4. Tätigkeitsbericht
Berichtszeitraum 2021 und 2022

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

4. Tätigkeitsbericht

des Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland

für die Jahre 2021 und 2022

vorgelegt im Juni 2023

Redaktionsschluss 31. Mai 2023

Inhaltsverzeichnis

Vorwort

Datenschutz in Krisenzeiten – (mehr als) ein Garant für Grund- und Freiheitsrechte!?

Menschen erleben die momentanen Zeiten zunehmend als eine krisenhafte Zuspitzung unseres gesellschaftlichen Miteinanders. Eine Krise folgt auf die andere: Corona-Pandemie, Klimawandel, Krieg in Europa, Energieversorgung und Inflation. Da haben es Freiheits- und Grundrechte nicht immer ganz leicht in der gesellschaftlichen und politischen Debatte durchzudringen. Aber spätestens seit Inkrafttreten der Datenschutz-Grundverordnung, einer Fahrt aufnehmenden Digitalisierung und im Blick auf die Herausforderungen von Zukunftstechnologien und datenethischen Fragen hat sich das Bewusstsein für den Schutz von personenbezogenen Daten in Europa und in Deutschland weiter verfestigt. Auch wenn kritische Stimmen zum Datenschutz weiterhin vernehmbar sind, steht der Datenschutz als solcher nicht zur Disposition.

Im kirchlichen und diakonischen Bereich wird der Datenschutz in den letzten Jahren seit Inkrafttreten des EKD-Datenschutzgesetzes nach und nach auch als Chance gesehen, um neben rechtlichen, technischen und organisatorischen Aspekten beim Umgang mit personenbezogenen Daten einen zusätzlichen Mehrwert im Bereich Ethik und Qualitätsmanagement zu erzielen.

Am Ende des Berichtszeitraums für diesen Tätigkeitsbericht liegt das dritte Jahr der Corona-Pandemie hinter uns allen. Die Pandemie hatte im Berichtszeitraum viele Bereiche des gesellschaftlichen, privaten und beruflichen Lebens tief durchdrungen. Da überrascht es nicht, dass uns aus dem kirchlichen und diakonischen Leben wieder viele Fragen zum Datenschutz, Datenschutzbeschwerden und Datenpannenmeldungen im Zusammenhang mit der Corona-Pandemie erreichten. Geht es doch in der Pandemie häufig um die Verarbeitung personenbezogener Daten und bei Gesundheitsdaten dann sogar um die Verarbeitung besonders sensibler personenbezogener Daten. Gleichwohl haben wir uns diesmal entschieden der Corona-Pandemie im Kapitel III „Über die Themen bei Aufsicht und Beratung“ keinen eigenen Bereich einzuräumen. Zumal sich am Ende des Berichtszeitraums ein Ende aller pandemiebezogenen Maßnahmen und Regeln abzeichnete. Vielmehr finden Sie in diesem Tätigkeitsbericht bei einigen Themen im dritten Kapitel auch Fälle im Zusammenhang mit der Corona-Pandemie.

Zweifelsohne befördert durch die Pandemie sehen wir im Berichtszeitraum eine verstärkte Sensibilisierung beim Umgang mit Beschäftigtendaten und somit eine Zunahme an beratenden und aufsichtlichen Fällen im Bereich des Beschäftigtendatenschutzes. Wir haben deswegen dem Thema Beschäftigtendatenschutz im dritten Kapitel dieses Tätigkeitsberichts einen eigenen Bereich eingeräumt. Diese Sensibilisierung beim Umgang mit Beschäftigtendaten kann aus Sicht des Datenschutzes nur begrüßt werden. Arbeiten in den über 33.000 diakonischen Einrichtungen doch knapp 600.000 Personen und im Bereich der sogenannten verfassten Kirche knapp 240.000 Personen. Aber auch die Themen Videoüberwachung, digitale Kommunikation und alle Fragen zum technischen Datenschutz gewinnen in unserer Arbeit stetig an Bedeutung.

Dieser Tätigkeitsbericht versteht sich als Weiterentwicklung der bisher vom Beauftragten für den Datenschutz der EKD vorgelegten Tätigkeitsberichte für die Berichtszeiträume 2015/2016, 2017/2018 und 2019/2020. Dabei wurde erstmals das Kapitel I „Über die Entwicklungen im Datenschutz“ ergänzt um Entscheidungen der EKD-Kirchengerichte im Bereich Datenschutz. Das Kapitel II „Über den Beauftragten für den Datenschutz der EKD“ wurde 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 ist somit nochmal praxisbezogener, umfangreicher und technischer als im letzten Tätigkeitsbericht.

Und so ist auch zukünftig die gesetzliche Aufforderung im EKD-Datenschutzgesetz, jede einzelne Person davor zu schützen, dass sie durch den Umgang mit personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtig 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 2023

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 kirchliche als auch der staatliche 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 seiner novellierten Fassung in Kraft. Die Novellierung stand in engem Zusammenhang mit der europäischen Datenschutz-Grundverordnung (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.

Im Berichtszeitraum wurde das EKD-Datenschutzgesetz an verschiedenen Stellen inhaltlich geändert. So wurde § 50a DSG-EKD im Jahr 2021 neu eingefügt, der die Verarbeitung personenbezogener Daten zur institutionellen Aufarbeitung sexualisierter Gewalt rechtlich möglich macht. Aufgrund des neuen § 50a DSG-EKD sind weitere Änderungen in § 4 Nr. 22, § 7 Abs. 1 Nr. 11, § 13 Abs. 1 Nr. 11 sowie § 49 Abs. 4 Nr. 5 DSG-EKD erforderlich geworden. Im Jahr 2022 wurde in § 39 Abs. 3 DSG-EKD ein weiterer Satz eingefügt, der die Finanzierung des **Beauftragten für den Datenschutz der EKD** betrifft.

Neben den bereits vorgenommenen Änderungen ist in § 54 Abs. 4 DSG-EKD vorgesehen, dass das EKD-Datenschutzgesetz innerhalb von fünf Jahren zu überprüfen ist. Dieser Evaluationsprozess hat bereits begonnen und wird durch das Kirchenamt der EKD gesteuert. Das zuständige Referat hat im Jahr 2022 eine Arbeitsgruppe eingerichtet, die das EKD-Datenschutzgesetz umfänglich evaluiert und dann konkrete Gesetzesänderungen vorschlagen wird. Parallel wurde zur weiteren Abstimmung eine Resonanzgruppe gebildet, die über die Ergebnisse der Arbeitsgruppe berät, bevor der Gesetzesentwurf im Jahr 2024 in den Gesetzgebungsprozess der EKD eingespeist wird. Es ist geplant, dass der EKD-Synode im Jahr 2024 der Gesetzentwurf zur Beschlussfassung vorgelegt werden soll. In beiden Arbeitsgruppen sind Vertreterinnen und Vertreter der Landeskirchen und der evangelischen Datenschutzaufsichtsbehörden vertreten. In der Resonanzgruppe wirkt der Beauftragte für den Datenschutz der EKD, Herr Michael Jacob, selbst mit.

Gemäß Art. 91 Abs. 2 DSGVO können Kirchen, die umfassende Datenschutzregeln anwenden, eine unabhängige Aufsichtsbehörde spezifischer Art errichten. Im Bereich der evangelischen Kirche gibt es seit Anfang 2023 neben dem Beauftragten für den Datenschutz der EKD zwei weitere Aufsichtsbehörden. Mit dem zum 1. Oktober 2023 bevorstehenden Übergang der Datenschutzaufsicht für die Nordkirche wird es im Bereich der evangelischen Kirche neben dem Beauftragten für den Datenschutz der EKD noch eine weitere Aufsichtsbehörde für zwei Landeskirchen und zwei diakonische Landesverbände mit ihren Mitgliedseinrichtungen geben. Der Beauftragte für den Datenschutz der EKD übt die Datenschutzaufsicht in der evangelischen Kirche über weite Bereiche von Kirche und Diakonie aus. Über die Aufgabenerledigung des Beauftragten für den Datenschutz der EKD wird in Kapitel II und III dieses Tätigkeitsberichts ausführlich Rechenschaft abgelegt.

Seit 2019 ist der Beauftragte für den Datenschutz der EKD (BfD EKD) Beklagter in insgesamt 13 Verfahren vor dem erst- und zweitinstanzlichen Kirchengericht der EKD (gewesen). Die nachfolgende Übersicht vermittelt einen Überblick über Gegenstand und Ergebnis der bisher abgeschlossenen Verfahren:

- Der Kläger begehrte die Erteilung einer Datenschutzauskunft nebst Kopien gemäß § 19 DSG-EKD. § 19 DSG-EKD entspricht ganz überwiegend Art. 15 DSGVO mit der Ausnahme, dass kein Recht auf Kopien vorgesehen ist. Das erstinstanzliche Gericht sah darin einen Verstoß gegen Art. 91 DSGVO und füllte § 19 DSG-EKD mit Art. 15 Abs. 3 DSGVO auf. Hiergegen richtete sich die Revision des BfD EKD, die zurückgewiesen wurde.

- Der Kläger erblickte im Einrichten eines E-Mail-Autoresponders mit der Mitteilung seiner neuen E-Mail-Adresse einen Datenschutzverstoß durch den kirchlichen Arbeitgeber. Der BfD EKD lehnte ein aufsichtsbehördliches Einschreiten ab und teilte dem Kläger in einem Abschlussschreiben mit, dass keine weiteren Maßnahmen veranlasst werden. Der Kläger begehrte daher die kirchengerichtliche Feststellung des Vorliegens eines Datenschutzverstoßes. Die Klage wurde abgewiesen.

- Der Kläger erblickte in der Weitergabe einer Beschwerde durch eine Beschwerdestelle nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) an den Arbeitgeber einen Datenschutzverstoß. Der BfD EKD lehnte ein aufsichtsbehördliches Einschreiten ab und teilte der Gegenseite in einem Abschlussschreiben mit, es läge bereits keine Offenlegung vor. Der Kläger begehrte daher die kirchengerichtliche Feststellung des Vorliegens eines Datenschutzverstoßes. Die Klage wurde abgewiesen.

- In einem – von der Klägerin betriebenen – ehemaligen Krankenhaus wurden Patientenunterlagen offen gelagert. Der BfD EKD beanstandete Datenschutzverstöße förmlich. Die gegen die Beanstandung gerichtete Klage wurde durch einen Prozessvergleich modifiziert.

- Die kirchliche Stelle wurde im Wege einer Anordnung (Verwaltungsakt) gemäß § 44 Abs. 3 Nr. 6 DSG-EKD zur Herausgabe eines Protokolls einer Kirchenvorstandssitzung angehalten. Vorliegend stand der Anordnung jedoch bereits die Rechtskraft eines kirchengerichtlichen Urteils entgegen. Erledigung durch Anerkenntnisurteil.

- Der Kläger klagte gegen seinen ehemaligen Arbeitgeber vor dem Arbeitsgericht. Dieser legte Urkunden, die personenbezogene Daten des Klägers enthielten, im Rahmen dieses Verfahrens als Beweismittel vor. Der Kläger meinte, dieses stelle eine unzulässige Offenlegung dar. Der BfD EKD lehnte im Rahmen des Beschwerdeverfahrens ein aufsichtsbehördliches Einschreiten ab, wogegen der Kläger Feststellungsklage erhob. Die Klage wurde abgewiesen.

- Die Klägerin wandte sich im Rahmen einer Beschwerde an den BfD EKD. Sie war der Auffassung, ihr Arbeitgeber habe unzulässig Personaldaten gegenüber Dritten offengelegt. Der BfD EKD lehnte eine Beanstandung ab, da sich schon der Sachverhalt der Klägerin nicht verifizieren ließ. Die gegen die Abschlussmitteilung erhobene Klage hat die Klägerin zurückgenommen.

- Der Kläger wandte sich gegen den Einsatz der Videokonferenzsoftware Zoom durch eine beigeladene kirchliche Stelle. Der BfD EKD sah in diesem konkreten Fall den Einsatz in der zuletzt von der kirchlichen Stelle verwendeten Konfiguration als nicht datenschutzwidrig an. Gegen die entsprechende Abschlussmitteilung erhob der Kläger Verpflichtungsklage, die auf aufsichtsbehördliches Einschreiten gerichtet war. Das Verfahren wurde durch Prozessvergleich beendet.

- Der Kläger vertrat die Auffassung, dass die von ihm begehrte Datenschutzauskunft auf der Grundlage der Datenschutz-Grundverordnung zu erteilen sei. Eine Entscheidung in der Sache erfolgte nicht, da der Rechtsstreit nach Erteilung der Auskunft durch die verantwortliche Stelle übereinstimmend für erledigt erklärt wurde.

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 innerhalb von drei Jahren ab Inkrafttreten am 24. Mai 2018 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 Entschließungen 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 des Bundes und der Länder wurde im Berichtszeitraum durch Inkrafttreten des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) sowie durch Änderungen im Infektionsschutzgesetz und in den jeweiligen Corona-Schutzverordnungen der Länder weiterentwickelt.

Inkrafttreten des TTDSG

Am 1. Dezember 2021 ist das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten. Das Gesetz soll den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation sowie in Telemedien genauer regeln. Es enthält spezifische Datenschutzvorschriften für Anbieter von Telekommunikationsdiensten und Telemediendiensten. Das TTDSG setzt unter anderem Vorgaben aus der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) um. Daher gibt es seit dem 1. Dezember 2021 ein neues Telekommunikationsgesetz (TKG). Das bisherige Telemediengesetz (TMG) besteht in einer gekürzten Fassung fort. In beiden Gesetzen sind keine Datenschutzvorschriften mehr enthalten. Weitere Erläuterungen zur Anwendbarkeit und Beachtung des TTDSG durch kirchliche und diakonische Einrichtungen sind in Kapitel III dieses Tätigkeitsberichts enthalten.

Infektionsschutzgesetz

Das Infektionsschutzgesetz enthält Regelungen, die es kirchlichen und diakonischen Stellen ermöglichen, sie aber auch dazu verpflichten, Gesundheitsdaten von Beschäftigten, Besuchenden und weiteren Dritten zu erheben und zu verarbeiten. Während der Corona-Pandemie wurden regelmäßig neue Rechtsgrundlagen zur Verarbeitung von Gesundheitsdaten geschaffen, die zwischenzeitlich größtenteils wieder außer Kraft getreten sind. Zu den datenschutzrechtlich relevanten Änderungen im Infektionsschutzgesetz wird in Kapitel III dieses Tätigkeitsberichts ausführlich Stellung genommen.

Corona-Regelungen der Bundesländer

Neben dem Infektionsschutzgesetz waren in den Corona-Regelungen, die von den einzelnen Bundesländern erlassen wurden, weitere Rechtsgrundlagen für die Erhebung und Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Corona-Pandemie vorgesehen. Die Corona-Regelungen waren auch von den kirchlichen und diakonischen Einrichtungen zu beachten. So mussten beispielsweise die Kirchengemeinden zur Einhaltung der vorübergehend geltenden 2G-Regelung die personenbezogenen Daten der Gottesdienstbesuchenden kontrollieren und die Kindertageseinrichtungen und Schulen in evangelischer Trägerschaft die Corona-Testpflicht bei Kindern und Beschäftigten umsetzen. Welche praktischen Auswirkungen die Corona-Regelungen der Bundesländer aus datenschutzrechtlicher Sicht für kirchliche und diakonische Einrichtungen zur Folge hatten, wird in Kapitel III dieses Tätigkeitsberichts näher erläutert.

Datenschutzaufsicht des Bundes und der Länder

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist eine unabhängige eigenständige oberste Bundesbehörde für den Datenschutz und die Informationsfreiheit und wird seit Anfang 2019 von Prof. Ulrich Kelber geleitet. In dieser Funktion überwacht er im föderalen System Deutschlands gemäß § 9 Bundesdatenschutzgesetz (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 Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) beschäftigt sich mit aktuellen Fragen des Datenschutzes in Deutschland und nimmt zu ihnen Stellung. Die Datenschutzkonferenz besteht aus dem 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 Entschließungen zu wichtigen Entwicklungen und Themen im Bereich Datenschutz.

Datenschutzrechtsprechung staatlicher Gerichte

Im Berichtszeitraum sind grundlegende Urteile staatlicher Gerichte zum Datenschutz ergangen. Von besonderer Bedeutung ist ein Urteil des Bundesgerichtshofs (BGH) sowie zwei Urteile des Bundesarbeitsgerichts (BAG), die sich mit dem Auskunftsrecht von betroffenen Personen beschäftigen. Darüber hinaus hat sich das Verwaltungsgericht Hannover in einem Urteil inhaltlich mit Art. 91 DSGVO und der Anwendung eigenen Datenschutzrechts für Religionsgemeinschaften auseinandergesetzt.

Umfang des Auskunftsanspruchs

Im Urteil vom 22. Februar 2022 hat sich der BGH mit dem Umfang des datenschutzrechtlichen Auskunftsanspruchs auseinandergesetzt (BGH, Urteil vom 22.02.2022, Az.: VI ZR 14/21).

