeldet. Beim Antritt einer Reise in ein Land im Nahen Osten haben Sicherheitskräfte das Handgepäck der Mitarbeiterin eines Missionswerkes beschlagnahmt, das unter anderem auch einen Laptop und ein Smartphone sowie Arbeitsdokumente enthielt. Sämtliche Dinge erhielt sie erst nach Ende der Reise per Post zurück.

Eine forensische Untersuchung des Laptops durch die zuständige IT-Abteilung der kirchlichen Einrichtung ergab, dass die Festplatte in der Zwischenzeit aus- und wieder eingebaut wurde. Es kann mit großer Wahrscheinlichkeit davon ausgegangen werden, dass auf der Festplatte enthaltene Daten den Sicherheitsbehörden zur Kenntnis gelangten. Der BfD EKD gab den dringenden Hinweis, dass eine Festplattenverschlüsselung eine angemessene technische Maßnahme zum Schutz der Vertraulichkeit darstellt.

Fazit: Datenträger sollten in allen (mobilen) Endgeräten als Standardmaßnahme verschlüsselt werden.

Privater Erwerb einer gebrauchten Festplatte

Im Berichtszeitraum erreichte den BfD EKD eine besondere Datenpannenmeldung. Der Chefarzt einer psychiatrischen Klinik im diakonischen Bereich erhielt eine anonyme E-Mail, dass auf einer gebrauchten erworbenen Festplatte ca. 80 Datensätze, in denen Klarnamen, Geburtsdaten, Diagnosen sowie die ärztliche Befund- und Verlaufsdokumentation enthalten waren, vorgefunden wurden.

Diese Daten stammten von einer ehemaligen Mitarbeiterin der Fachklinik, die seit mehreren Jahren nicht mehr im Unternehmen tätig war. Die Mitarbeiterin hatte offensichtlich die Daten auf ihrem privaten Rechner ohne Zustimmung und Kenntnis ihrer Vorgesetzten gespeichert. Die unbekannt Person hatte die Festplatte später bei einem Privatverkauf erworben. Dieser Vorfall zeigt, wie wichtig vorhandene Regelungen zum Umgang mit privaten IT-Geräten für den Datenschutz sind, die üblicherweise die Verarbeitung dienstlicher Daten auf privaten Endgeräten verbieten. Beschäftigte sollten diesbezüglich wiederholt sensibilisiert werden.

Ähnliche Situationen können auch entstehen, wenn alte dienstliche IT-Geräte ausgesondert und den Beschäftigten zur privaten Weiternutzung angeboten werden. Auch in diesem Fall ist eine datenschutzkonforme Datenlöschung vor der Weitergabe zwingend vorzunehmen.

Multi-Faktor-Authentifizierung als Stand der Technik?!

Ob Multi-Faktor-Authentifizierung (MFA) dem Stand der Technik entspricht, wurde im Austausch mit

örtlich Beauftragten für den Datenschutz immer wieder gefragt. Konkret ging es um einen App-Anbieter, der sich weigerte, seine Software mit einer MFA auszustatten.

Gemäß § 27 DSGVO sind geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. MFA ist ein Sicherheitsmechanismus, der für die Zugriffsgewährung über die herkömmliche Passwortabfrage hinausgeht. Er verwendet dazu mehrere Authentifizierungsfaktoren. Der Nachweis der Identität von Nutzenden erfolgt mit mehr als einem Faktor wie z. B. Passwort + One-Time-Passwort oder Passwort + Fingerabdruck oder Passwort + Token. Wenn ein System lediglich mit einer Ein-Faktor-Authentifizierung gesichert ist, besteht für die Nutzenden ein erhöhtes Risiko des Identitätsdiebstahls, -missbrauchs und -betrugs.

Ziel von MFA ist es, die Sicherheit personenbezogener Daten in Apps und auf Endgeräten maßgeblich zu erhöhen. MFA hat sich in den letzten Jahren als ein essenzieller Bestandteil moderner IT-Sicherheitskonzepte etabliert. Ihre Verwendung schützt nicht nur vor einfachen Passwort-Diebstählen, sondern macht es Angreifenden erheblich schwieriger, Zugang zu sensiblen Daten zu erlangen.