Hintergrund des Urteils ist die Klage eines Mieters, der geltend macht, dass der beklagte Vermieter seinen Anspruch auf Auskunft nicht vollumfänglich erfüllt hat. Vor der Geltendmachung des Auskunftsanspruchs hatte der Beklagte dem Kläger mitgeteilt, dass es eine Beschwerde gegen ihn wegen starker Geruchsbelästigung und Ungeziefer im Treppenhaus gegeben habe. Daher bat der Beklagte um einen Besichtigungstermin der Wohnung. Bei dem Besichtigungstermin wurde ein verwahrloster Zustand festgestellt und der Kläger zur Reinigung aufgefordert. Ein zweiter Besichtigungstermin fand nicht mehr statt, da die Wohnung zwischenzeitlich gereinigt wurde. Der Kläger verlangte anschließend bei dem Beklagten Auskunft darüber, wer sich über ihn beschwert hat. Der Beklagte hat die Auskunft mit der Begründung, den Hausfrieden wahren zu wollen, verweigert.

Wie auch schon in anderen Urteilen (z. B. BGH, Urteil vom 15.06.2021, Az.: VI ZR 576/19) geht der BGH auch in diesem Urteil von einem weiten Normenverständnis aus. Er stellt in seinem Urteil fest, dass grundsätzlich vollumfänglich Auskunft zu gewähren ist und der Anspruch potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnamen oder Beurteilungen umfasse. Vorausgesetzt wird, dass es sich um Informationen über die Person handelt, die den Anspruch geltend gemacht hat. Dabei ist es ausreichend, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist.

In Bezug auf den vorliegenden Sachverhalt nahm der BGH an, dass der Auskunftsanspruch des Klägers grundsätzlich auch den Namen desjenigen umfasst, der sich über ihn beschwert hat. Zu prüfen sei aber, ob dem Anspruch gegebenenfalls Rechte Dritter, hier desjenigen, der sich beschwert hat, entgegenstehen. Dies müsse im Rahmen einer Interessenabwägung festgestellt werden. Da die Vorinstanz diese Interessenabwägung nicht vorgenommen hatte, hob der BGH das Urteil der Vorinstanz auf und verwies die Sache an das Berufungsgericht zurück.

Bestimmtheit von Auskunftsansprüchen

Im Berichtszeitraum hat sich das BAG in der Entscheidung vom 27. April 2021 (BAG, Urteil vom 27.04.2021, Az.: 2 AZR 342/20) mit den Anforderungen an die Bestimmtheit eines geltend gemachten Auskunftsanspruchs beschäftigt. Hintergrund dieses Urteils war die Klage eines ehemaligen Mitarbeiters der Beklagten, dem

in der Probezeit gekündigt worden war. Der Kläger verlangte von der Beklagten unter anderem Auskunft über die gespeicherten personenbezogenen Daten sowie die Überlassung von Kopien von diesen Daten. Diese Ansprüche machte der Kläger unter Wiederholung des Gesetzestextes (Art. 15 DSGVO) geltend. Die Beklagte erteilte zwar Auskunft, überließ dem Kläger aber keine Kopien.

Das BAG entschied, dass der Klageantrag nicht hinreichend bestimmt sei und hob das vorinstanzliche Urteil auf. Ein Klageantrag unter bloßer Wiederholung des Wortlauts von Art. 15 Abs. 3 Satz 1 DSGVO sei nicht hinreichend bestimmt. Eine daraufhin ergehende Verurteilung sei nicht vollstreckbar. Daher sei eine Konkretisierung erforderlich.

Anders als der BGH, der die Ansicht vertritt, dass der Auskunftsanspruch auch durch die Zurverfügungstellung einer Kopie erfüllt werden könne und der Anspruch auf eine Kopie ein Unterfall des Auskunftsanspruchs darstelle, vertritt das BAG die Ansicht, dass der Auskunftsanspruch und der Anspruch auf eine Kopie zwei voneinander getrennte Ansprüche seien, die im Rahmen einer Stufenklage nach § 254 Zivilprozessordnung durchzusetzen sind.

Anforderungen an die Geltendmachung von Auskunftsansprüchen

In einer weiteren Entscheidung vom 16. Dezember 2021 (BAG, Urteil vom 16.12.2021, Az.: 2 AZR 235/21), setzte sich das BAG erneut mit den Anforderungen, die an die Bestimmtheit von Auskunftsansprüchen zu stellen sind, auseinander. Der zweiten Entscheidung lag eine Klage eines ehemaligen Mitarbeiters des Beklagten zugrunde, dem zuvor aufgrund verschiedener Vorwürfe gekündigt worden war. Nach der Kündigung hat der Kläger Kündigungsschutzklage eingelegt und zugleich Auskunft über die von seinem ehemaligen Arbeitgeber verarbeiteten und nicht in der Personalakte gespeicherten personenbezogenen Leistungs- und Verhaltensdaten verlangt.

Das BAG hat die Klage mangels hinreichend bestimmter Klageanträge als unzulässig abgewiesen. Die gestellten Klageanträge enthielten auslegungsbedürftige Begriffe. So bestünden bei den Parteien Zweifel, was unter Leistungs- und Verhaltensdaten zu verstehen sei.

„SELK-Urteil“

Im Berichtszeitraum ist ein weiteres bedeutsames Urteil des Verwaltungsgerichts Hannover (Urteil vom 15.12.2022, Az.: 10 A 1195/21) ergangen, dass sich inhaltlich mit Art. 91 DSGVO und der Anwendung eigenen Datenschutzrechts für Religionsgemeinschaften beschäftigt. Hintergrund des Urteils ist die Klage einer Religionsgemeinschaft, die geltend gemacht hat, nicht in den Anwendungsbereich der DSGVO zu fallen und eigene abweichende Datenschutzregeln erlassen zu dürfen und nicht unter die Aufsicht der Beklagten, der Landesbeauftragten für den Datenschutz Niedersachsen, zu fallen. Darüber hinaus vertrat die Klägerin die Ansicht, eine eigene unabhängige Aufsichtsbehörde spezifischer Art errichten zu dürfen.

Bei der Klägerin handelt es sich um die Selbständige Evangelisch-Lutherische Kirche (SELK), die in der Rechtsform einer Körperschaft des öffentlichen Rechts organisiert ist. Am 20. März 1993 erließ die Klägerin die „Richtlinie über den Datenschutz in der Selbständigen Evangelisch-Lutherischen Kirche“. Einen Tag vor dem Geltungsbeginn der DSGVO – am 24. Mai 2018 – beschloss die Klägerin eine neue „Richtlinie über den Datenschutz in der Selbständigen Evangelisch-Lutherischen Kirche“, die bis zum 24. Mai 2019 vorläufig galt. Die 14. Kirchensynode beschloss am 24. Mai 2019 eine neue Richtlinie zum Datenschutz, die im Wesentlichen dem EKD-Datenschutzgesetz vom 15. November 2017 entspricht. Diese trat am 1. August 2019 in Kraft. Darüber hinaus bestellte die Klägerin im Jahr 2019 einen örtlich Beauftragten für den Datenschutz, der zugleich als Aufsichtsbehörde fungierte.

Die Klägerin ist der Ansicht, dass sie eigenständige umfassende Datenschutznormen seit 1993 anwende, die im Jahr 2018 in Einklang mit der DSGVO gebracht worden seien. Auch habe die Klägerin eine Aufsichtsbehörde spezifischer Art eingerichtet und unterliege daher weder der DSGVO noch sei die Beklagte die zuständige Datenschutzaufsichtsbehörde der Klägerin.

Das Verwaltungsgericht Hannover hat die Klage als unbegründet abgewiesen. Zunächst hat das Gericht festgestellt, dass die Klägerin nicht berechtigt ist, nach Art. 91 Abs. 1 DSGVO eigene Datenschutzvorschriften anzuwenden. Die Klägerin habe zum maßgeblichen Zeit-

punkt keine umfassenden Datenschutzregeln im Sinne des Art. 91 Abs. 1 DSGVO angewandt. Maßgeblicher Zeitpunkt sei das Inkrafttreten der DSGVO am 25. Mai 2016. Zu diesem Zeitpunkt wandte die Klägerin noch die Datenschutzrichtlinie von 1993 an, die keine umfassenden Datenschutzregeln enthalten habe.

Gemäß dem Urteil liegen umfassende Datenschutzregeln einer Religionsgemeinschaft nur dann vor, wenn diese vollständig sind und nicht durch staatliche Regelungen ergänzt werden müssen. In der Datenschutzrichtlinie von 1993 fehlten jedoch beispielsweise vollständige Aussagen zum Anwendungsbereich sowie die wesentlichen Datenschutzgrundsätze. Auch waren keine konkreten Rechtsgrundlagen und Erlaubnistatbestände zur Verarbeitung von personenbezogenen Daten enthalten. Insofern stellte das Verwaltungsgericht Hannover fest, dass die Klägerin bis zum 24. Mai 2016 keine umfassenden Datenschutzregeln anwendete und Art. 91 Abs. 1 DSGVO daher nicht zur Anwendung kommt.

Darüber hinaus urteilte das Gericht, dass die Klägerin auch nach Inkrafttreten der DSGVO nicht berechtigt ist, eigene Datenschutzregeln zu erlassen. Die Regelungsbefugnis der Religionsgemeinschaften sei durch Art. 91 Abs. 1 DSGVO stark begrenzt und ermögliche nur in kleinem Umfang eigenständige Regeln. Dabei verwies das Gericht auf die beiden großen Kirchen, die ihr Datenschutzrecht bei der Neufassung in enger Parallelität zur DSGVO gestaltet haben. Zweck des Art. 91 DSGVO sei es, den bereits bestehenden Datenschutzvorschriften der beiden großen Kirchen weiterhin Geltung zu verschaffen. Mit Art. 91 DSGVO werde jedoch nicht der Zweck verfolgt, jeder Religionsgemeinschaft die Schaffung eigener Datenschutzvorschriften zu ermöglichen.

Abschließend stellte das Verwaltungsgericht Hannover fest, dass die Klägerin auch nicht berechtigt ist, eine unabhängige Aufsichtsbehörde spezifischer Art gemäß Art. 91 Abs. 2 DSGVO einzurichten. Dies könnten nur Religionsgemeinschaften, die Datenschutzregeln anwenden, die alle Voraussetzungen des Art. 91 Abs. 1 DSGVO erfüllen. Da die Klägerin diese Voraussetzungen nicht erfülle, falle sie unter die Datenschutzaufsicht der Beklagten.

Die von der Klägerin zugleich geforderte Vorlage verschiedener Fragen an den EuGH lehnte das Verwaltungsgericht Hannover ab. Es ließ aber die Berufung zu.

In der Europäischen Union

In der Europäischen Union waren im Berichtszeitraum im Datenschutz insbesondere die Datenübermittlung in Drittländer sowie die Weiterentwicklung des Auskunftsrechts wichtige Themen.

Europäisches Datenschutzrecht

In der Europäischen Union wurde das Datenschutzrecht im Berichtszeitraum durch Fragen zur Datenübermittlung in die USA, den Erlass neuer Standarddatenschutzklauseln sowie durch den Brexit geprägt und weiterentwickelt.

Datenübermittlung in die USA

Bereits im 3. Tätigkeitsbericht hat der BfD EKD umfänglich auf das sog. „Schrems II“-Urteil des EuGH (EuGH, Urteil vom 16.07.2020, Az.: C-311/18) und die sich daraus ergebenden Folgen für Datenübermittlungen in die USA hingewiesen. Auch im aktuellen Berichtszeitraum hat die Europäische Kommission keinen neuen Angemessenheitsbeschluss gefasst. Gleichwohl konnten Fortschritte in Bezug auf einen neuen Angemessenheitsbeschluss erzielt werden.

Am 7. Oktober 2022 hat US-Präsident Joe Biden das Dekret „Executive Order on Enhancing Safeguards für United States Signals Intelligence Activities“ unterzeichnet, das auf US-amerikanischer Seite die rechtliche Grundlage für einen neuen Rechtsrahmen zur Datenübermittlung in die USA schafft. In dem Dekret sind unter anderem Maßnahmen vorgesehen, die den Schutz von personenbezogenen Daten vor dem Zugriff durch US-amerikanische Geheimdienste stärken und das Datenschutzniveau in den USA verbessern sollen. Auf der Grundlage des Dekrets hat die Europäische Kommission nunmehr einen Entwurf eines Angemessenheitsbeschlusses zum Datenschutzrahmen EU-USA vorgelegt. Der Entwurf muss nun das Annahmeverfahren durchlaufen, nach dessen Abschluss die Europäische Kommission den endgültigen Angemessenheitsbeschluss annehmen kann. Das Annahmeverfahren kann sich über mehrere Monate hinziehen, sodass bislang nicht absehbar ist,

wann es einen neuen Angemessenheitsbeschluss für die Übermittlung von personenbezogenen Daten in die USA geben wird.

Neue Standarddatenschutzklauseln
Neben dem Entwurf eines Angemessenheitsbeschlusses hat die Europäische Kommission im Berichtszeitraum neue Standarddatenschutzklauseln zur Übermittlung von personenbezogenen Daten aus der Europäischen Union in Drittländer beschlossen und am 4. Juni 2021 veröffentlicht. Die neuen Standarddatenschutzklauseln unterscheiden sich sowohl im Aufbau als auch im Inhalt von den vorherigen Standarddatenschutzklauseln. So sind die neuen Standarddatenschutzklauseln in vier Module aufgebaut. Welches Modul im Einzelfall heranzuziehen ist, ist davon abhängig, ob die personenbezogenen Daten von einem Verantwortlichen an einen anderen Verantwortlichen, von einem Verantwortlichen an einen Auftragsverarbeiter, von einem Auftragsverarbeiter an einen anderen Auftragsverarbeiter oder von einem Auftragsverarbeiter an einen Verantwortlichen übermittelt werden.

Inhaltlich unterscheiden sich die neuen Standarddatenschutzklauseln von den Vorherigen dadurch, dass nun Garantien vorgesehen sind, die die Einhaltung der Klauseln durch den Datenimporteur sicherstellen und die Rechte der Betroffenen stärken sollen. So wurden die Informationspflichten des Datenimporteurs gegenüber dem Datenexporteur sowie gegenüber der betroffenen Person erhöht. Darüber hinaus ist der Datenimporteur verpflichtet, zu prüfen, ob zusätzlich zu den in den Standarddatenschutzklauseln vorhandenen Garantien weitere technische und organisatorische Maßnahmen zu ergreifen sind, um ein Schutzniveau herstellen zu können, das mit dem in der Europäischen Union vergleichbar ist.

Eine weitere Änderung hat sich auch im Hinblick auf die Verarbeitung von personenbezogenen Daten im Auftrag ergeben. So ist in Fällen, in denen sich der Auftragsverarbeiter in einem Drittland befindet, neben der Verwendung der Standarddatenschutzklauseln für die Übermittlung von personenbezogenen Daten in Drittländer kein zusätzlicher Auftragsverarbeitungsvertrag zu schließen. In Art. 1 Abs. 2 des Durchführungsbeschlusses 2021/914 ist ausdrücklich festgelegt, dass in den Standarddatenschutzklauseln auch die Rechte und Pflichten der Verantwortlichen und der Auftragsverarbeiter in Bezug auf die in Art. 28 Abs. 3 und 4 DSGVO genannten Fragen zur Übermittlung personenbezogener Daten von einem Verantwortlichen an einen Auftragsverarbeiter festgelegt sind. Dies gilt auch in Fällen, in denen personenbezogene Daten von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter übermittelt werden.

Um die dauerhafte Einhaltung der Klauseln sicherstellen zu können, ist in den neuen Standarddatenschutzklauseln geregelt, dass die Parteien eine sogenannte Datentransfer-Folgenabschätzung (DTFA) durchführen müssen. Dabei müssen die Parteien insbesondere die Umstände der Übermittlung, die geltenden Gesetze und Rechtsvorschriften des jeweiligen Drittlandes berücksichtigen sowie die Klauseln durch weitere vertragliche, technische und organisatorische Garantien ergänzen.

Brexit
Nach dem Austritt des Vereinigten Königreichs aus der Europäischen Union (Brexit), findet dort die DSGVO keine Anwendung mehr. Das Vereinigte Königreich ist somit ein Drittland im Sinne des § 10 DSG-EKD.

Am 28. Juni 2021 hat die Europäische Kommission zwei Angemessenheitsbeschlüsse gefasst, einen im Rahmen der DSGVO und einen im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung. Damit ist die Übergangsregelung, wonach eine Datenübermittlung personenbezogener Daten von der Europäischen Union in das Vereinigte Königreich nach dem Brexit zunächst nicht als Datenübermittlung in ein Drittland galt, außer Kraft getreten. Mit den Beschlüssen stellt die Europäische Kommission im Vereinigten Königreich ein gleichwertiges Datenschutzniveau wie in der Europäischen Union fest. Datenübermittlungen in das Vereinigte Königreich können damit auf § 10 Abs. 1 Nr. 1 DSG-EKD gestützt werden. Eine Besonderheit der Angemessenheitsbeschlüsse ist die Verfallsklausel: Beide Beschlüsse laufen vier Jahre nach ihrem Inkrafttreten aus. Während dieser Zeit hat die Europäische Kommission gemäß Art. 45 Abs. 4 DSGVO die Entwicklungen im Vereinigten Königreich fortlaufend zu überwachen und bei Bedarf Maßnahmen gemäß Art. 45 Abs. 5 DSGVO zu ergreifen.

Datenschutzaufsicht der Europäischen Union

Der Europäische Datenschutzbeauftragte (EDSB) ist die zuständige Datenschutzkontrollbehörde für alle EU-Organe und EU-Einrichtungen. 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 EU 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 Mitgliedstaaten und des Europäischen Datenschutzbeauftragten (EDSB).

Datenschutzrechtsprechung des Europäischen Gerichtshofs

Dem Europäischen Gerichtshof (EuGH) wurde im Berichtszeitraum eine auch für die kirchlichen und diakonischen Einrichtungen bedeutsame Frage zum Auskunftsanspruch vorgelegt. Der EuGH hat in seinem Urteil vom 12. Januar 2023 (Az.: C-154/21) über die vorgelegte Frage entschieden.

Dem Urteil ist ein Rechtsstreit zwischen einer Privatperson (Kläger) und der österreichischen Post (Beklagte) vorausgegangen. Der Kläger hat Anfang 2019 von der Beklagten Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten verlangt. Unter anderem bat er auch um Mitteilung, ob seine Daten gegenüber Dritten offengelegt wurden und wer die Empfänger konkret waren. Die Beklagte erteilte die Auskunft, jedoch ohne die konkreten Empfänger der personenbezogenen Daten des Klägers zu nennen.

Der Kläger bestritt daraufhin den Rechtsweg. Das erstinstanzliche Gericht sowie das Berufungsgericht wiesen die Klage mit der Begründung ab, dass Art. 15 Abs. 1 lit. c) DSGVO dem Verantwortlichen die Wahl einräume, ob der betroffenen Person die konkreten Empfänger oder lediglich die Kategorien betroffener Personen mitgeteilt werden. Der Kläger legte daraufhin Revision beim Obersten Gerichtshof in Österreich ein. Der Oberste Gerichtshof wendete sich mit der Frage, wie Art. 15 Abs. 1 lit. c) DSGVO auszulegen ist, an den EuGH.

Der EuGH hat nun entschieden, dass ein Verantwortlicher, der personenbezogene Daten gegenüber Empfängern offengelegt hat oder noch offenlegen wird, verpflichtet ist, der betroffenen Person die Identität der Empfänger mitzuteilen. Dies folge unter anderem aus Erwägungsgrund 63, nach dem die betroffene Person ein Anrecht darauf habe, zu wissen, wer die Empfänger der personenbezogenen Daten sind. Auch sehe der Erwägungsgrund nicht vor, dass dieses Recht lediglich auf die Kategorien von Empfängern beschränkt werden kann. Darüber hinaus bestehe zwischen Empfängern und den Kategorien von Empfängern kein Vorrangverhältnis. Die betroffene Person müsse daher wählen können, ob sie Informationen über bestimmte Empfänger oder über Kategorien von Empfängern erhalten möchte. Letztlich weist der EuGH in seinem Urteil auf frühere Urteile hin, in denen der EuGH bereits entschieden hat, dass es betroffenen Personen durch Ausübung des Auskunftsrechts ermöglicht werden muss, zu prüfen, ob die sie betreffenden Daten richtig sind, in zulässiger Weise verarbeitet werden und ob sie gegenüber Empfängern offengelegt wurden, die zu ihrer Verarbeitung befugt sind. Die Geltendmachung weiterer Betroffenenrechte, wie beispielsweise das Recht auf Berichtigung und das Recht auf Löschung, mache es erforderlich, dass die betroffene Person die Identität der Empfänger kennt.

Ausnahmen von der Verpflichtung des Verantwortlichen, die konkreten Empfänger mitzuteilen, kommen nach Ansicht des EuGH nur in Betracht, wenn es nicht möglich ist, die Empfänger zu identifizieren oder wenn der Verantwortliche nachweisen kann, dass der Antrag auf Auskunft offenkundig unbegründet oder exzessiv ist.

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, die ihre Datenschutzaufsicht auf die EKD übertragen haben, 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. Im Berichtszeitraum haben vier Gliedkirchen und zwei diakonische Landesverbände die Datenschutzaufsicht weiterhin eigenständig wahrgenommen.

Überblick zur Datenschutzaufsicht in der EKD

Vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofes zur Unabhängigkeit von Datenschutzaufsichtsbehörden wurden mit der Novellierung des EKD-Datenschutzgesetzes 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 seit Januar 2014 die gleichnamige, unabhängige und eigenständige Behörde (BfD EKD) und übt für große Bereiche der evangelischen Kirche die Datenschutzaufsicht in Kirche und Diakonie aus. Dadurch wird die Datenschutzaufsicht innerhalb der evangelischen Kirche seit dem Jahr 2014 einheitlicher als in der Vergangenheit und in größeren Strukturen wahrgenommen. Im Berichtszeitraum haben vier Gliedkirchen und zwei diakonische Landesverbände die Datenschutzaufsicht weiterhin mit eigenen Behörden wahrgenommen. Der Beauftragte für den Datenschutz der Nordkirche – Herr Peter von Loeper – ist seit dem 1. Oktober 2018 und noch bis zur Übertragung der Datenschutzaufsicht der Nordkirche auf den BfD EKD zum 30. September 2023 der stellvertretende Beauftragte für den Datenschutz der EKD. Zum Jahresanfang 2023 ist auch die Datenschutzaufsicht der Evangelischen Kirche der Pfalz auf den BfD EKD übergegangen. Seit 1. September 2021 wird die stellvertretende Behördenleitung beim BfD EKD von Frau Sandra Coors wahrgenommen. Die IT-Leitung liegt bei Herrn Michael Tolk.

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 Jahr 2021 eine Schwerpunktprüfung im Bereich der Kindertageseinrichtungen begonnen und im Jahr 2022 abgeschlossen.

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 für 18 Gliedkirchen, die gliedkirchlichen Zusammenschlüsse und für dreizehn diakonische Landesverbände wahr. Seit dem 1. Januar 2014 haben die nachfolgenden Gliedkirchen und gliedkirchlichen Zusammenschlüsse sowie diakonischen Landesverbände die Datenschutzaufsicht auf die EKD übertragen:

- 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) (ab 1. Oktober 2023)
- Evangelisch-Lutherische Kirche in Oldenburg
- Evangelische Kirche der Pfalz
- Evangelisch-reformierte Kirche
- Evangelische Kirche im Rheinland
- 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 der Ev. Landeskirche in Baden e. V.
- Diakonisches Werk der Evangelisch-Lutherischen Kirche in Bayern e. V.
- Diakonisches Werk Berlin-Brandenburg-schlesische Oberlausitz e. V.
- Diakonisches Werk Bremen e. V.
- Diakonisches Werk Hamburg e. V.
- Diakonisches Werk in Hessen und Nassau und Kurhessen-Waldeck e. V.
- Diakonisches Werk Mecklenburg-Vorpommern e. V.
- Diakonisches Werk evangelischer Kirchen in Niedersachsen e. V.
- Diakonisches Werk der Ev.-Luth. Kirche in Oldenburg e. V.
- Diakonisches Werk der Evangelischen Kirche der Pfalz
- Diakonisches Werk Rheinland-Westfalen-Lippe e. V.
- Diakonisches Werk Schleswig-Holstein e. V.
- Diakonisches Werk der evangelischen Kirche in Württemberg e. V.

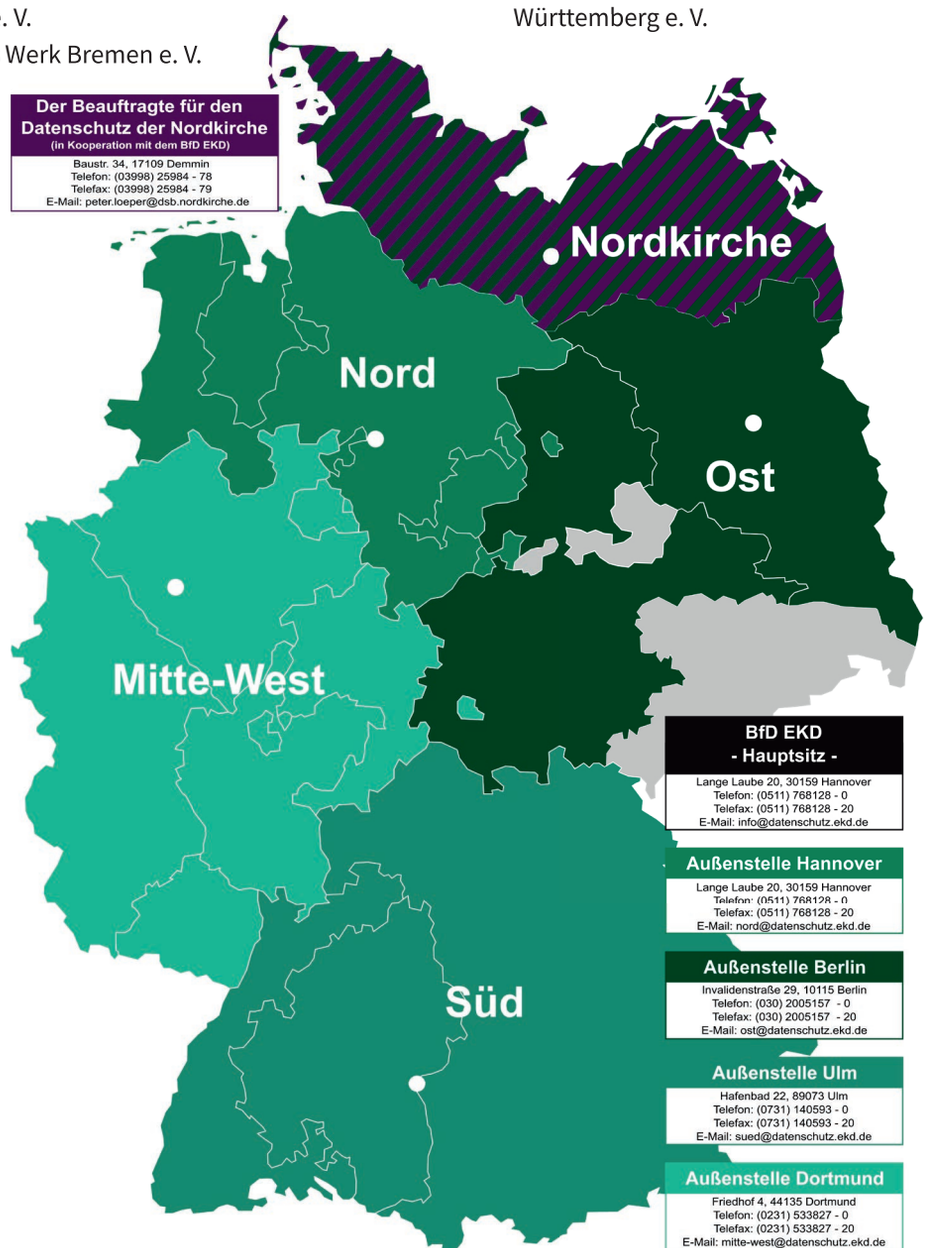

Abbildung 1: Karte mit Datenschutzregionen und Außenstellen
(Der Kooperationspartner Nordkirche ist schraffiert hinterlegt, da die diakonischen Landesverbände auf dem Gebiet der Nordkirche bereits zum 1. Januar 2022 die Datenschutzaufsicht übertragen haben. Die Nordkirche überträgt die Datenschutzaufsicht zum 1. Oktober 2023 auf den BfD EKD. Die übrigen Gliedkirchen mit eigenständiger Datenschutzaufsicht sind grau hinterlegt.)

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)“. Im Berichtszeitraum haben der Beauftragte für den Datenschutz der Nordkirche und der BfD EKD ihre Kooperation – mit dem Ziel der Übertragung der Datenschutzaufsicht der Nordkirche auf den BfD EKD – weiter vorangetrieben.

Organisation

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

Die Behörde hat insgesamt 23 (Plan-) Stellen. Alle Stellen sind zum 1. März 2023 besetzt. Alle vier Außenstellen sind mit mindestens einer oder einem Regionalverantwortlichen (volljuristische Qualifikation), einer IT-Sachbearbeitung und einer Teamassistenz besetzt. Im Berichtszeitraum konnten vakante Regionalverantwortlichen-Stellen in den Außenstellen Berlin, Ulm und Hannover sowie die Stelle der IT-Sachbearbeitung in der Außenstelle Dortmund erfolgreich wiederbesetzt werden. Am Hauptsitz in Hannover konnte erstmals sowohl eine Regionalverantwortlichen als auch eine Assistenzstelle sowie dauerhaft die Stelle der IT-Leitung und nach einer längeren Vakanz auch die Stelle für die Sachbearbeitung Finanzen besetzt werden. Die Auswahl von Mitarbeitenden erfolgte stets potenzial- und genderorientiert. Die Aufbauorganisation des BfD EKD zum 1. März 2023 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 ein Mitarbeitender vor Ort Leitungsverantwortung hat. Somit unterstehen alle Mitarbeitenden der Fach- und Dienstaufsicht des Behördenleiters.

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 Grundschutz 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 DSG-EKD (sog. „Verfahrensverzeichnis“)
- Diverse Hausverfügungen (z. B. zu Vertretungsregelungen, Zeichnungsbefugnissen, Beschaffungsentscheidungen etc.)
- Diverse Prozessbeschreibungen (zur Etablierung eines Qualitätsmanagementsystems)
- Styleguide

Auch das IT-Sicherheitskonzept des BfD EKD ist im Berichtszeitraum kontinuierlich fortgeschrieben worden. Um die Anforderungen und Standards aus dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu gewährleisten, erfolgte ein Upgrade auf ein neues Informationsmanagementsystem (ISMS). Der Datenbestand aus dem Altverfahren wurde in das neue System migriert. Ziel ist es, einen Grundschutz nach dem BSI Grundschutz Kompendium zu erreichen.

Abbildung 2: Organigramm des BfD EKD

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

Personal

Mit dem Ziel, den Aufgabenbereich Personal stärker selbst wahrzunehmen, hat der BfD EKD im Berichtszeitraum den Ablauf und die Zuständigkeiten für die Durchführung von Stellenbesetzungsverfahren neu geregelt. In diesem Zusammenhang wurde zusammen mit der Stabsstelle Chancengerechtigkeit im Kirchenamt 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. So nahm der BfD EKD im Jahr 2020 erfolgreich an der vom Kirchenamt initiierten Auditierung zum Thema „Vereinbarkeit von Beruf und Familie“ teil. Im Rahmen der Auditierung wurden die bestehenden Arbeitsbedingungen besprochen und Zielvereinbarungen für die nächsten drei Jahre getroffen. Einige der getroffenen Zielvereinbarungen konnten bereits im Berichtszeitraum erfolgreich umgesetzt werden. 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.

Im Sinne einer kontinuierlichen Personalentwicklung nehmen alle Mitarbeitenden regelmäßig und bedarfsgerecht an fachlichen sowie persönlichen Weiterbildungsmaßnahmen teil. 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 auch in der Vergangenheit – von der Abteilung Finanzen im Kirchenamt der EKD unterstützt. Die praktische Umsetzung und Abwicklung erfolgte zumeist unmittelbar durch die Behörde des BfD EKD. Die Personal- und Sachkosten des BfD EKD werden durch eine Finanzumlage derjenigen finanziert, die die Datenschutzaufsicht vereinbarungsgemäß oder auf gesetzlicher Grundlage auf die EKD übertragen haben.

Der Finanzbeirat der EKD hat im September 2022 den Finanzbedarf der Behörde für Personal- und Sachkosten für das Jahr 2023 neu festgelegt. Grundlage des Finanzbedarfs ist die mittelfristige Finanzplanung 2030 des BfD EKD, die sich in den Prozess zur Neuorientierung der Finanzstrategie der EKD einordnet und ständig fortgeschrieben und angepasst wird. Der so festgestellte Finanzbedarf des BfD EKD wird zu zwei Dritteln auf den Bereich der verfassten Kirche und zu einem Drittel auf den Bereich der Diakonie umgelegt. Die Höhe der Umlage errechnet sich im Bereich der verfassten Kirche neben einem Sockelbetrag jeweils zur Hälfte auf der Grundlage des Schlüssels Gemeindegliederzahlen und des Schlüssels Beschäftigtenzahlen. Im Bereich der Diakonie werden die Umlagen nur auf der Grundlage des Schlüssels Beschäftigtenzahlen ermittelt. Diese nach unterschiedlichen Schlüsseln errechnete Umlage muss erst nach der tatsächlichen Übertragung der Datenschutzaufsicht auf die EKD erbracht werden. Nach einer entsprechenden Gesetzesänderung wird im Juni 2023 erstmals der Rat der EKD auf Empfehlung des Finanzbeirats den Finanzbedarf des BfD EKD festlegen und beschließen.

Um die Finanzmittelverwendung auch im Hinblick auf den Prozess zur Neuorientierung der Finanzstrategie der EKD noch transparenter und nachvollziehbarer zu gestalten, professionalisiert die Behörde fortwährend ihr Handeln in Finanz- und Haushaltsangelegenheiten. Diese Neustrukturierung sorgt für eine detailliertere Darstellung aller Erträge und Aufwendungen des BfD EKD im Haushaltsplan der EKD. Einzelheiten sind den Haushaltsplänen und Haushaltsabschlüssen der EKD zu entnehmen.