Eine App oder ein Service, der MFA nicht unterstützt, kann potenziell schwerwiegende Folgen nach sich ziehen, insbesondere wenn es um den Schutz sensibler, personenbezogener Daten geht. Das Erreichen eines angemessenen Schutzniveaus durch geeignete TOMs ist nur möglich, wenn MFA angeboten wird. Es ist daher unerlässlich, dass sowohl Entwickler als auch Nutzende die Bedeutung von MFA erkennen und sie als selbstverständlich in ihre Sicherheitsstrategien integrieren.

Auslagerung der IT-Infrastruktur in die Azure-Cloud

Die Azure-Cloud von Microsoft ist – wie alle Cloud-Dienste – ein digitaler Speicher zur Ablage von unterschiedlichen Informationen (z. B. Dokumente, virtuelle Angebote, Datensicherungen). Kirchliche Stellen können ihre IT-Infrastruktur in eine Cloud auslagern und darin virtuell betreiben. Eine bisher im eigenen Rechenzentrum oder im Rechenzentrum eines

IT-Dienstleisters betriebene IT kann auf diesem Weg skalierbar und als virtuell zur Verfügung gestelltes Angebot in der Azure-Cloud von Microsoft betrieben werden.

Die Auslagerung der eigenen IT-Infrastruktur in die Azure-Cloud stellt verantwortliche Stellen im Hinblick auf den im Rahmen der Rechenschaftspflicht gemäß § 5 Abs. 2 DSGVO zu dokumentierenden Nachweis über die Einhaltung der Grundsätze der Verarbeitung vor große Herausforderungen.

Verantwortliche Stellen müssen sich zu Beginn eines solchen Digitalisierungsprojekts immer bewusst machen, dass als Nachweis das Verzeichnis der Verarbeitungstätigkeiten (VVT) entsprechend angepasst werden muss. Dieses Verzeichnis enthält die in § 31 Abs. 1 Satz 2 DSGVO genannten Angaben, zu denen unter anderem die Zwecke der Verarbeitung, die Kategorien von Empfängern einschließlich Empfängern in Drittländern sowie gegebenenfalls die Übermittlungen von personenbezogenen Daten an ein Drittland und wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOMs) gemäß § 27 DSGVO gehören.

Aufgrund der Verwendung neuer Technologien und dem als Folge verbundenen voraussichtlich hohen Risiko für die Rechte natürlicher Personen muss auch eine DSFA durchgeführt werden. Die DSFA hat auf der Grundlage der Verarbeitung und deren Zweck zum Ziel, Risiken zu ermitteln, für deren Bewältigung angemessene Abhilfemaßnahmen als TOMs ermittelt werden, die zur Gewährleistung eines angemessenen Schutzniveaus dienen sollen.

Fazit: Eine DSFA zeigt insbesondere risikominimierende TOMs auf, die im VVT beschrieben werden können. Wenn die Verarbeitung oder die Zwecke nicht klar beschrieben werden können, kann auch ein dokumentierter Nachweis nicht geführt werden.

Durchführung von Backups mithilfe von Cloud-Diensten

Aufgrund einiger Beratungsanfragen, ob Backups (Datensicherungen) auch mit Cloud-Diensten durchgeführt werden können, gab der BfD EKD einige Hinweise. Das Ziel von Datensicherung ist die Wiederherstellung

von Daten und Systemen, die gelöscht oder sogar physikalisch zerstört wurden. Die Wiederherstellungszeit muss angemessen sein. Die Speichersysteme und Datenleitungen müssen dafür eine ausreichende Kapazität bereitstellen. Dies ist insbesondere bei Cloud-Lösungen zu prüfen, da die Bandbreite zum Internet möglicherweise einen stark limitierenden Faktor darstellt. Es wird empfohlen, nicht auf lokale Backups zu verzichten. Auch bei cloudbasierten Backups kann es zu Ausfällen kommen. Bei einem Ausfall der Datenleitung zum Cloud-Anbieter ist ein Restore bzw. Backup nicht möglich.

Mit externen Dienstleistern muss ein Auftragsverarbeitungsvertrag (AV-Vertrag) geschlossen werden. Die technischen und organisatorischen Maßnahmen zum Schutz der Daten müssen darin beschrieben werden.

Ohne den Nachweis einschlägiger Zertifizierungen (ISO 27001 ff, Trustes Cloud, BSI Grundschutz etc.) ist eine Einschätzung über den Sicherheitsstandard kaum möglich.