IT-Infrastruktur und Kommunikation

Im Bereich der vorhandenen technischen Infrastruktur sorgten das eigenständige IT-Konzept des BfD EKD, die damit verbundene zentrale Terminalserverlösung sowie die Ausstattung der Mitarbeitenden mit mobilen Endgeräten dafür, dass die Arbeitsfähigkeit der Behörde während der Corona-Pandemie auch unter Bedingungen des Arbeitens im Homeoffice unmittelbar und ohne Einschränkungen aufrechterhalten werden konnte. Diese zentrale IT-Struktur ermöglicht ein ortsunabhängiges Arbeiten im (digitalen) Aktenplan, in dem nicht nur analoge, sondern auch digitale Informationen 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. So ist es allen Mitarbeitenden des BfD EKD möglich, mittels asymmetrischer Verschlüsselung (PGP) ihre E-Mail-Kommunikation zu sichern. Durch diese Verschlüsselung ist es auch jedem Außenstehenden möglich, über ein Webformular auf der Website Ende-zu-Ende-verschlüsselt mit der Behörde zu kommunizieren. Hierbei werden die entstehenden Metadaten zusätzlich durch eine Transportverschlüsselung gesichert. Alle Nutzenden eines eigenen PGP-Plug-Ins für ihren E-Mail Client können den öffentlichen PGP-Schlüssel des BfD EKD auf unserer Internetseite finden. Sollten Gesprächspartner keine Möglichkeit der Ende-zu-Ende-Verschlüsselung mittels PGP besitzen, können diese den BfD EKD auf herkömmliche Weise kontaktieren. In einem zweiten Schritt wird dann eine Ende-zu-Ende-verschlüsselte Kommunikation mit dem BfD EKD über den Dienst FTAPI ermöglicht.

Die Sicherstellung einer funktionierenden internen Kommunikation ist ein weiterer wichtiger Schlüssel zur Professionalisierung der Arbeit des BfD EKD. Für diesen Zweck wurden mehrere Kommunikationsinstrumente etabliert, um einerseits sicherzustellen, dass alle Mitarbeitenden die erforderlichen Informationen zur Aufgabenerledigung erhalten und um andererseits zu ermöglichen, dass die Behördenleitung einheitliche und verlässliche organisatorische und inhaltliche Absprachen mit den Mitarbeitenden treffen kann. Grundsätzlich finden alle zwei Monate hierarchieübergreifende Dienstbesprechungen statt. Dabei finden im Frühjahr und im Herbst jeweils zweitägige Klausurtagungen statt. Die Leitung der Dienstbesprechungen obliegt in der Regel der Behördenleitung. Zur Ergebnissicherung werden über die Dienstbesprechungen interne Protokolle erstellt.

Zum fachlichen Austausch finden zwischen den einzelnen Dienstbesprechungen regelmäßig Telefon- oder Videokonferenzen und Treffen unter den Mitarbeitenden mit der gleichen Funktion innerhalb der Behörde (Regionalverantwortliche, IT-Sachbearbeitende und Teamassistenz) statt. Davon unabhängig organisieren sich die Mitarbeitenden in den Außenstellen der Behörde eigenständig zum weiteren fachlichen und organisatorischen Austausch. In Zeiten der Corona-Pandemie hat der Austausch überwiegend im Rahmen von Telefon- oder Videokonferenzen stattgefunden. Ab April 2022 hat es auch wieder Treffen in Präsenz gegeben.

Der BfD EKD hat im Berichtszeitraum zur weiteren Digitalisierung der Behörde und zur Stärkung der standortübergreifenden Zusammenarbeit das Projekt „Digitalisierung“ initiiert und gestartet. Im Rahmen dieses Projektes wird der BfD EKD bis Ende 2023 ein softwarebasiertes Adress- und Veranstaltungsmanagement einführen und plant in einer zweiten Phase die Einführung eines Dokumentenmanagementsystems. Zudem soll im kommenden Berichtszeitraum die Telefonanlage ausgebaut werden, um die vorhandene Technologie Voice over IP (VoIP) vollumfänglich nutzen zu können und um dadurch 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

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 2021

	Aufsicht	Beratung	Weiterbildung	Gesamt
Hauptsitz	16	27	3	**46**
AS Hannover	74	69	5	**148**
AS Berlin	77	71	1	**149**
AS Ulm	165	288	1	**454**
AS Dortmund	159	210	3	**372**
Summe	**491**	**665**	**13**	**1169**

Tabelle 3: Statistik über die Anzahl der Tätigkeiten im Jahr 2022

	Aufsicht	Beratung	Weiterbildung	Gesamt
Hauptsitz	12	18	1	**31**
AS Hannover	84	52	6	**142**
AS Berlin	111	97	4	**212**
AS Ulm	190	200	3	**393**
AS Dortmund	150	168	4	**322**
Summe	**547**	**535**	**18**	**1100**

Tabelle 4: Statistik über die Anzahl der gemeldeten Datenpannen und eingegangenen Beschwerden in den Jahren 2021 und 2022

	2021	2022
Datenpannen	328	352
Beschwerden	163	195
Summe	**491**	**547**

Aufgaben und Tätigkeiten des BfD EKD ist der Matrix in Tabelle 1 auf Seite 23 zu entnehmen. Über die Anzahl der in den Jahren 2021 und 2022 bearbeiteten Vorgänge in den einzelnen Aufgabenbereichen geben die Tabellen 2 und 3 auf Seite 24 Auskunft.

Aufsicht

Im Bereich seines aufsichtlichen Handelns verzeichnet 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. Im Berichtszeitraum wurden eingehende Datenpannenmeldungen, Beschwerden und Eingaben ordnungsgemäß bearbeitet.

Aufgrund der gesetzlichen Anforderungen in § 43 und § 44 DSG-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 2021 startete der BfD EKD die erste Schwerpunktprüfung. Diese wurde in 100 zufällig ermittelten evangelischen Kindertageseinrichtungen durchgeführt. Die Abfrage in den betroffenen Kindertageseinrichtungen erfolgte im Rahmen eines Online-Fragebogens und wurde teilweise durch die Vorlage von Dokumenten und die Durchführung von Vor-Ort-Terminen ergänzt. Nach Ende der Abgabefrist lag die Antwortquote bereits bei 90 %. In Einzelfällen, in denen der Fragebogen nicht oder nicht vollständig ausgefüllt wurde, kam es zu einer Vor-Ort-Prüfung durch die jeweils zuständige Außenstelle. Pandemiebedingt wurden die Vor-Ort-Prüfungen per Videokonferenz durchgeführt. Die Anforderung der Dokumente und die abschließende Prüfung erfolgten in den jeweils zuständigen Außenstellen und endeten mit entsprechenden Abschlussschreiben an die geprüften Kindertageseinrichtungen. Mit der Veröffentlichung des Abschlussberichts auf der Internetseite des BfD EKD im September 2022 endete die erste Schwerpunktprüfung (https://datenschutz.ekd.de/ueber-uns/schwerpunktpruefungen/). Über die Ergebnisse der Schwerpunktprüfung wird in Kapitel III dieses Tätigkeitsberichts berichtet. Die nächste Schwerpunktprüfung wird der BfD EKD in den Jahren 2023 und 2024 in evangelischen Krankenhäusern durchführen.

Im Berichtszeitraum hat der BfD EKD im Rahmen einer ökumenischen Projektgruppe die Entwicklung des „Kirchlichen Datenschutzmodells“ (KDM) abgeschlossen. Mit dem KDM bietet der BfD EKD erstmals ein Tool zur praktischen Umsetzung von gesetzlichen Datenschutzanforderungen an. Das KDM bietet sowohl der Aufsichtsbehörde als auch den verantwortlichen Stellen sowie den örtlich Beauftragten für den Datenschutz in kirchlichen und diakonischen Einrichtungen ein Verfahren, welches auf systematische und reproduzierbare Weise die Umsetzung der kirchlichen Datenschutzvorgaben in konkrete technische und organisatorische Maßnahmen beschreibt. Das KDM basiert auf dem Standard-Datenschutzmodell (SDM) der Datenschutzkonferenz. Im April 2021 hat der BfD EKD die Internetseite für das Kirchliche Datenschutzmodell online gestellt (https://kirchliches-datenschutzmodell.de).

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
- Datenschutz im gemeindlichen Alltag
- Datenschutz im diakonischen Alltag
- Umgang mit Beschäftigtendaten
- Digitale Kommunikation in Videokonferenzen
- Videoüberwachung
- Datensicherheit, Verschlüsselung und Cookies
- Softwareprüfung und -bewertung
- Aufbewahrung und Löschung

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.

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 Entschließung, Häufig gestellte Fragen (FAQ), Handreichung, Kurzinformation, Kurzpapiere, Muster, Sensibilisierung und Stellungnahme zugeordnet. Die Verbreitung dieser Materialien erfolgt insbesondere über die Rubrik Infothek auf der Website des BfD EKD unter https://datenschutz.ekd.de/infothek/ und in Papierform.

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 DSG-EKD 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, die die Datenschutzaufsicht auf den BfD EKD übertragen haben. 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, die im Berichtszeitraum grundlegend überarbeitet wurden, wird eine Einführung in den rechtlichen und technischen Datenschutz sowie in die Organisation des Datenschutzes gegeben. Der Kostenbeitrag umfasst anteilig die vom BfD EKD erbrachten Leistungen inklusive Schulungsmaterial, Übernachtungs- und Verpflegungskosten. In den Jahren 2021 und 2022 betrug er 350,00 €. Für die Online-Seminare lag der Kostenbeitrag bei 180,00 €.

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. Der Kostenbeitrag umfasst anteilig die vom BfD EKD erbrachten Leistungen inklusive Schulungsmaterial, Übernachtungs- und Verpflegungskosten. In den Jahren 2021 und 2022 betrug er 350,00 €. Für die Online-Seminare lag der Kostenbeitrag bei 180,00 €.

Die Anzahl der in den Jahren 2021 und 2022 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. Die Datenschutz-Infotage richten sich an (künftige) örtlich Beauf-

tragte für den Datenschutz in kirchlichen und diakonischen Einrichtungen aus Landeskirchen und Diakonischen Landesverbänden, die die Datenschutzaufsicht auf den BfD EKD übertragen haben. 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 2021 wurden vier und im Jahr 2022 insgesamt fünf Datenschutz-Infotage durchgeführt. Die Hauptthemen waren im Jahr 2021 die Schwerpunktprüfung in Kindertageseinrichtungen, die Methodik des Kirchlichen Datenschutzmodells sowie die Datenübermittlung in Drittländer. Im Jahr 2022 standen die Ergebnisse der ersten Schwerpunktprüfung, die Umsetzung des Kirchlichen Datenschutzmodells sowie der Auskunftsanspruch und Aktuelles zum Beschäftigtendatenschutz im Vordergrund. Aufgrund der Corona-Pandemie wurden die Datenschutz-Infotage im Jahr 2021 ausschließlich online durchgeführt. Im Jahr 2022 fanden die Datenschutz-Infotage wieder regulär in Präsenz an den Standorten der Außenstellen des BfD EKD statt. Zusätzlich wurde ein online-Termin durchgeführt. An den Datenschutz-Infotagen nahmen in den Jahren 2021 und 2022 jeweils ca. 400 Personen teil.

Erfahrungsaustauschkreise

Vernetzung und Erfahrungsaustausch ist ein wichtiges Instrument, um örtlich Beauftragte für den Datenschutz in ihrer Arbeit zu unterstützen. Der BfD EKD schafft mit der Durchführung der Erfahrungsaustauschkreise (Erfa-Kreise) eine solche Möglichkeit. Die Erfa-Kreise ermöglichen den örtlich Beauftragten für den Datenschutz, sich datenschutzrechtlichen oder technischen Problemen und Themen fachlich zu nähern und dazu auszutauschen. Die Erfa-Kreise bieten auch die Möglichkeit sich mit anderen örtlich Beauftragten für den Datenschutz zu vernetzen, auch wenn die Vernetzung bei Online-Veranstaltungen nur eingeschränkt möglich ist. Außerdem soll genug Raum bleiben, um aktuelle Probleme oder konkrete Fragen zu besprechen. Die Erfa-Kreise richten sich an (künftige) örtlich Beauftragte für den Datenschutz in kirchlichen und diakonischen Einrichtungen aus den Gliedkirchen und Diakonischen Landesverbänden, die die Datenschutzaufsicht auf den BfD EKD übertragen haben. Die Regionalverantwortlichen und IT-Sachbearbeitenden der Außenstellen des BfD EKD moderieren die Erfa-Kreise. Die Erfa-Kreise werden in unregelmäßigen Abständen von den Außenstellen des BfD EKD angeboten. Die Termine werden zeitnah auf der Website des BfD EKD veröffentlicht. Im Berichtszeitraum fanden die Erfa-Kreise aufgrund der Corona-Pandemie ausschließlich

Tabelle 5: Statistik über die Anzahl der durchgeführten Grund- und Aufbauseminare im Jahr 2021

	AS Berlin	AS Dortmund	AS Hannover	AS Ulm	Nordkirche	Hauptsitz	Summe
Grundseminare 2021	1	1	1	1	1		**5**
Aufbauseminare 2021						5	**5**
Gesamt	**1**	**1**	**1**	**1**	**1**	**5**	**10**

Tabelle 6: Statistik über die Anzahl der durchgeführten Grund- und Aufbauseminare im Jahr 2022

	AS Berlin	AS Dortmund	AS Hannover	AS Ulm	Nordkirche	Hauptsitz	Summe
Grundseminare 2022	1	1	1	1	1		**5**
Aufbauseminare 2022						5	**5**
Gesamt	**1**	**1**	**1**	**1**	**1**	**5**	**10**

Tabelle 7: Statistik über die Anzahl der durchgeführten Erfa-Kreise in den Jahren 2021 und 2022

	AS Berlin	AS Dortmund	AS Hannover	AS Ulm	Summe
Erfa-Kreise 2021	2	2	2	4	**10**
Erfa-Kreise 2022	2	4	2	4	**12**
Gesamt	**4**	**6**	**4**	**8**	**22**

online statt. Für die Teilnahme an den Erfa-Kreisen fällt keine Gebühr an. Die Anzahl der durchgeführten Erfa-Kreise kann der Tabelle 7 auf dieser Seite entnommen werden.

Sensibilisierung

Daneben widmet sich der BfD EKD auch der Sensibilisierung von anderen Beschäftigten und (Leitungs-)Gremien zu datenschutzrechtlichen und -technischen Themen mit individuellen Vorträgen. Im Berichtszeitraum 2021/2022 hat der BfD EKD ungefähr 40 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.

Schwerpunktthemen

Neben den regulären Aufgaben (Aufsicht, Beratung, Weiterbildung) beschäftigt sich der BfD EKD mit dem Thema Datenschutz auch unter Berücksichtigung von vier Schwerpunktthemen (Kinder, Jugendliche und junge Erwachsene – Diakonie (Gesundheitsdatenschutz) – Ehrenamtliche – Mitarbeitende (Beschäftigtendatenschutz)). Jede Außenstelle bearbeitet ein Schwerpunktthema. Um der kirchlichen Datenschutzaufsicht somit auch zielgruppenorientiert gerecht zu werden, wurden im Berichtszeitraum mit diesen vier Schwerpunktthemen 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. In Kindertageseinrichtungen werden eine Vielzahl sensibler Daten verarbeitet. Daher wählte der BfD EKD diesen Bereich für seine erste Schwerpunktprüfung aus, die im Jahr 2021 gestartet ist und im September 2022 mit der Veröffentlichung des Abschlussberichts und des Prüffragebogens auf der Internetseite des BfD EKD abgeschlossen wurde. Geplant ist zudem eine Handreichung, die das Thema Datenschutz in Kindertagesstätten erneut aufgreift und erläutert. Außerdem wurde zur Sensibilisierung von Schülerinnen und Schülern ein Postermagazin mit dem Titel „Du siehst mich?!“ erstellt. 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. Im Berichtszeitraum hat der BfD EKD mehrere Vorträge zum Schwerpunktthema 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. Zentrales Thema war dabei die Verarbeitung von Gesundheitsdaten im Zusammenhang mit der Corona-Pandemie. In diesem Zusam-

menhang veröffentlichte der BfD EKD zwei Stellungnahmen zur Verarbeitung von Gesundheitsdaten von Beschäftigten. Für eine noch bessere und intensivere Zusammenarbeit innerhalb der evangelischen Kirche hat der BfD EKD im Berichtszeitraum die Fachgruppe Diakonie ins Leben gerufen, 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 2022 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 DSG-EKD. Im Berichtszeitraum hat der BfD EKD zum Thema Beschäftigtendatenschutz zwei Stellungnahmen (Stellungnahme zur Verarbeitung des Covid-19 Impfstatus und der Genesung im Beschäftigungsverhältnis aus datenschutzrechtlicher Sicht vom 7. Oktober 2021; Stellungnahme des Beauftragten für den Datenschutz der EKD zum 3G-Nachweis am Arbeitsplatz und zum einrichtungsbezogenen Immunitätsnachweis vom 15. März 2022) veröffentlicht und Vorträge gehalten. Zur Wahrnehmung des Schwerpunktthemas gehörte 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 an den Menschen 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 Datenschutzes nachvollziehen. Im Bereich Infothek können interessierte Personen die vom BfD EKD erstellten Materialien herunterladen. Viele 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:

- Entschließung
  - Entschließung der Konferenz der Beauftragten für den Datenschutz in der EKD zur Nutzung von Facebook-Fanpages durch kirchliche und diakonische Stellen vom 28. April 2022

- Häufig gestellte Fragen (FAQ)
  - Häufig gestellte Fragen zu Direktwerbung
  - Häufig gestellte Fragen zum TTDSG – Teil I
  - Häufig gestellte Fragen zum TTDSG – Teil II
  - Häufig gestellte Fragen zu gemeinsam verantwortlichen Stellen

- Muster
  - Vertrag zur Auftragsverarbeitung und Zusatzerklärung

- Stellungnahme
  - Stellungnahme zum 3G-Nachweis am Arbeitsplatz und zum einrichtungsbezogenen Impfnachweis vom 14. März 2022
  - Gemeinsame Stellungnahme der Konferenz der

Beauftragten für den Datenschutz in der EKD zur Datenübermittlung in die USA vom 15. Oktober 2021
- Stellungnahme zur Verarbeitung des Covid-19 Impfstatus und der Genesung im Beschäftigtenverhältnis aus datenschutzrechtlicher Sicht vom 6. Oktober 2021

Zudem veröffentlicht der BfD EKD seit 2017 in regelmäßigen Abständen eigene Pressemitteilungen. Im Berichtszeitraum wurden folgende eigene Pressemitteilungen veröffentlicht:
- Digitalisierung braucht Datenschutz, veröffentlicht am 28. Januar 2022
- 3G am Arbeitsplatz muss datenschutzkonform gestaltet werden, veröffentlicht am 24. November 2021
- BfD EKD legt 3. Tätigkeitsbericht vor, veröffentlicht am 24. Juni 2021
- Evangelische und katholische Datenschutzaufsichtsbehörden veröffentlichen „Kirchliches Datenschutzmodell“, veröffentlicht am 30. April 2021

Seit 2019 arbeitet der BfD EKD gemeinsam mit den katholischen Diözesandatenschutzbeauftragten in der katholischen Kirche an der Erstellung eines „Kirchlichen Datenschutzmodells“ (KDM). Am 30. April 2021 ist die separate Internetseite für das KDM online gegangen (https://kirchliches-datenschutzmodell.de). Dort können alle Interessierten das KDM und weitere Materialien herunterladen.