Allgemein sind bei der Nutzung von Cloud-Diensten erhöhte Sicherheitsvorkehrungen zu treffen. Besondere Kategorien personenbezogener Daten unterliegen einem höheren Schutzbedarf als sonstige personenbezogene Daten und dürfen deswegen, aufgrund ihrer besonderen Sensibilität, nur verschlüsselt in Cloud-Diensten gespeichert werden. Es ist darauf zu achten, dass die Daten verschlüsselt werden, bevor sie auf dem Server des Cloud-Anbieters gespeichert werden. Die hierfür verwendeten Schlüssel dürfen dem Cloud-Anbieter nicht bekannt sein und müssen dem Stand der Technik entsprechen.

Es wird empfohlen, den Zugang zu Backup-Systemen, für die ein Cloud-Dienst genutzt wird, mit einer Zwei-Faktor-Authentifizierung abzusichern. Zur Ausgestaltung von Backups sollte die sogenannte „Großvater-Vater-Sohn-Backup-Regel“ berücksichtigt werden. Dies ermöglicht die Rücksicherung von Daten aus drei unterschiedlichen Generationen, falls dies benötigt wird.

Fazit: Die Nutzung eines Cloud-Dienstes zur Verbesserung der Backup-Strategie kann unter besonderer

Berücksichtigung der Vertraulichkeit mit geeigneten Schutzmaßnahmen realisiert werden. Entsprechende Nachweise sind vom Cloud-Anbieter vorzulegen und von der verantwortlichen Stelle zu dokumentieren.

Nutzung von Social Media und Software

Die datenschutzkonforme Nutzung von Social Media und von Software war im aktuellen Berichtszeitraum Gegenstand verschiedener Beschwerden, Datenpannenmeldungen und Beratungsanfragen von kirchlichen und diakonischen Einrichtungen.

Veröffentlichungen auf Social Media

Immer wieder kommt es zu Datenschutzverletzungen durch unzulässige Veröffentlichungen personenbezogener Daten auf Social Media. Diese Datenschutzverletzungen lassen sich in unterschiedliche Kategorien einteilen.

Offenlegung personenbezogener Daten bei der Personalgewinnung: In zahlreichen kirchlichen und diakonischen Einrichtungen wird Personalgewinnung auch über Facebook und Instagram betrieben. Dazu werden Beiträge veröffentlicht, die Einblicke in den Arbeitsalltag geben. Manchmal wird dabei nicht darauf geachtet, dass in den eingestellten Beiträgen auf abgebildeten Unterlagen oder Fotos keine personenbezogenen Daten erkennbar sein dürfen. Hier ist eine regelmäßige Sensibilisierung der jeweiligen Redakteure unerlässlich.

Veröffentlichung von Beschäftigtenfotos: Häufig werden in kirchlichen und diakonischen Einrichtungen im Rahmen der Öffentlichkeitsarbeit Fotos von Beschäftigten auf der Grundlage von Einwilligungen angefertigt und veröffentlicht. Dabei passiert es gelegentlich, dass Fotos auf Social Media veröffentlicht werden, für die keine Einwilligung zur Veröffentlichung auf Social Media vorliegt. Auch wenn entsprechende Einwilligungen vorliegen, müssen nach einem Widerruf der Einwilligung veröffentlichte Fotos auf Social Media unverzüglich gelöscht werden.

Nutzung privater Smartphones von Beschäftigten: Gelegentlich wird festgestellt, dass Beschäftigte von kirchlichen oder diakonischen Einrichtungen mit ihren

privaten Smartphones z. B. Fotos anfertigten, auf denen Kinder, Patienten oder Heimbewohnende abgebildet sind. Häufig werden diese Fotos dann mit einem Messenger-Dienst an Dritte weitergeleitet. Solche Handlungen sind deutliche Datenschutzverletzungen. Diese Datenschutzverletzungen hat der BfD EKD zum Teil als Mitarbeitendenexzess eingestuft und den staatlichen Behörden zur weiteren Bearbeitung übermittelt. Unabhängig von datenschutzrechtlichen Konsequenzen ziehen solche Handlungen häufig auch arbeitsrechtliche Maßnahmen nach sich.

Einbindung von Social Media - Angeboten

Den BfD EKD erreichten vermehrt Anfragen zur Einbindung von Social Media - Angeboten auf der eigenen Homepage von kirchlichen Stellen. Wird dazu ein Link genutzt, ist das allein noch keine Verarbeitung im Sinne des Datenschutzes und eine Erläuterung in der Datenschutzerklärung der eigenen Homepage ist nicht notwendig.

Die Übermittlung personenbezogener Daten, wie z. B. der dynamischen IP-Adresse des Besuchers einer Homepage an einen Social Media - Dienst, erfolgt erst bei aktiver Nutzung des bereitgestellten Links. Der bewusste Wechsel auf die Website des Social Media - Dienstes durch Nutzen des Links stellt eine aktive Entscheidung des Ausführenden dar. Ab diesem Moment liegt die Verantwortung für das Einholen einer Einwilligung sowie eine eventuelle Erläuterung in der Datenschutzerklärung beim Social Media - Anbieter und nicht mehr bei der kirchlichen Stelle.

Werden aber die Funktionalitäten eines Social Media - Anbieters auf der Website einer kirchlichen Stelle eingebunden, findet eine Verarbeitung in der Verantwortung der kirchlichen Stelle statt. Solche Funktionalitäten können unter anderem das Einbinden eines YouTube-Films oder die Bereitstellung eines Like-Buttons für Facebook auf der eigenen Website sein.

Schon beim Ansehen des Videos oder beim Drücken des Like-Buttons werden personenbezogene Daten, wie z. B. die dynamische IP-Adresse der Nutzenden der Website, an den Social Media - Anbieter

weitergeleitet. Die Nutzenden der Website müssen in diesen Fällen vorher in die Übermittlung an die Social Media - Dienste einwilligen und über ihre Risiken durch den Betreiber der Website aufgeklärt werden.

Fazit: Sollen Social Media - Dienste über die eigene Website einer kirchlichen Stelle erreichbar sein, ist es ratsam, dafür einen Link zu nutzen.

Social Media auf privaten Endgeräten am Arbeitsplatz

Im Berichtszeitraum wurde der BfD EKD um Beratung gebeten, inwiefern eine rechtliche Verpflichtung besteht, dass verantwortliche Stellen regelmäßig Social Media - Dienste durchsuchen müssen, ob Mitarbeitende personenbezogene Daten anderer Personen (z. B. von Patientinnen oder Patienten, betreuten Personen oder von anderen Mitarbeitenden) widerrechtlich veröffentlicht haben.

Eine derartige rechtliche Verpflichtung gibt es nicht. Sie wäre auch praktisch gar nicht realisierbar. Verantwortliche Stellen müssen zur Vorbeugung aber angemessene technische und organisatorische Maßnahmen treffen. Dienstliche Daten sollten grundsätzlich nicht auf privaten Endgeräten verarbeitet werden. Messenger-Dienste und Social Media - Dienste dürfen nur auf der Grundlage entsprechender datenschutzkonformer Regelungen eingesetzt werden. Zudem muss regelmäßig eine Sensibilisierung und Schulung der Mitarbeitenden zu diesem Thema stattfinden.

Wenn verantwortliche Stellen konkrete Hinweise erhalten oder Verdachtsmomente vorliegen, muss die verantwortliche Stelle dem unverzüglich und umfassend nachgehen.

Gleiche Inhalte auf mehreren Social Media - Plattformen

Für die Erstellung von Inhalten und deren Veröffentlichung auf mehreren Social Media - Plattformen wird häufig eine spezielle Software eingesetzt. Sofern diese Anwendung als Cloud-Dienst angeboten wird, entsteht die Frage, ob diese Programme datenschutzkonform genutzt werden können. Der Einsatz kann problematisch sein. Das liegt an den Trackingfunktionen des Herstellers auf den verwend-

ten Servern und in der App. Einzelheiten finden sich dazu in der Regel in den Nutzungsbedingungen und der Datenschutzrichtlinie des Herstellers. Der Einsatz muss im Hinblick auf die Sensibilität der zu verarbeitenden Daten und des konkreten Einsatzzweckes im Einzelfall genauer geprüft und abgewogen werden. Dabei sind neben den Inhaltsdaten auch die personenbezogenen Daten der Mitarbeitenden für die Nutzung des Cloud-Dienstes zu berücksichtigen. Eine Datenminimierung durch das Einrichten eines Funktionsaccounts und das Aktivieren spezieller Add-ons zum Schutz vor Trackern minimieren einen Datenabfluss, auch wenn sie ihn nicht komplett verhindern können.