Kooperation mit der Aufsichtsbehörde der Nordkirche

Mit der Berufung von Herrn Peter von Loeper zum stellvertretenden Beauftragten für den Datenschutz der EKD zum 1. Oktober 2018 ist eine Kooperation mit der Aufsichtsbehörde der Nordkirche begründet worden. Seit dem Jahr 2019 werden die Seminare für örtlich Beauftragte für den Datenschutz in Kooperation mit dem Beauftragten für den Datenschutz der Nordkirche durchgeführt. Die Internetseite des Beauftragten für den Datenschutz der Nordkirche ist zum 1. Januar 2022 in der Internetseite des BfD EKD aufgegangen. Mustertexte, Merkblätter und Berichte für den Bereich der Nordkirche sind im Bereich „Vernetzung/Nordkirche“ auf der Internetseite des BfD EKD zu finden. Bei grundlegenden Datenschutzfragen stimmen beide Aufsichtsbehörden ihre Positionen und ihr Vorgehen miteinander ab. Zum 1. Januar 2022 wurde bereits die Datenschutzaufsicht für das Diakonische Werk Hamburg e. V., das Diakonische Werk Mecklenburg-Vorpommern e. V. und das Diakonische Werk Schleswig-Holstein e. V. auf den BfD EKD übertragen. Zum 1. Oktober 2023 wird auch die Datenschutzaufsicht der Nordkirche auf den BfD EKD übergehen.

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, die die Datenschutzaufsicht auf die EKD übertragen haben. Seit 2018 werden in jeder Datenschutzregion jährliche Treffen mit den Datenschutzreferentinnen und Datenschutzreferenten organisiert. Diese Treffen dienen dem fachlichen Austausch und haben im Berichtszeitraum als Online-Seminare stattgefunden. In den Jahren 2021 und 2022 nutzte der BfD EKD diese Treffen, um sich mit den Datenschutzreferentinnen und Datenschutzreferenten über die Arbeit in Zeiten von Corona und die Auswirkungen des EuGH Urteils „Schrems II“ auszutauschen sowie über das aufsichtliche Handeln des BfD EKD zu informieren. In diesem Zusammenhang informierte der BfD EKD über

den Stand der Schwerpunktprüfung in Kindertageseinrichtungen sowie über aktuelle Klagen gegen den BfD EKD.

Der BfD EKD steht auch in Erfüllung des gesetzlichen Auftrags zur Zusammenarbeit in regelmäßigem Kontakt zu den anderen Beauftragten für den Datenschutz innerhalb der EKD. Einmal im Jahr wird 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 2021 hat die Konferenz online stattgefunden. Im Jahr 2022 wurde die Konferenz wieder in Präsenz durchgeführt und hat in Berlin stattgefunden. Im Rahmen der Zusammenarbeit sind im Berichtszeitraum folgende Entschließung und folgende Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD erarbeitet und veröffentlicht worden:

- Entschließung der Konferenz der Beauftragten für den Datenschutz in der EKD zur Nutzung von Facebook-Fanpages vom 23. März 2022
- Gemeinsame Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zur Datenübermittlung in die USA vom 15. Oktober 2021

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 treffen sich 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 fokussierte sich die Zusammenarbeit vor allem auf das Projekt „Kirchliches Datenschutzmodell“, welches mittlerweile mit einem Bericht der Projektleitung auf dem Ökumenischen Datenschutztag im April 2023 abgeschlossen wurde. Die Weiterentwicklung des Modells und die Rezeption künftiger SDM-Versionen, wird zukünftig durch eine neue ständige 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. Dieser Kontakt soll weiterhin, auch 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 mit den spezifischen Aufsichtsbehörden teil. Zudem ist der BfD EKD Mitglied in den folgenden fünf Arbeitskreisen der Datenschutzkonferenz:

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

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 Datenerhebung und bei der Erfüllung von Auskunftsrechten vor Herausforderungen. Der BfD EKD beschäftigte sich daher im Berichtszeitraum mit diesem Themenkomplex sowohl im Rahmen von Datenschutzbeschwerden als auch im Zusammenhang mit verschiedenen Beratungsanfragen.

Positiver Corona-Test in Testzentrum öffentlich gemacht

Im Berichtszeitraum kam es wiederholt zu Beschwerden über Abläufe in kirchlich- oder diakonisch betriebenen Corona-Testzentren. So beschwerte sich beispielsweise ein Petent darüber, dass sein positives Testergebnis lautstark mündlich in der Öffentlichkeit von einem Mitarbeitenden geäußert worden sei. Hierbei handelte es sich um eine **unzulässige Offenlegung von Gesundheitsdaten**, für die es keine Rechtsgrundlage gab, so dass ein Datenschutzverstoß vorlag.

Im konkreten Fall wurde darüber hinaus festgestellt, dass in der kirchlichen Einrichtung keine ausreichenden **technischen und organisatorischen Maßnahmen** zum Schutz von personenbezogenen Daten umgesetzt wurden. Die verantwortliche Stelle hat aufgrund der Beschwerde die Mitarbeitenden ausführlich sensibilisiert und im Übrigen personalrechtliche Konsequenzen ergriffen, damit sich ein ähnlicher Vorfall nicht wiederholt.

Fazit: Gerade bei der Verarbeitung von Gesundheitsdaten ist darauf zu achten, dass die Verarbeitung diskret und vor einer Kenntnisnahme durch unberechtigte Dritte geschützt erfolgt. Zum Schutz der personenbezogenen Daten sind hohe Anforderungen an technische und organisatorische Maßnahmen zu stellen.

Aufforderung der Polizei zur Herausgabe einer Kontaktdatenliste

In einer Beratungsanfrage hat eine verantwortliche Stelle geschildert, dass sie während der Corona-Pandemie von der Polizei zur Herausgabe einer sogenannten Kontaktdatenliste – unter Androhung der Beschlagnahme als Beweismittel zur Aufklärung einer Straftat durch die Staatsanwaltschaft – aufgefordert wurde.

Auf **Grundlage der Corona-Regelungen der Bundesländer** waren während der Pandemie kirchliche und diakonische Stellen zeitweise verpflichtet, bestimmte personenbezogene Daten zu erheben und vorübergehend zu speichern. Die Corona-Regelungen der Bundesländer sahen aber ausschließlich vor, dass diese **Kontaktdatenlisten nur an die Gesundheitsämter** zum Zweck der Nachvollziehbarkeit von Infektionsketten und der Eindämmung der Verbreitung des Covid-19 Erregers herausgegeben und somit offengelegt werden durften. Die Nutzung der Kontaktdatenlisten außerhalb der Pandemiebekämpfung zum Beispiel zur Strafverfolgung war von diesem Zweck nicht umfasst. Für die Offenlegung der Kontaktdatenliste gegenüber der Polizei oder anderer Strafverfolgungsbehörden war auch keine andere Rechtsgrundlage ersichtlich. Aufgrund einer fehlenden Rechtsgrundlage wurde von der **Herausgabe der Kontaktdatenliste an die Polizei** oder an andere Strafverfolgungsbehörden ohne Beschlagnahme dringend **abgeraten**.

Fazit: Auch in einer pandemischen Ausnahmesituation dürfen personenbezogene Daten nur aufgrund einer Rechtsgrundlage erhoben und für die darin bestimmten Zwecke verarbeitet werden.

Mitwirkung Zensus 2022

Im Jahr 2022 wurde wieder ein Zensus – allgemein als **Volkszählung** bezeichnet – durchgeführt. In diesem Zusammenhang fragte eine diakonische Einrichtung an, ob sie die angeforderten Daten der Bewohner der Einrichtung übermitteln darf.

Durch den Zensus wird ermittelt, wie Menschen in Deutschland leben und arbeiten. Der Zensus liefert verlässliche Bevölkerungszahlen für die Kommunen, die Bundesländer und für Deutschland insgesamt. Neben ergänzenden Daten zur Demografie – wie zum Beispiel Alter, Geschlecht oder Staatsbürgerschaft – werden auch allgemeine Angaben zur Wohn- und Wohnraumsituation in Deutschland erfasst. In diesem Zusammenhang wurden auch Daten in sog. **Gemeinschaftsunterkünften** angefragt. Gemeinschaftsunterkünfte sind Einrichtungen, in denen Personen längerfristig untergebracht und versorgt werden. Personen, die in Gemeinschaftsunterkünften leben, führen in der Regel keinen eigenen Haushalt und werden in der Unterkunft durch deren Betreiber versorgt und betreut.

Zu Gemeinschaftsunterkünften zählen insbesondere

- Einrichtungen für Kinder und Jugendliche,
- Einrichtungen für Menschen mit Behinderung,
- Einrichtungen für Ältere und/oder Pflegebedürftige,
- Gemeinschaftsunterkünfte von Geflüchteten,
- Internate,
- Klöster
- Krankenhäuser (z. B. mit psychiatrischer Abteilung),
- Mutter- bzw. Vater-Kind-Einrichtungen,
- Sonstige sozialtherapeutische Einrichtungen und
- (Not-)Unterkünfte für Wohnungslose.

Die diakonische Einrichtung gilt als Gemeinschaftsunterkunft und durfte die Daten übermitteln, weil die Datenverarbeitung auf dem **Zensusgesetz**, also auf einer gesetzlichen Grundlage beruht. Einrichtungen sollten allerdings bei der Übermittlung darauf achten, dass die Daten verschlüsselt übermittelt werden.

Fehler beim Versenden von Fax und E-Mail

Bereits in der Vergangenheit hat der BfD EKD im Rahmen von Beratungsanfragen und Beschwerdeverfahren mehrfach auf die **Risiken**, die mit der Nutzung von Faxen und E-Mails einhergehen, hingewiesen. Gleichwohl gab es auch im aktuellen Berichtszeitraum zahlreiche Meldungen von Datenpannen, die bei dem Versenden von Fax und E-Mail aufgetreten sind. Hintergrund sind in der Regel **menschliche Fehler**, die meist durch **technische und organisatorische Maßnahmen** hätten verhindert werden können.

Bei dem **Versand von Fax und E-Mail** treten Datenpannen besonders häufig als Folge von **falsch eingegebenen Empfänger-Nummern** und **E-Mail-Adressen** auf. Auch die oft eingestellte Autovervollständigungsfunktion bei der Eingabe von E-Mail-Adressen in E-Mailprogrammen führt immer wieder dazu, dass versehentlich falsche E-Mail-Adressen ausgewählt werden. Diesen Risiken kann bereits durch einfache Maßnahmen – wie der nochmaligen Kontrolle der Faxnummer oder der E-Mail-Adresse nach der Eingabe, falls möglich im Vier-Augen-Prinzip – begegnet werden. Handelt es sich um einen Erstkontakt oder bestand längere Zeit kein Kontakt, empfiehlt der BfD EKD, sich von der betroffenen Person bestätigen zu lassen, dass die Faxnummer oder die E-Mail-Adresse (noch) korrekt ist.

Darüber hinaus wird bei dem **Versand von E-Mails** häufig auch versehentlich die **cc-Funktion** statt der **bcc-Funktion** genutzt. Mit dieser Funktion können E-Mails gleichzeitig an eine Vielzahl von Personen geschickt werden, wobei die E-Mail-Adressen aller Empfangenden bei der cc-Funktion gegenseitig zu sehen sind. Dies wird, sobald es über interne Mitteilungen hinausgeht, regelmäßig zum Problem. Zum einen wird die Offenlegung der E-Mail-Adressen an andere Empfangende grundsätzlich nicht erforderlich sein. Zum anderen kann unter Umständen aus dem Zusammenhang entnommen werden, wer beispielsweise Patient oder Patientin in einer Gesundheitseinrichtung oder ähnlichem ist. Daher ist grundsätzlich auf die bcc-Funktion zurückzugreifen, da dabei ein gegenseitiges Offenlegen der Empfängeradressen gerade nicht stattfindet.

Neben dieser unerlaubten Offenlegung von personenbezogenen Daten werden bei dem E-Mailversand personenbezogene Daten in vielen Fällen auch nicht ausreichend geschützt. So werden **Dokumente** mit personenbezogenen Daten häufig **unverschlüsselt** einer E-Mail angehängt. Das damit im Zusammenhang stehende Risiko, dass personenbezogene Daten von unberechtigten Dritten zur Kenntnis genommen werden, wird dabei nicht beachtet. Aufgrund dessen empfiehlt der BfD EKD, Unterlagen – insbesondere wenn diese besondere Kategorien personenbezogener Daten enthalten – nur verschlüsselt per E-Mail zu versenden. Alternativ kann – in Fällen, in denen Dokumente lediglich intern versendet werden sollen – ein geschütztes Verzeichnis erstellt werden, in dem die entsprechenden Dokumente abgelegt werden und auf das nur berechtigte Personen zugreifen können. Ein Versand der Unterlagen per E-Mail ist dann nicht erforderlich. Stattdessen ist es ausreichend, an die berechtigten Personen eine E-Mail mit der Verknüpfung zu dem Verzeichnis zu senden.

Fazit: Den häufig auftretenden Fehlern bei der Versendung von Fax oder E-Mail ist durch entsprechende technische und organisatorische Maßnahmen entgegenzutreten, die das Risiko der Verletzung des Schutzes personenbezogener Daten auf ein Minimum reduzieren. Des Weiteren ist nach Möglichkeit auf verschlüsselte Verfahren auszuweichen, bei denen Risiken auf dem Übertragungsweg weitestgehend ausgeschlossen werden können.

Auftragsverarbeitung bei IT-Wartungsarbeiten

Regelmäßig erreichten den BfD EKD im Berichtszeitraum Anfragen, ob mit Dienstleistern, die IT-(Fern-)Wartungsarbeiten erbringen, ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) zu schließen ist.

Anders als in den Datenschutzgesetzen im staatlichen Bereich enthält das EKD-Datenschutzgesetz in **§ 30 Abs. 6 DSG-EKD** weiterhin die ausdrückliche Vorgabe, dass die Regelungen zur **Auftragsverarbeitung entsprechend** gelten, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen werden und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Hintergrund der Regelung ist, dass mit den Wartungsarbeiten regelmäßig der (zumindest potenzielle) Zugriff auf personenbezogene Daten der Auftraggeber einhergeht.

Grundsätzlich sind **AV-Verträge** abzuschließen, wenn Dienstleister genutzt werden, um zielgerichtet personenbezogene Daten für den Auftraggeber zu verarbeiten. Werden AV-Verträge wirksam abgeschlossen, gelten die Dienstleister datenschutzrechtlich nicht mehr als Dritte und verarbeiten die personenbezogenen Daten als Auftragsverarbeiter somit „intern“. Eine weitere Rechtsgrundlage ist dann für die Offenlegung der personenbezogenen Daten gegenüber dem Auftragsverarbeiter nicht erforderlich. Bei einem AV-Vertrag ist insbesondere notwendig, dass die Auftragsverarbeiter vertraglich verpflichtet werden, nur **nach Weisungen der Auftraggeber** mit den personenbezogenen Daten umzugehen und entsprechende **Sicherungsmaßnahmen** bei der Verarbeitung vorzuhalten.

Gleiches gilt gemäß § 30 Abs. 6 DSG-EKD für **IT-(Fern-)Wartungsarbeiten**, bei denen nicht zwangsläufig zielgerichtet auf personenbezogene Daten zugegriffen wird, aber in der Regel ein potenzieller Zugriff nicht ausgeschlossen werden kann. In der Praxis ist nun fraglich, wann diese Voraussetzungen erfüllt sind und wann auf den Abschluss eines AV-Vertrages verzichtet werden kann. Zu prüfen ist also nicht, ob die Dienstleistung die zielgerichtete Verarbeitung von personenbezogenen Daten betrifft, sondern ob deren **Kenntnisnahme bei Ausführung der Dienstleistung** möglich ist. Dies ist nicht auszuschließen, wenn Dienstleistern – wie bei der Wartung von Speicher- und Festplatten – in irgendeiner Weise Zugriff auf die IT-Systeme der Auftraggeber gewährt wird. Bei einer rein technischen Wartung der Infrastruktur ist der Anwendungsbereich von § 30 Abs. 6 DSG-EKD dagegen in der Regel nicht eröffnet. Dies ist beispielsweise bei der Wartung der Belüftung, Elektrik, Kühlung oder Heizung der Datenverarbeitungsanlagen anzunehmen. In diesen Fällen werden die Dienstleister in der Regel nicht als Auftragsverarbeiter tätig, sodass der Abschluss eines AV-Vertrags dann mangels tatsächlicher Offenlegung von personenbezogenen Daten entbehrlich ist.

Fazit: Grundsätzlich ist bei IT-(Fern-)Wartungsarbeiten der Abschluss eines AV-Vertrags erforderlich. Lediglich in Fällen, in denen ein Zugriff auf personenbezogene Daten sicher ausgeschlossen werden kann, ist der Abschluss eines AV-Vertrags nicht erforderlich. Die Entscheidung sollte gut dokumentiert sein.

Auskunft aus Gremienprotokollen zulässig?

Das Auskunftsrecht ist als zentrales Betroffenenrecht Gegenstand von vielen Beratungen und Beschwerden. So hat sich im Berichtszeitraum eine Petentin wegen der Weigerung einer Kirchengemeinde, Auskunft über den Inhalt von Protokollen des Kirchengemeinderats zu erteilen, an den BfD EKD gewandt.

Nach Prüfung des Sachverhaltes hat der BfD EKD festgestellt, dass die Kirchengemeinde die Auskunft zu Recht verweigert hat. Zwar lagen die Voraussetzungen für einen **Auskunftsanspruch nach § 19 Abs. 1 Satz 1 DSG-EKD** dem Grunde nach vor, da über die Petentin personenbezogene Daten durch die Kirchengemeinde verarbeitet wurden. Letztendlich stand der Auskunftserteilung aber eine **Ausnahme** nach **§ 19 Abs. 2 DSG-EKD** entgegen. Danach darf die Auskunft unter anderem nicht erteilt werden, soweit die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

Der von der Petentin beantragten Auskunft stand eine spezielle Rechtsvorschrift aus der landeskirchlichen Kirchengemeindeordnung entgegen. Danach sind – wie im konkreten Fall – Kirchengemeinderatssitzungen als **nichtöffentliche Sitzungen** durchzuführen, sofern der Verhandlungsgegenstand der Verschwiegenheitspflicht

unterliegt. **Niederschriften** von nichtöffentlichen Sitzungen des Kirchengemeinderates dürfen nur von Personen, die dem Kirchengemeinderat angehören, eingesehen werden. Die Kirchengemeinde hat die Auskunft über Protokollinhalte aus den nichtöffentlichen Sitzungen des Kirchengemeinderats gemäß § 19 Abs. 2 DSG-EKD zu Recht verweigert.

Fazit: Inhalte aus nichtöffentlichen Gremiensitzungen dürfen im Rahmen eines von einem Dritten geltend gemachten Auskunftsanspruchs nicht beauskunftet werden.

Interessenabwägung bei Auskunftserteilung

Der **Bundesfreiwilligendienst** ist ein Angebot an Frauen und Männer jeden Alters, sich außerhalb von Beruf und Schule für das Allgemeinwohl zu engagieren. Um einen Bundesfreiwilligendienst ableisten zu können, müssen sich die Interessierten bei einem **Träger** um einen Platz bei einer **Einsatzstelle** bewerben. Sofern die Bewerbung erfolgreich ist, sind die Bundesfreiwilligen für die Dauer des Freiwilligendienstes bei dem Träger tätig, der sie während des Einsatzes betreut und das Bindeglied zwischen ihnen und der Einsatzstelle darstellt. Die Bundesfreiwilligen sind verpflichtet, **regelmäßig Berichte** zu ihrem Einsatz zu verfassen und diese dem Träger zu übergeben. Immer wieder kommt es vor, dass in den Berichten auch Probleme geschildert werden, die nicht durch gemeinsame Gespräche oder eine Schlichtung durch den Träger gelöst werden können. In Einzelfällen kann der Wechsel der Einsatzstelle erforderlich sein. Als letztes Mittel kann der Einsatzstelle die Anerkennung – als Grundlage für die weitere Beschäftigung von Bundesfreiwilligen – entzogen werden.

Im Rahmen einer Beschwerde hatte sich eine Einsatzstellenleitung, der zuvor die Anerkennung entzogen wurde, an den Träger gewandt und eine **Auskunft** über die verarbeiteten personenbezogenen Daten verlangt. Zwar wurde die Auskunft erteilt, allerdings **ohne Berücksichtigung der Berichte der Bundesfreiwilligen**. Mit der daraufhin beim BfD EKD eingelegten Beschwerde rügte die Einsatzstellenleitung, dass ihr die Berichte vorenthalten und auch keine geschwärzten Berichte beauskunftet wurden.

Der Träger durfte sich bei der Auskunftserteilung – insbesondere auch vor dem Hintergrund seiner Fürsorgepflicht für die Bundesfreiwilligen – zu Recht auf eine gesetzliche Ausnahme berufen und die Auskunft einschränken. Der Träger berief sich auf eine Ausnahme von der Auskunftspflicht nach **§ 19 Abs. 2 DSG-EKD**. Bei der dabei vorzunehmenden **Interessenabwägung** waren das Interesse der Einsatzstellenleitung an einer vollständigen Auskunft gegen das Schutzinteresse der Bundesfreiwilligen abzuwägen. Der Träger ist dabei zu dem Ergebnis gelangt, dass der **Schutz der Bundesfreiwilligen höher zu bewerten** ist als das Auskunftsinteresse der Einsatzstellenleitung. Zu diesem Ergebnis kam der Träger unter anderem aufgrund der Tatsache, dass die Einsatzstellenleitung in der Vergangenheit bereits Schadensersatzansprüche gegen frühere Bundesfreiwillige geltend gemacht hatte und erneut mit der Geltendmachung von Schadensersatzansprüchen drohte. Aufgrund der geringen Anzahl von Bundesfreiwilligen bei der Einsatzstelle wäre bei Beauskunftung auch mittels geschwärzter Berichte über die jeweiligen Zeiträume und die jeweiligen Inhalte ein Rückschluss auf konkrete Bundesfreiwillige möglich gewesen. Der Träger hat die Interessen der Beteiligten sachgerecht gegeneinander abgewogen.

Fazit: Die Auskunftserteilung kann eingeschränkt sein, wenn im Rahmen einer Interessenabwägung schutzwürdige Interessen Dritter überwiegen.

Datenschutzerklärung auf der Internetseite

Im Rahmen von Beratungsanfragen wurde der BfD EKD von verantwortlichen Stellen wiederholt gebeten, die Datenschutzerklärung auf der eigenen Internetseite zu prüfen und Hinweise zu den gesetzlichen Anforderungen zu geben. Vereinzelt erhielt der BfD EKD im Berichtszeitraum auch Hinweise und Beschwerden über eine nicht datenschutzkonforme Ausgestaltung von Internetseiten Dritter. Auch im Zusammenhang mit sonstigen Beschwerden und Datenpannenmeldungen hat der BfD EKD regelmäßig die Internetseiten der verantwortlichen Stellen auf Datenschutzkonformität überprüft. Dabei wurden immer wieder **Mängel in den Datenschutzerklärungen** auf den Internetseiten der kirchlichen und diakonischen Einrichtungen festgestellt. Mit Inkrafttreten des neuen Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) am 1. Dezember 2021 wurden in zahlreichen Fällen weitere Anpassungen in den Datenschutzerklärungen auf den Internetseiten erforderlich.

Die Datenschutzerklärung dient gemäß § 17 DSG-EKD auch der **Erfüllung der Informationspflichten** in Bezug auf die Internetseite. Die Informationen müssen nach § 16 DSG-EKD präzise, transparent, verständlich und leicht zugänglich sein. Die Inhalte sollten also übersichtlich, kurz gefasst und konkret auf die betreffende Internetpräsenz zugeschnitten sein. Häufig nutzen kirchliche und diakonische Stellen frei im Internet verfügbare **Muster** oder **Generatoren** für Datenschutzerklärungen oder sonstige Mustervorlagen, ohne sie auf die individuellen rechtlichen und technischen Rahmenbedingungen anzupassen.

Bei den Überprüfungen wurde zum Beispiel festgestellt, dass sich viele Datenschutzerklärungen auf die DSGVO und nicht auf das EKD-Datenschutzgesetz und sich somit auf **falsche Rechtsgrundlagen** für die Datenverarbeitung beziehen. Daneben besteht in den Datenschutzerklärungen häufig ein großer Schwachpunkt in der **unzulänglichen Information über die konkreten Datenverarbeitungen**, die bei dem Besuch der Internetseite stattfinden. Dazu gehören zum Beispiel das Setzen von Cookies und die Einbindung von Drittanbieter-Ressourcen (z. B. Bilder, Scripte, Social-Media-Komponenten). Zahlreiche Internetseiten haben eine überlange Datenschutzerklärung, die Informationen zu den unterschiedlichen Social-Media-Anbindungen enthält, ohne dass auf der Internetseite tatsächlich solche Techniken genutzt werden. Häufig sind auch Standardtexte zur Cookie-Setzung enthalten, ohne dass diese im aufgeführten Umfang genutzt werden. In vielen Fällen werden auch personenbezogene Daten (zum Beispiel die IP-Adresse) an Drittanbieter übermittelt, ohne dass in der Datenschutzerklärung darüber informiert wird. Alle Datenübermittlungen an Drittanbieter sind vollständig und übersichtlich darzustellen. Dazu gehören ebenfalls Angaben über vorhandene Auftragsverarbeitungen bei durch Drittanbieter bereitgestellten Funktionen und Diensten auf der Internetseite. Sofern nach § 36 DSG-EKD örtlich Beauftragte für den Datenschutz zu bestellen sind, müssen entsprechende Kontaktdaten in den Datenschutzerklärungen enthalten sein. Diese Angaben fehlten manchmal vollständig. Teilweise wurde fälschlicherweise auch der BfD EKD als Kontakt angegeben. Es wird empfohlen in den Datenschutzerklärungen als Kontaktmöglichkeit zur oder zum örtlich Beauftragten für den Datenschutz, eine **E-Mail-Funktionsadresse** (z. B. datenschutz@domain.de) einzurichten. Auf eine **wortreiche Darstellung** von Begriffsdefinitionen, Gesetzestextauszügen und allgemeinen Selbstverständlichkeiten, die manchmal in den im Internet bereitgestellten Vorlagen enthalten sind, sollte aus Gründen der Übersichtlichkeit **verzichtet** werden.

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 der Kirchengemeinden im Berichtszeitraum immer wieder spezielle datenschutzrechtliche Fragestellungen ergeben.

Erfassung des Impfstatus bei Gottesdienstbesuchen

Die Corona-Pandemie und die damit im Zusammenhang stehenden ständigen Änderungen der gesetzlichen Grundlagen haben die kirchlichen Einrichtungen auch im aktuellen Berichtszeitraum vor große Herausforderungen gestellt. Nachdem Gottesdienste über einen längeren Zeitraum nicht mehr stattfinden durften, wurden diese schließlich unter Einhaltung bestimmter Sicherheitsvorkehrungen wieder zugelassen. Während im Berichtszeitraum 2019/2020 die Erfassung von Gottesdienstbesuchenden zur Nachvollziehbarkeit der Infektionskette im Vordergrund stand, erreichten den BfD EKD im Jahr 2021 vermehrt Anfragen – aber auch Beschwerden – zur Erfassung des Impfstatus der Gottesdienstbesuchenden.

So sahen die verschiedenen Corona-Regelungen, die zur Eindämmung der Corona-Pandemie von den Bundesländern erlassen wurden, vorübergehend vor, dass lediglich geimpfte oder genesene Personen (**sogenannte 2G-Regelung**) bestimmte Veranstaltungen besuchen durften. In einigen Bundesländern umfassten die Regelungen ausdrücklich auch den **Besuch von Gottesdiensten**. In anderen Bundesländern war dagegen festgelegt, dass die Kirchen ein mit den jeweils geltenden Corona-Regelungen vergleichbares Schutzniveau sicherstellen mussten. In diesen Fällen haben die Landeskirchen ebenfalls die Anwendung der sogenannten 2G-Regelung empfohlen. Aufgrund dessen waren die Kirchengemeinden vorübergehend dazu befugt und dazu verpflichtet, den **Impf- oder**

Genesenenstatus der Besucherinnen und Besucher zu **kontrollieren**. Welche Daten genau kontrolliert werden durften und wie die Kontrolle zu erfolgen hatte, ergab sich aus den meisten Corona-Regelungen jedoch nicht. Dies hat bei vielen Kirchengemeinden, aber auch bei vielen Gottesdienstbesuchenden zu Verunsicherungen geführt.

In vielen Fällen wurde die Umsetzung der 2G-Regelung daher nicht nur auf die Kontrolle des Impf- oder Genesenennachweises beschränkt, sondern auch darüberhinausgehende personenbezogene Daten **ohne Rechtsgrundlage** erfasst und gespeichert. So haben viele Kirchengemeinden aus praktischen Gründen den Impfausweis der Gottesdienstbesuchenden **einmalig kontrolliert** und den Impfstatus sowie den Namen der Besucherinnen und Besucher **dokumentiert** und **aufbewahrt**. Dadurch sollte verhindert werden, dass die Besucherinnen und Besucher bei jeder Gottesdienstteilnahme erneut kontrolliert werden müssen. Dieses Vorgehen war jedoch nicht von den Corona-Regelungen der Bundesländer umfasst. Diese erlaubten den Kirchengemeinden lediglich den Impf- oder Genesenennachweis der Besucherinnen und Besucher zu kontrollieren. Für eine darüberhinausgehende Verarbeitung von personenbezogenen Daten wäre eine weitere Rechtsgrundlage erforderlich gewesen. Eine Rechtsgrundlage zur Dokumentation und Speicherung der personenbezogenen Daten der Besucherinnen und Besucher sowie der Art des vorgelegten Dokuments ergab sich weder aus den Corona-Regelungen der Bundesländer noch aus dem EKD-Datenschutzgesetz.

Insofern kam eine derartige Verarbeitung von personenbezogenen Daten allein auf der Grundlage einer **Einwilligung** der betroffenen Personen in Betracht. Bezüglich der Einwilligung war zu beachten, dass die vorgelegten Dokumente **Gesundheitsdaten** der betroffenen Personen enthielten und insofern besonders sensibel waren. Der BfD EKD hat daher im Rahmen der Beratungsanfragen und der Beschwerdeverfahren auf § 13 Abs. 2 Nr. 1 DSG-EKD hingewiesen. Danach ist eine Verarbeitung von besonderen Kategorien personenbezogener Daten nur zulässig, wenn die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke **ausdrücklich** eingewilligt hat. Darüber hinaus wurde auf die sich aus § 11 DSG-EKD ergebenden Anforderungen für eine wirksame Einwilligung hingewiesen und es wurde empfohlen, die Einwilligungen im Sinne der Rechenschaftspflicht nach § 5 Abs. 2 DSG-EKD stets **schriftlich** einzuholen.

Filmen von Taufgottesdiensten

Im Zusammenhang mit der zunehmenden Digitalisierung und auch als Folge der im Berichtszeitraum weiterhin anhaltenden Corona-Pandemie haben viele Kirchengemeinden angefangen, **Gottesdienste zu filmen und die Videos anschließend im Internet zu veröffentlichen**. Dieses Vorgehen ermöglicht es Personen, die aus verschiedenen Gründen keinen Gottesdienst besuchen können oder möchten, an den Gottesdiensten ihrer Kirchengemeinde oder einer anderen Kirchengemeinde online teilzunehmen. Gleichwohl sind damit auch **Risiken für den Schutz der personenbezogenen Daten** – insbesondere der auf den Videos zu sehenden Personen – verbunden. Diese Risiken sind im Vorfeld von der Kirchengemeinde als verantwortliche Stelle im Sinne des § 4 Nr. 9 DSG-EKD zu ermitteln und zu bewerten. Aufgrund der bestehenden Risiken für den Schutz der personenbezogenen Daten haben den BfD EKD im Berichtszeitraum mehrere Beschwerden in Bezug auf das Filmen von Gottesdiensten und der anschließenden Veröffentlichung im Internet erreicht.