Fazit: Der Einsatz einer Software zur Erstellung von Inhalten auf mehreren Social Media - Diensten muss deshalb vor der Einführung konkret geprüft werden und erfordert Maßnahmen zum Schutz der Vertraulichkeit und Datenminimierung.

Einsatz von Programmen zur Fremdsprachenübersetzung

In vielen Arbeitsfeldern besteht die Notwendigkeit in einer fremden Sprache zu kommunizieren. Es gibt mittlerweile einige Angebote zur schnellen Übersetzung diverser Fremdsprachen ins Deutsche.

Den BfD EKD erreichte die Anfrage einer kirchlichen Einrichtung, ob sie das Produkt DeepL nutzen dürfe. Das Programm ist nicht in einer Offline-Version ohne jeglichen Datenabfluss verfügbar. DeepL wird in den Versionen Free und Pro angeboten, wobei die Version Pro deutlich datensparsamer arbeitet. Beispielsweise werden die Daten in der Version Free nicht sofort nach der Verarbeitung gelöscht. Positiv zu bewerten ist, dass die Verarbeitung der Daten grundsätzlich innerhalb eines Mitgliedstaats der Europäischen Union stattfindet, so dass mit der DSGVO ein verbindlicher und verlässlicher rechtlicher Rahmen vorgegeben ist. Den Datenschutzbedingungen ist auch zu entnehmen, dass eine Weitergabe der Daten an Dritte ebenfalls unterbleibt. Der Hersteller behält sich allerdings vor, die Daten für eigene Zwecke auszuwerten.

Sofern besondere Kategorien personenbezogener Daten betroffen sind, wird dazu geraten, diese auf offline zu betreibenden Alternativen zu verarbeiten.

Es muss genau geprüft werden, welche Daten tatsächlich betroffen sind. Anfragen wie z. B. Smalltalk über das Wetter sind anders zu beurteilen als die Übersetzung von Gesundheitsdaten, wie z. B. in Diagnosen oder Arztbriefen. Es ist darauf hinzuwirken, dass so wenig personenbezogene Daten wie möglich verarbeitet werden.

Fazit: In einem verbindlich festgelegten Rahmen ist die datenschutzkonforme Nutzung von Programmen zur Fremdsprachenübersetzung möglich.

Nutzung von Kita-Apps

Der BfD EKD erhielt mehrere Beschwerden von Eltern über die Verarbeitung personenbezogener Daten ihrer Kinder in Kita-Apps durch die betreuenden Kindertageseinrichtungen. Dabei ging es unter anderem um das Führen einer digitalen Anwesenheitsliste ohne Vorliegen einer Einwilligung. Beim eigenhändigen Check-In durch die Eltern waren in einer Übersicht Daten aller Kinder einsehbar, z. B. zu akuten Krankmeldungen. Die entsprechenden Sachverhalte wurden zum Anlass genommen, den Einsatz der Kita-App in den jeweiligen Kindertageseinrichtungen zu überprüfen. Für die Eltern war nicht ersichtlich, dass die Erfassung bestimmter personenbezogener Daten der Kinder auf einer Einwilligung als Rechtsgrundlage, die Erfassung anderer personenbezogener Daten aber auf gesetzlichen Rechtsgrundlagen beruhte.

Die vorgelegten Einwilligungserklärungen und Datenschutzinformationen entsprachen nicht den gesetzlichen Anforderungen aus §§ 11, 17 DSGVO. Eine angeforderte DSFA konnte nicht vorgelegt werden. Dies wurde damit begründet, dass eine extern durchgeführte allgemeine Schwellwertanalyse für die Kita-Software nur ein geringes Risiko ergeben habe.

In Abstimmung mit den Kita-Trägern wurden umfangreiche Hinweise zur Verbesserung der Einwilligungserklärungen und Datenschutzinformationen gegeben. Es wurde weiterhin klargestellt, dass für den Einsatz von Kita-Apps, die über die Kommunikation mit den Eltern hinausgehen, eine DSFA erforderlich ist, diese aber nicht allgemeingültig für die App erstellt werden kann, sondern auf die konkreten Daten-

verarbeitungsvorgänge in der jeweiligen Kita Bezug nehmen muss. Der Check-In-Prozess wurde verändert, so dass nur das befugte Kita-Personal die Daten eingeben und einsehen darf.

Datenpanne in Kita-App

Im Frühjahr 2024 veröffentlichte der Heise-Verlag in seinem Online-Portal aufgrund eines anonymen Hinweises einen Artikel über eine Datenpanne beim Anbieter der Kita-App Stay Informed. Infolge der Fehlkonfiguration eines freizugänglichen Webservers kam es zu dieser Datenpanne, bei der personenbezogene Daten in einem längeren Zeitraum über das Internet frei abrufbar waren.

Die Sicherheitslücke wurde umgehend nach Bekanntwerden vom Anbieter der App geschlossen und der Vorfall transparent aufgearbeitet. Über die Datenpanne informierte der Anbieter seine Auftraggeber und Nutzenden auch auf der eigenen Homepage. Der Anbieter unterstützte seine Kunden auch hinsichtlich der Datenpannenmeldungen. Alle Einrichtungen wurden informiert, inwieweit sie von der Datenpanne betroffen waren.

Die App ist in Deutschland weit verbreitet. Sie wird vor allem von Kindertageseinrichtungen, Schulen und Pflegeeinrichtungen genutzt und dient der Kommunikation mit Eltern und Angehörigen sowie dem Bereitstellen von Informationen und Terminen und bietet darüber hinaus eine Chatfunktion an. Der Anbieter bietet die App als „Software-as-a-Service“ an und schließt mit seinen Kunden einen Auftragsverarbeitungsvertrag ab. Von den ca. 9.000 Kunden in Deutschland unterliegen rund 2.000 dem EKD-Datenschutzgesetz.

Die Datenpanne betraf insbesondere Namen, Geburtsdaten, Adressen sowie besondere Kategorien personenbezogener Daten. Konkret handelte es sich um einen Datenabfluss von einem freizugänglichen Webserver des Anbieters. Auf diesem Server konnten Mitarbeitende der Einrichtungen und deren Träger mehr als 1.300 Dateien mit personenbezogenen Daten, insbesondere von Minderjährigen, einsehen und herunterladen. Zudem waren auf dem Server ca. 16.000 Bilder von Avataren frei verfügbar, die der Nutzung in der Chatfunktion

dienten. Bei den Bildern gab es auch Personenfotos im Original. Des Weiteren waren PDF-Dateien offen zugänglich, die die Einrichtungen als Anlage über die Chatfunktion der App mit Eltern austauschen konnten und teilweise sogar digitale Unterschriften enthielten.

Da die sogenannte Zusatzvereinbarung zum Auftragsverarbeitungsvertrag Bestandteil des Vertrages zwischen dem Anbieter und den kirchlichen Stellen war, ermöglichte dies dem BfD EKD als evangelische Aufsichtsbehörde tätig zu werden und mit dem Anbieter den Sachverhalt aufzuklären. Aufgrund der Vielzahl der zu erwartenden Datenpannenmeldungen hat der BfD EKD die betroffenen kirchlichen Stellen darum gebeten, Sammelmeldungen abzugeben. Darüber hat der BfD EKD alle Betroffenen auf seiner Homepage informiert.

Fazit: Es sollte ein Datenpannenmanagement mit klaren Verantwortlichkeiten und Kommunikationswegen etabliert und wiederkehrend überprüft werden.

Örtlich Beauftragte für den Datenschutz

Den BfD EKD erreichten im Berichtszeitraum einige Beratungsanfragen zur Bestellung und Haftung von örtlich Beauftragten für den Datenschutz.

Gemeinsame Bestellung von örtlich Beauftragten für den Datenschutz

Vor dem Hintergrund einer Beratungsfrage musste sich der BfD EKD mit der Frage beschäftigen, ob und wie örtlich Beauftragte für den Datenschutz für verschiedene verantwortliche Stellen in einer diakonischen Einrichtung oder in einer Landeskirche bestellt werden können, wenn örtlich Beauftragte Mitarbeitende einer der verantwortlichen Stellen in der diakonischen Einrichtung oder in einer Landeskirche sind. Gemäß § 36 Abs. 2 DSGVO kann sich eine Bestellung auf mehrere verantwortliche Stellen erstrecken.