Im Rahmen eines Beschwerdeverfahrens hat eine Kirchengemeinde unter anderem auch Taufgottesdienste gefilmt und die Videos anschließend im Internet veröffentlicht. Da bei den Taufgottesdiensten auch die **Taufhandlung als solche gefilmt** wurde, waren auf den Videos nicht nur der Pfarrer oder die Pfarrerin, sondern auch das getaufte Kind, die Eltern sowie Verwandte und Freunde zu sehen. Die Kirchengemeinde hat die Eltern im Vorfeld über die Anfertigung und Veröffentlichung des Videos mündlich informiert. Eine Information an die Verwandten und Freunde ist jedoch nicht erfolgt. Lediglich an den Eingängen zur Kirche sowie zu Beginn des Gottesdienstes wurden die Teilnehmenden auf die Anfertigung und die Veröffentlichung des Videos hingewiesen. Im Zusammenhang mit der Prüfung der eingelegten datenschutzrechtlichen Beschwerde hat der BfD EKD festgestellt, dass die Kirchengemeinde sowohl durch die **Anfertigung** als auch durch die **Veröffentlichung des Gottesdienstvideos** gegen datenschutzrechtliche Vorschriften verstoßen hat. Es lag weder für die Anfertigung noch für die Veröffentlichung des Videos eine Rechtsgrundlage vor.

Allgemein ist bei der Aufzeichnung oder Übertragung von Gottesdiensten zunächst **§ 53 DSG-EKD** zu beachten. Eine Aufzeichnung oder Übertragung von Gottesdiensten ist demnach nur dann zulässig, wenn die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden. Für Gottesdienste, bei denen keiner der Gottesdienstbesuchenden auf dem Video zu erkennen und zu identifizieren ist, ist es in der Regel ausreichend, wenn die Teilnehmenden **vor Beginn des Gottesdienstes** auf die Anfertigung des Videos hingewiesen werden. Dies kann beispielsweise durch **Hinweisschilder** im Eingangsbereich der Kirche und auch durch einen entsprechenden **mündlichen Hinweis** vor Beginn des Gottesdienstes erfolgen.

Sofern die Gottesdienstbesucher jedoch auf den Videos zu erkennen sind, ist neben § 53 DSG-EKD noch eine **weitere Rechtsgrundlage** für die Anfertigung des Videos erforderlich. Als Rechtsgrundlagen für die Anfertigung des Videos kommen in diesen Fällen **§ 6 Nr. 4 in Verbindung mit § 6 Nr. 8 DSG-EKD** sowie die Einwilligung der betroffenen Personen in Betracht. Ob die entsprechenden Voraussetzungen im Einzelfall vorliegen, ist von der Kirchengemeinde als verantwortliche Stelle eigenständig zu prüfen und aufgrund der Rechenschaftspflicht aus § 5 Abs. 2 DSG-EKD auch zu dokumentieren.

In dem vorliegenden Beschwerdeverfahren lagen die Voraussetzungen von § 6 Nr. 4 in Verbindung mit § 6 Nr. 8 DSG-EKD nicht vor. Im Zusammenhang mit der dabei erforderlichen **Interessenabwägung** war zugunsten der Kirchengemeinde zu berücksichtigen, dass das Filmen von Gottesdiensten einem größeren Personenkreis die Teilnahme an dem Gottesdienst ermöglichte. Dazu war es jedoch nicht erforderlich, dass neben dem Pfarrer oder der Pfarrerin auch weitere Personen auf dem Video zu sehen sind. Darüber hinaus wurde in dem vorliegenden Beschwerdeverfahren ein Taufgottesdienst gefilmt, bei dem zusätzlich zu beachten ist, dass hier in der Regel **Minderjährige** betroffen sind, die einem erhöhten Schutz unterliegen. Insofern war in dem vorliegenden Fall davon auszugehen, dass die schutzwürdigen Interessen der betroffenen Personen das berechtigte Interesse der verantwortlichen Stelle überwiegen.

Eine wirksame **Einwilligung** aller auf dem Video zu sehenden Personen lag der Kirchengemeinde ebenfalls nicht vor, sodass die **Anfertigung des Videos** mangels Vorliegen einer Rechtsgrundlage **nicht rechtmäßig** erfolgt ist.

Auch die **Veröffentlichung des Taufgottesdienstes im Internet** ist vorliegend ohne Rechtsgrundlage erfolgt. Bezüglich der Veröffentlichung von Bildnissen, worunter auch Videos zu verstehen sind, sind neben dem EKD-Datenschutzgesetz die Regelungen des **Kunsturhebergesetzes** (KunstUrhG) zu berücksichtigen. Gemäß § 22 KunstUrhG ist für eine Veröffentlichung von Videos grundsätzlich eine **Einwilligung** der darauf zu sehenden Personen erforderlich. Lediglich bei Vorliegen der in § 23 KunstUrhG beschriebenen Voraussetzungen ist ausnahmsweise keine Einwilligung der betroffenen Person einzuholen. Eine **Ausnahme** nach § 23 KunstUrhG war in dem vorliegenden Beschwerdeverfahren nicht gegeben. Die Kirchengemeinde hätte daher von allen Personen, die auf dem Video zu sehen und zu erkennen gewesen sind, eine Einwilligung für die Veröffentlichung des Videos einholen müssen. Dies ist nicht erfolgt. Mangels Vorliegen einer Rechtsgrundlage hat die Kirchengemeinde auch durch die **Veröffentlichung des Videos** im Internet **gegen datenschutzrechtliche Vorschriften verstoßen**.

In diesem konkreten Beschwerdeverfahren lag somit weder eine Rechtsgrundlage noch eine Einwilligung der betroffenen Personen für die Anfertigung und Veröffentlichung des Taufgottesdienstvideos vor. Der BfD EKD hat daher eine Beanstandung ausgesprochen.

Fazit: Bei der Anfertigung und Veröffentlichung von Gottesdienstvideos sollte darauf geachtet werden, dass die Gottesdienstbesuchenden nicht auf dem Video zu erkennen sind. Sofern die Gottesdienstbesuchenden beispielsweise auf Tauf- oder Konfirmationsvideos zu sehen sind, ist die verantwortliche Stelle verpflichtet, zu prüfen, ob sowohl für die Anfertigung als auch für die Veröffentlichung des Videos eine Rechtsgrundlage gegeben ist. Sofern die Einwilligung der betroffenen Person erforderlich ist, ist darauf zu achten, dass die Anforderungen für eine wirksame Einwilligung eingehalten werden und die Einwilligung im Sinne der Rechenschaftspflicht schriftlich erfolgt und somit dokumentiert werden kann.

Veröffentlichung von Amtshandlungen und Geburtstagen im Internet

Immer wieder erreichten den BfD EKD Hinweise und Beschwerden über die Veröffentlichung von Amtshandlungen und Geburtsdaten in Gemeindebriefen, die im Internet veröffentlicht werden (**Internet-Gemeindebrief**).

Der Gemeindebrief ist für die Kirchengemeinden eine gute Möglichkeit über das gemeindliche Leben, Termine und Neuigkeiten zu berichten. Auch die **Amtshandlungen** (Taufen, Konfirmationen, Trauungen, Bestattungen) werden im Nachhinein häufig im Gemeindebrief veröffentlicht. Ebenso wird oft zu runden **Geburtstagen** und **Ehejubiläen** gratuliert. Mittlerweile wird der Gemeindebrief jedoch nicht mehr nur als Druckausgabe innerhalb der Kirchengemeinde verteilt, sondern vielfach auch auf den Internetseiten der Kirchengemeinden veröffentlicht. Hier gilt es die rechtlichen Unterschiede, die diese beiden Veröffentlichungsformen mit sich bringen, zu beachten.

Da der Internet-Gemeindebrief nicht nur die eigenen Gemeindeglieder erreicht, sondern einen **unüberschaubaren** Adressatenkreis hat, kann als Rechtsgrundlage für die Offenlegung der Amtshandlungen nicht auf § 8 Nr. 1 DSG-EKD und § 9 DSG-EKD zurückgegriffen werden. Auch die Rechtsgrundlagen zur Veröffentlichung von Geburtstagen und Ehejubiläen, die viele Landeskirchen geschaffen haben, greifen aufgrund des großen Adressatenkreises nicht beim Internet-Gemeindebrief. Sollen Amtshandlungen, Geburtstage oder Ehejubiläen im Internet veröffentlicht werden, ist zwingend eine **Einwilligung** der betroffenen Personen zur datenschutzkonformen Datenverarbeitung einzuholen. Diese Einwilligung muss die Voraussetzungen aus § 11 DSG-EKD erfüllen. Sie muss also insbesondere **informiert** und **freiwillig** erfolgen. Auch muss auf die jederzeitige Widerrufbarkeit der Einwilligung hingewiesen werden. Die **Schriftform** wird aufgrund des Nachweises der Rechenschaftspflichten gemäß § 5 Abs. 2 DSG-EKD und aus Gründen der Rechtssicherheit angeraten.

Spendenportale und digitale Zahlungswege

Bei größeren Spenden – bei denen die Gebenden in der Regel eine Spendenquittung erwarten und schon deshalb ihre Identität gegenüber den Empfangenden der Spende offenbaren – sind digitale Zahlungswege in Form von **bargeldlosen Überweisungen** schon lange die Regel. Im Berichtszeitraum haben den BfD EKD vermehrt auch Anfragen zur Datenschutzkonformität digitaler Zahlungswege über **Spendenportale** für Kleinspenden – etwa in Form der Kollekte während eines Gottesdienstes – erreicht.

Die Vermittlung bargeldloser Zahlungen von Kleinbeträgen wird von verschiedenen **Dienstleistern** angeboten, die ihre Dienste entweder Jedermann anbieten oder sich als Spezialanbieter für soziale und kirchliche Zwecke positionieren. Ziel des Einsatzes der „modernen“ Formen der Kleinspende war und ist eine erhöhte Resonanz in der Gruppe der „digital Natives“ zu erreichen, für die bargeldlose Zahlungen auch von kleinen Beträgen völlig normal sind. Weiterhin wird eine erleichterte und transparente Handhabung der Spendeneinnahmen erwartet.

Im Ergebnis hat der BfD EKD festgestellt, dass eine datenschutzkonforme Nutzung der Plattformen durchaus möglich ist. Durch die Verwendung des Portals durch den Spendenden einerseits und den Empfangenden (z. B. die Kirchengemeinde) andererseits kommt es in der Regel nicht zu einer Auftragsverarbeitung und auch nicht zu einem Vertragsverhältnis zwischen den Gebenden und den Empfangenden. Vielmehr agiert der Portalbetreiber als **selbstständige verantwortliche Stelle**, der sowohl mit den Gebenden als auch mit den Empfangenden eigene vertragliche Beziehungen eingeht. Auf der Geberseite ist die Verarbeitung der personenbezogenen Daten (z. B. Name und Kontoverbindung, von der abgebucht werden soll) durch die Notwendigkeit der Verarbeitung für die Erfüllung eines freiwillig geschlossenen Vertrages mit dem Portalbetreiber begründet. Auf der Empfängerseite kann die Verarbeitung personenbezogener Daten (etwa der Mitarbeitenden im Gemeindebüro) vermieden werden, wenn als Kontaktinformation eine dienstliche Funktionsadresse verwendet wird. Damit die Nutzung des Portals durch die Spendenden wirklich freiwillig erfolgt, muss allerdings eine alternative Methode, etwa die herkömmliche Bargeldsammlung, weiterhin angeboten werden

Fazit: Eine Nutzung von datenschutzkonformen Spendenportalen und digitalen Zahlungswegen ist möglich, wenn auch andere Zahlungswege angeboten werden.

Weitergabe einer Impfausweiskopie über den Masernimpfstatus an ein Gesundheitsamt

Den BfD EKD erreichte eine Beschwerde darüber, dass eine Kindertageseinrichtung eine Impfausweiskopie über den Masernimpfstatus eines Kindes an das zuständige Gesundheitsamt weitergegeben hat.

Die **Erhebung** des Nachweises über die Masernimpfung durch die Kindertageseinrichtung ist gemäß § 20 Abs. 9 IfSG zulässig. Eine **Offenlegung** des Nachweises ist von dieser Rechtsgrundlage allerdings nicht umfasst. Die Weitergabe einer Impfausweiskopie an das Gesundheitsamt stellt eine Offenlegung im Sinne von § 8 DSG-EKD dar. Eine **Rechtsgrundlage**, die eine Offenlegung der Gesundheitsdaten rechtfertigt, ist **nicht ersichtlich**. Auch wurden die Eltern über die Weitergabe weder informiert noch wurde eine Einwilligung eingeholt. Die verantwortliche Stelle teilte im Rahmen des Beschwerdeverfahrens mit, dass die Weitergabe der Daten vom Gesundheitsamt erwartet werde, um in einem Infektionsfall schneller handeln zu können. Eine schriftliche Aufforderung durch das Gesundheitsamt lag jedoch nicht vor. Da es sich zudem bei den Daten im Impfausweis um Gesundheitsdaten und somit um eine besondere Kategorie personenbezogener Daten handelt, ist ein sensibler Umgang mit diesen Daten dringend geboten.

Das Verhalten der Kindertageseinrichtung stellte einen **Datenschutzverstoß** dar und wurde durch den BfD EKD beanstandet. Die Kindertageseinrichtung wurde aufgefordert, künftig keine Daten mehr an das Gesundheitsamt weiterzugeben. Die Bundesländer empfehlen in ihren Merkblättern und Vordrucken lediglich zu dokumentieren, dass ein Nachweis über den Impfschutz bzw. die Tatsache, dass eine Impfung wegen medizinischer Kontraindikation nicht möglich ist, vorgelegt wurde. Der BfD EKD rät dringend, den Empfehlungen der Bundesländer zu folgen, keine Kopien anzufertigen und diese auch nicht an Dritte weiterzugeben.

Fazit: Bei der Erhebung des Nachweises über die Masernimpfung darf eine Kindertageseinrichtung keine Kopien anfertigen und diese auch nicht an Gesundheitsämter weitergeben.

Testpflicht in Kindertageseinrichtungen und Schulen

Mit Blick auf die hohen Corona-Infektionszahlen im Herbst/Winter 2021/2022 sahen die Corona-Regelungen der Bundesländer eine Testpflicht in Kindertageseinrichtungen und Schulen vor. Die Kinder mussten zuhause getestet werden und durften nur bei Vorliegen eines negativen Testergebnisses die jeweilige Einrichtung betreten. Für diesen Zweck wurden durch die Einrichtungen kostenlos sogenannte Selbsttests ausgegeben. Die Einrichtungen waren verpflichtet, die **Testergebnisse zu kontrollieren** und **zu dokumentieren**. Positive Fälle mussten **gemeldet** werden. Auch die Anzahl der ausgegebenen Tests musste zur Bedarfsabfrage erfasst werden. In vielen Einrichtungen wurden **Formulare** erstellt, die zur Dokumentation des Ergebnisses genutzt werden sollten. In einigen Fällen gab es Rückfragen zum Umfang der abgefragten Daten und zur Aufbewahrung der ausgefüllten Formulare.

Der **Umfang der abgefragten Daten** wurde durch die jeweils geltenden Corona-Regelungen und deren Ausgestaltung durch die Ministerien im Grunde vorgegeben. Einige Corona-Regelungen sahen vor, dass statt des Kindes auch eine andere im Haushalt lebende Person getestet werden darf. In diesen Fällen durfte lediglich dokumentiert werden, dass eine ersatzweise Testung einer im Haushalt lebenden Person stattgefunden hat. Der Name der Person und weitere personenbezogene Daten durften dagegen nicht erhoben und verarbeitet werden.

Bezüglich der **Aufbewahrung** wurde auf die allgemein geltenden Regelungen zur datenschutzkonformen Aufbewahrung hingewiesen. Konkret wurde empfohlen, die Formulare in abschließbaren Schränken in der Kindertageseinrichtung aufzubewahren, auf deren Schlüssel nur ein ausgewählter Personenkreis Zugriff hat. Auch beim Abgeben der ausgefüllten Formulare durch die Eltern in der Kindertageseinrichtung hat der BfD EKD darauf hingewiesen, dass die Formulare nur so entgegengenommen werden durften, dass eine Kenntnisnahme durch andere Personen ausgeschlossen werden konnte. Die Formulare sollten niemals unbeaufsichtigt im Eingangsbereich zurückgelassen werden.

Fazit: Für die Erfüllung der Testpflicht in Kindertageseinrichtungen und Schulen durften nur die personenbezogenen Daten der Kinder sowie der im Haushalt lebenden

Personen kontrolliert und dokumentiert werden, die in den Corona-Regelungen der Bundesländer vorgegeben wurden.

Exkurs: Schwerpunktprüfung in Kindertageseinrichtungen

In Erfüllung der Aufgaben der Datenschutzaufsichtsbehörden und der Vorgaben der Rechtsprechung des Europäischen Gerichtshofs führte der BfD EKD im Berichtszeitraum erstmalig Schwerpunktprüfungen durch. Eine Schwerpunktprüfung ist eine **anlasslose Prüfung in einem kirchlichen oder diakonischen Tätigkeitsfeld** mit dem Ziel der kontinuierlichen Verbesserung des Datenschutzes in der geprüften Einrichtung.