Nur in den kirchlichen und diakonischen Stellen, zu denen ein Anstellungsverhältnis besteht, erfolgt eine interne Bestellung. Für andere kirchliche oder diakonische Stellen erfolgt eine externe Bestellung.

Die Leistungen sind dann gemäß § 36 Abs. 5 DSGVO vertraglich zu regeln. Dabei ist darauf zu achten, dass die vertraglich übertragenen Aufgaben für alle verantwortlichen Stellen, für die eine Bestellung erfolgt ist, innerhalb der vereinbarten Arbeitszeit erledigt werden können.

Aus §§ 36 ff DSGVO ergeben sich die Aufgaben und Pflichten von örtlich Beauftragten für den Datenschutz. Sie sollen die verantwortlichen Stellen und die Beschäftigten beraten, informieren und schulen. Gleichzeitig sollen örtlich Beauftragte für den Datenschutz die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme überwachen, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen. Auch können Datenschutzkoordinatoren in den einzelnen verantwortlichen Stellen die örtlich Beauftragten für den Datenschutz unterstützen und damit den Zeitaufwand pro Einrichtung reduzieren. Stets zu beachten ist, dass örtlich Beauftragte für den Datenschutz für jede einzelne verantwortliche Stelle durch die jeweilige diakonische oder kirchliche Einrichtung bestellt werden müssen.

Datenschutzniveau in kleinen kirchlichen Einrichtungen

In kleinen kirchlichen Einrichtungen, z. B. in Kirchengemeinden, die aufgrund ihrer geringen Beschäftigtenzahl die Voraussetzungen nach § 36 Abs. 1 DSGVO zur Bestellung von örtlich Beauftragten für den Datenschutz nicht erfüllen, stellt der BfD EKD immer wieder Probleme bei der Umsetzung der datenschutzrechtlichen Anforderungen fest. Regelmäßig gehen Beschwerden und Hinweise zu Datenschutzverletzungen in kleinen Kirchengemeinden ein. Diese betreffen Mängel beim Auskunftsrecht nach § 19 DSGVO, bei der Umsetzung von Widersprüchen bezüglich Veröffentlichungen im Gemeindebrief sowie unzulängliche Einwilligungen oder auch fehlerhafte Datenschutzerklärungen und nicht datenschutzkonforme technische Umsetzungen auf der jeweiligen Internetseite.

Das Fehlen von örtlich Beauftragten für den Datenschutz wirkt sich offensichtlich negativ auf das Datenschutzniveau aus. Durch umfangreichen Schriftverkehr, individuelle Videokonferenzen und

persönliche Beratungsgespräche vor Ort versucht der BfD EKD, die Beschäftigten und Ehrenamtlichen mit Hinweisen und Hilfestellungen zu unterstützen, um die festgestellten Defizite zu beseitigen.

Fazit: Jede Kirchengemeinde sollte auf das Fachwissen von örtlich Beauftragten für den Datenschutz zurückgreifen können. Den Landeskirchen wird empfohlen, Konzepte zu entwickeln, wie eine flächendeckende Versorgung sichergestellt werden kann, ohne dass jede Kirchengemeinde eigene örtlich Beauftragte für den Datenschutz bestellt.

Haftung von örtlich Beauftragten für den Datenschutz

Im Zusammenhang mit der Frage, ob Mitarbeitende von kirchlichen und diakonischen Einrichtungen auch für mehrere verantwortliche Stellen als örtlich Beauftragte für den Datenschutz bestellt werden können, schließt sich die Frage nach der Haftung von örtlich Beauftragten für den Datenschutz an.

Hierbei ist zu unterscheiden, ob es sich um interne Mitarbeitende handelt, die als örtlich Beauftragte für den Datenschutz bestellt werden, oder um externe Beauftragte. Intern bestellte örtlich Beauftragte für den Datenschutz haften als Mitarbeitende nur für Vorsatz und grobe Fahrlässigkeit. Extern bestellte örtlich Beauftragte für den Datenschutz profitieren nicht von dieser arbeitsrechtlichen Regelung.

Im Verhältnis der verantwortlichen Stelle, die den örtlich Beauftragten für den Datenschutz beschäftigt, und den weiteren verantwortlichen Stellen, die den örtlichen Beauftragten für den Datenschutz als externen Beauftragten bestellen, bedarf es einer Vereinbarung über die Haftungsübernahme zugunsten des Beschäftigten. Das Haftungsrisiko, das durch diese externe Bestellung entsteht, kann durch den Abschluss einer entsprechenden Versicherung reduziert werden.

Ausblick

Beim Blick nach vorne ...

... stimmen mich das Thema Datenschutz und der Umgang mit personenbezogenen Daten nachdenklich und ich bin mir unsicher, wohin sich das Thema in Europa, in Deutschland und in unserer Kirche bewegt. Drei Aspekte gehen mir dabei durch den Kopf:

- Immer wenn es in letzter Zeit um das Thema Bürokratieabbau geht, wird der Datenschutz als Beispiel für eine ausufernde Bürokratie genannt. Sicher: Manche im Datenschutzrecht angelegten Dokumentations- und Rechenschaftspflichten werden – vor allem in Deutschland – umfassend eingefordert und „gelebt“. Da gibt es einen Gestaltungsspielraum für Weniger. Aber geht es doch bei diesen Pflichten für verantwortliche Stellen nicht in erster Linie darum, lästige Formalia zu erfüllen, sondern darum, den Grundrechtsschutz von betroffenen Personen mit den Interessen der verantwortlichen Stellen abzuwägen und in Einklang zu bringen. Diesem Ziel verpflichtet müssen im staatlichen und kirchlichen Bereich sowohl die Gesetzgebung als auch die Verwaltung den Rahmen für einen bürokratieärmeren Datenschutz neu justieren.
- Immer häufiger wird die (angeblich ausbaufähige) Datennutzung als Gegenspieler zum (umfänglich vorhandenen) Datenschutz gesehen. Das ist zumindest missverständlich und zu kurz gegriffen, wenn nicht gar falsch. Unterstellt es nämlich, dass es beim Datenschutz nicht um die Datennutzung ginge. Davon kann keine Rede sein. Geht es doch beim Datenschutz immer um die Verarbeitung und somit auch um die Nutzung von personenbezogenen Daten. Allerdings ist seit dem sogenannten Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 das Recht des Einzelnen auf informationelle Selbstbestimmung als Schranke bei der Datennutzung zu beachten. Eine schrankenlose Nutzung von personenbezogenen Daten ist gerade nicht grundrechtskonform. Mit unterschiedlichen rechtli-

chen und praktischen Vergewisserungen werden sich diesem Ziel nationale und europäische – auch kirchliche – Gerichte weiterhin verpflichtet fühlen und somit rechtsfortbildend wirken.

- Und geradezu als zwanghafter Reflex ist man beim Umgang mit Zukunftstechnologien und Künstlicher Intelligenz häufig der Auffassung, dass deren Einsatz vom Datenschutz ausgebremst und behindert werden. Klar: Auf die Zukunft ausgerichtete Technologien bieten immer viele Chancen und Möglichkeiten, aber sie sind eben nicht frei von Schwächen und Risiken. Da ist der Datenschutz ein im Gesamtkonstrukt angelegtes Korrektiv. Und gerade der kirchliche Datenschutz kann neben den grenzenlos anmutenden Entwicklungs- und Innovationsmöglichkeiten noch eine andere Perspektive in den Diskurs bringen: Wollen wir beim Umgang mit personenbezogenen Daten wirklich alles zulassen, was technisch möglich und rechtlich erlaubt ist? Diese datenethischen Fragestellungen sollten wir als Kirche zukünftig noch hörbarer als in der Vergangenheit in die gesellschaftlichen Debatten einbringen.

Mit Blick nach vorne haben wir als kirchliche Datenschützer mit unserem Thema etwas beizutragen ... für eine schlankere und bürokratieärmere Gestaltung des Datenschutzes ... für eine offenere und aufgeschlossener, aber weiterhin grundrechtsbasierte Datennutzung und ... für einen verantwortungsbewussten, auf einer christlichen Datenethik basierenden Einsatz von Zukunftstechnologien. Lassen Sie uns diese Chancen gemeinsam nutzen!

<https://datenschutz.ekd.de>