Für die ersten Schwerpunktprüfungen wurde der Bereich der Kindertageseinrichtungen ausgesucht. Dabei wurden EKD weit **100 evangelische Kindertageseinrichtungen** nach dem Zufallsprinzip für die Durchführung einer Schwerpunktprüfung ausgewählt. Die Schwerpunktprüfungen wurden mithilfe eines **onlinebasierten Fragebogens** durchgeführt. Der Fragebogen enthielt neben allgemeinen Fragen zum rechtlichen und organisatorischen Umfeld insbesondere auch Fragen zum technischen Umfeld. Jede geprüfte Kindertageseinrichtung bekam am Ende der Prüfung ein **individuelles Abschlussschreiben**. Diese Schreiben zeigten die Ergebnisse sowie die erkennbar gewordenen Mängel auf und gaben den Einrichtungen konkret umzusetzende Anforderungen und Empfehlungen an die Hand. Die Schwerpunktprüfung konnte insgesamt im **Herbst 2022 abgeschlossen** werden. Der BfD EKD veröffentlichte in diesem Zusammenhang einen Abschlussbericht und den verwendeten Fragebogen auf seiner Internetseite.

Die Prüfung hat gezeigt, dass es sowohl im rechtlichen und organisatorischen Bereich als auch im technischen Umfeld **zum Teil noch Verbesserungsbedarf** beim Datenschutz gibt. Die Prüfung hat aber ebenfalls aufgezeigt, dass es in den allermeisten Kindertageseinrichtungen **keine strukturellen Defizite** gibt und eine gewisse **Sensibilität** für datenschutzrechtliche Fragen **vorhanden** ist. So ist zum Beispiel positiv aufgefallen, dass die Verpflichtung auf das Datengeheimnis gemäß § 26 DSG-EKD in den allermeisten Kindertageseinrichtungen bereits gut umgesetzt wird. Auch die notwendige Bestellung von örtlich Beauftragten für den Datenschutz im Sinne des § 36 Abs. 1 DSG-EKD wurde in der Zwischenzeit weitestgehend vorgenommen. Verbesserungsbedarf besteht jedoch im Umgang mit der Meldung von Datenpannen nach § 32 DSG-EKD. Defizite wurden auch bei der Aufbewahrung und Verschlüsselung mobiler Endgeräte festgestellt. Handlungsbedarf besteht ebenfalls bezüglich der Datenschutzerklärungen auf den Internetseiten. Festzuhalten bleibt, dass ein gutes Datenschutzniveau nur über die kontinuierliche Weiterarbeit an den Themen etabliert werden kann.

Die **nächste Schwerpunktprüfung** findet im Bereich der **evangelischen Krankenhäuser** im Zeitraum 2023/2024 statt.

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 spezielle Datenschutzfragen.

Datenaustausch zwischen diakonischen und staatlichen Stellen

Diakonische Einrichtungen arbeiten als **freie Träger** oftmals mit staatlichen Leistungsträgern zusammen. Im Rahmen dieser Zusammenarbeit findet ein **permanenter Datenaustausch** zwischen diakonischen Einrichtungen und staatlichen Stellen statt, um die von den diakonischen Einrichtungen erbrachten Leistungen abrechnen zu können. Viele Einrichtungen haben für den Datenaustausch **Prozesse** entwickelt. Gleichwohl bestehen häufig Unsicherheiten in Bezug auf die Frage, welche Daten bzw. wie viele Daten notwendig sind, um die erbrachten Leistungen nachzuweisen.

Erbringen freie Träger Leistungen für Sozialleistungsträger, handelt es sich dabei in der Regel um die Konstellation des **sozialrechtlichen Dreiecksverhältnisses**. Der Begriff sozialrechtliches Dreiecksverhältnis beschreibt das Verhältnis von Hilfeberechtigten, Leistungserbringern (diakonische Einrichtungen) und dem zuständigen öffentlichen Leistungs- und Kostenträger (bspw. Jugendamt, Arbeitsagentur). Die Hilfeberechtigten haben einen Anspruch auf Leistung gegenüber dem jeweiligen Leis-

tungsträger. Dieser erfüllt den Anspruch jedoch nicht selbst, sondern bedient sich einem freien Träger – beispielsweise einer diakonischen Einrichtung – als Leistungserbringer. Dazu schließt der Leistungsträger (Rahmen-)Verträge mit der jeweiligen diakonischen Einrichtung hinsichtlich der Ausführung der Leistung sowie der Kosten. Die diakonische Einrichtung wiederum schließt Verträge mit den Hilfeberechtigten, die sie versorgt.

Datenschutzrechtlich bestehen bei den Konstellationen des sozialrechtlichen Dreiecksverhältnisses zwischen den Beteiligten keine Auftragsverarbeitungsverhältnisse. Vielmehr handeln hier zwei verantwortliche Stellen **eigenverantwortlich** nebeneinander. Aufgrund der Eigenverantwortlichkeit können die für die Erfüllung der jeweiligen Aufgaben erforderlichen personenbezogenen Daten nicht ohne **Rechtsgrundlage** zwischen den diakonischen Einrichtungen und den Sozialleistungsträgern ausgetauscht werden. Vielmehr besteht auch aus Sicht der diakonischen Einrichtung eine **eigene vertragliche Beziehung** zu den Hilfeberechtigten, die auch einen vertraulichen Umgang mit den personenbezogenen Daten bedingt. Die diakonische Einrichtung erhebt hier Daten in eigener Verantwortung und es bedarf im Fall einer **Offenlegung** einer entsprechenden Rechtsgrundlage. Hier ist im Einzelfall und je nach Einsatzbereich zu prüfen, welche personenbezogenen Daten die diakonische Einrichtung zur Erfüllung des Vertrags mit dem Leistungsträger oder aufgrund gesetzlicher Verpflichtungen zu übermitteln hat. Die Hilfeberechtigten sind im Rahmen der Informationspflicht bei Vertragsschluss über die Verarbeitungen der personenbezogenen Daten zu informieren.

Für personenbezogene Daten, die nicht zur Erfüllung der Aufgaben der verantwortlichen Stelle oder beispielsweise zur Durchführung eines Vertrages im Gesundheits- oder Sozialbereich **erforderlich** sind, die aber dennoch verarbeitet werden sollen, bedarf es einer **Einwilligung** der Hilfeberechtigten. Eine nicht erteilte Einwilligung kann dazu führen, dass die dadurch ausbleibende Datenübermittlung für die Hilfeberechtigten negative Folgen in Beziehung zum Leistungsträger nach sich zieht.

Fazit: Diakonische Einrichtungen müssen prüfen und transparent darüber informieren, welche personenbezogenen Daten ihrer Hilfeberechtigten für die Durchführung der jeweiligen Dienstleistung offengelegt werden müssen. Personenbezogene Daten, die darüber hinausgehen, aber „schon immer geliefert wurden“ oder zusätzlich von Leistungsträgern angefordert werden, bedürfen grundsätzlich einer expliziten Einwilligung der betroffenen Person.

Veröffentlichung von OP-Daten in sozialen Netzwerken

Immer wieder erreichen den BfD EKD Meldungen von Datenpannen, bei denen Gesundheitsdaten Dritter in sozialen Netzwerken geteilt und veröffentlicht wurden.

In einem Fall hatte ein Praktikant im Rettungssanitätsdienst, der im OP-Bereich eines Klinikums eingesetzt war, (legitimen) Zugriff auf den OP-Plan. Er nutzte diese Zugriffsrechte, um in mindestens einem Fall ein **Foto** von einem Eintrag im OP-Plan **anzufertigen**, aus dem zu einer geplanten OP auch die personenbezogenen Daten der Patientin sowie der Name des Operateurs hervorgingen. Dieses Foto wurde an mindestens zwei weitere Personen in einem **sozialen Netzwerk verteilt**. Die Anfertigung und die Veröffentlichung des Fotos sowie die damit einhergehende Veröffentlichung von Gesundheitsdaten stellt eine datenschutzwidrige Offenlegung von besonderen Kategorien personenbezogener Daten dar, sodass das Klinikum den Vorfall als Datenpanne an den BfD EKD meldete.

Das Klinikum führte ein Gespräch mit dem Praktikanten zur Klärung, ob weitere Fotos angefertigt und gegebenenfalls weitergegeben wurden. Es wurde die **Löschung** bereits veröffentlichter Fotos veranlasst. Weitere personalrechtliche Maßnahmen folgten.

Fazit: Für die Anfertigung und Veröffentlichung von Fotos ist stets eine Rechtsgrundlage erforderlich. Gesundheitsdaten dürfen nicht ohne Einwilligung der betroffenen Personen in sozialen Netzwerken veröffentlicht werden.

Durchsetzung eines Hausverbots

Den BfD EKD erreichte im Berichtszeitraum eine Beratungsanfrage einer diakonischen Einrichtung zum datenschutzkonformen Umgang mit erteilten Hausverboten. Dabei ging es insbesondere um die Fragen, ob das für eine Einrichtung erteilte Hausverbot auch an andere Einrichtungen und Fachbereiche derselben Muttergesell-

schaft weitergemeldet werden darf, ob das Sicherheitspersonal und die Mitarbeitenden der Einrichtung über das Hausverbot informiert werden dürfen und ob ihnen in diesem Zusammenhang auch ein Lichtbild der von dem Hausverbot betroffenen Person gezeigt werden darf.

Wie stets im Datenschutzrecht ist bei der Beantwortung dieser Fragen zu beachten, dass es für jede Verarbeitung und damit auch für jede **Offenlegung** von personenbezogenen Daten einer **Rechtsgrundlage** bedarf und die Verarbeitung **zwingend erforderlich** sein muss.

In Bezug auf die Offenlegung eines erteilten Hausverbotes **gegenüber anderen Einrichtungen und Fachbereichen** ist festzustellen, dass nur diejenigen Einrichtungen von einem Hausverbot unterrichtet werden dürfen, die das Hausverbot auch verhängt haben und für die es gilt. Im Übrigen besteht **keine Rechtsgrundlage** und auch **keine Notwendigkeit**, andere Einrichtungen und Fachbereiche derselben Muttergesellschaft über das erteilte Hausverbot zu informieren. Sofern das Hausverbot tatsächlich für mehrere Einrichtungen ausgesprochen wird, ist darauf zu achten, dass die Offenlegung der erforderlichen Information auf einem **sicheren Weg**, gegebenenfalls über eine verschlüsselte E-Mail, erfolgt.

Innerhalb der Einrichtung ist zu beachten, dass personenbezogene Daten von Personen, für die ein Hausverbot gilt, auch nur den Personen zugänglich sein dürfen, die diese **Informationen benötigen**, um das Hausverbot durchsetzen zu können. Dazu können beispielsweise das Sicherheitspersonal, einzelne Mitarbeitende, die Einrichtungsleitung sowie die Fachbereichsleitung gehören.

Zur Durchsetzung eines erteilten Hausverbots wird in vielen Fällen ein **Lichtbild der Person**, gegen die das Hausverbot ausgesprochen wurde, an das Sicherheitspersonal sowie an die Mitarbeitenden der Einrichtung verteilt. Bei einem Lichtbild handelt es sich um ein personenbezogenes Datum, sofern eine Person direkt oder indirekt identifizierbar ist. Insofern ist auch für die Offenlegung des Lichtbildes gegenüber dem Sicherheitspersonal sowie gegenüber den Mitarbeitenden der Einrichtung eine Rechtsgrundlage erforderlich. Diesbezüglich ist davon auszugehen, dass es für die effektive Durchsetzung eines Hausverbotes grundsätzlich erforderlich ist, den Personen, die das Hausverbot durchsetzen müssen, ein Lichtbild der vom Hausverbot betroffenen Person zu zeigen. Zu Nachweiszwecken ist die datenschutzrechtliche Prüfung der einzelnen Fragen, die mit der Durchsetzung eines Hausverbotes in Zusammenhang stehen, zu dokumentieren.

Fazit: Bei der Durchsetzung eines Hausverbotes ist darauf zu achten, dass die dafür erforderlichen personenbezogenen Daten der betroffenen Person nur gegenüber denjenigen Einrichtungen, für die das Hausverbot gilt, sowie gegenüber dem Sicherheitspersonal und den Mitarbeitenden der einzelnen Einrichtung, die das Hausverbot durchsetzen müssen, offengelegt werden. Eine Kenntnisnahme durch Dritte muss ausgeschlossen sein.

Konzernprivileg für diakonische Einrichtungen?

Eine Frage, die sich größere diakonische Einrichtungen häufig stellen, betrifft den **Datenaustausch zwischen** der **Muttergesellschaft** und ihren **Tochtergesellschaften**.

Wie auch im privatwirtschaftlichen Bereich, werden bei größeren diakonischen Trägern einzelne Unternehmensteile (aus betriebswirtschaftlichen Gründen) oftmals in Tochtergesellschaften ausgegliedert. Hierbei liegt regelmäßig die Konstellation vor, dass die Muttergesellschaft 100% der Gesellschaftsanteile der Tochtergesellschaften hält und damit Direktionsbefugnis hat. Trotzdem handelt es sich bei den **Tochtergesellschaften** datenschutzrechtlich um **eigene verantwortliche Stellen**. Dies hat zur Folge, dass jede Tochtergesellschaft als **Dritte** im Sinne des EKD-Datenschutzgesetzes anzusehen ist und daher bei einem Datenaustausch zwischen den einzelnen Gesellschaften grundsätzlich eine Rechtsgrundlage erforderlich ist. Somit sind entweder Einwilligungen der betroffenen Personen oder der Abschluss von **Verträgen zur Auftragsverarbeitung** (**AV-Vertrag**) mit den Tochtergesellschaften nötig, um einen Datenaustausch zu ermöglichen.

Ein **konkret normiertes Konzernprivileg**, das den Gesellschaften auch ohne Rechtsgrundlage einen Datenaustausch untereinander ermöglicht, gibt es im EKD-Datenschutzgesetz nicht. Auch in der DSGVO ist ein Konzernprivileg nicht ausdrücklich geregelt. Ein Konzernprivileg ergibt sich jedoch aus den Erwägungsgründen der DSGVO. Dort wird klargestellt, dass der

Austausch von personenbezogenen Daten für **interne Verwaltungszwecke** ein **berechtigtes Interesse** im Sinne des Art. 6 lit. f DSGVO von Unternehmensgruppen sein kann. Damit kann nach einer zugunsten der verantwortlichen Stelle positiv ausfallenden Interessenabwägung das berechtigte Interesse als **Rechtsgrundlage** herangezogen werden. Wichtig ist, dass diese zulässige Datenübertragung auf interne Verwaltungszwecke, die auch die Verarbeitung personenbezogener Daten von Kunden und Beschäftigten betreffen kann, beschränkt ist und, soweit relevant, auch die Voraussetzungen einer Datenübermittlung in Drittstaaten zusätzlich vorliegen müssen. Daraus ergibt sich, dass bei einer **„unternehmensgruppeninternen" Übermittlung von personenbezogenen Daten für interne Verwaltungszwecke** die berechtigten Interessen der Unternehmen in der Regel höher und die schutzwürdigen Interessen der betroffenen Personen niedriger zu bewerten sind als beim Datentransfer zwischen nicht verbundenen Unternehmen.

Die in den Erwägungsgründen der DSGVO beschriebene Konstellation lässt sich auch **aus dem EKD-Datenschutzgesetz** herleiten. Unter Zugrundelegung von § 6 Nr. 4 in Verbindung mit § 6 Nr. 8 DSG-EKD können sich auch hier Fälle ergeben, in denen das Interesse der betroffenen Person hinter **das berechtigte Interesse des Unternehmens an der Datenübermittlung** zurücktritt, weil die Datenübertragung in dieser Struktur teilweise ohnehin als **erforderlich** zu bezeichnen wäre und letztlich **keine Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen entgegenstehen**. Früher wurden diese Datenströme über zahlreiche unternehmensinterne AV-Verträge gelöst, die insbesondere durch die Weisungsbefugnis des Auftraggebers gekennzeichnet waren. Dieses Merkmal lässt sich auch hier auf die Konstellation des beherrschenden Unternehmens in Beziehung zu seinen Tochtergesellschaften übertragen. Auch hier hat die Muttergesellschaft die Befugnis, Datenschutzvorschriften nach ihren „Weisungen" umsetzen zu lassen. Ob der empfangende Unternehmensteil im Einzelfall seine Verarbeitung auf berechtigte Interessen oder auf Vertragserfüllung gegenüber der beherrschenden Muttergesellschaft stützen kann, ist in der Unternehmensgruppe zu prüfen und zu dokumentieren. Hervorzuheben bleibt, dass transparent über diese Datenströme zu informieren ist.

Fazit: Auch im diakonischen Bereich kann unter Vorliegen der dargestellten Umstände ein berechtigtes Interesse der Unternehmensgruppe bzw. der Muttergesellschaft vorliegen, personenbezogene Daten für interne Verwaltungszwecke unternehmensgruppenintern zu verarbeiten.

Umgang mit Beschäftigtendaten

Viele kirchliche und diakonische Einrichtungen haben sich im Berichtszeitraum mit verschiedenen Fragen zur Verarbeitung personenbezogener Daten von Beschäftigten an den BfD EKD gewandt.

Intranet-Registrierung mit privaten Kontaktdaten

Im Berichtszeitraum erreichten den BfD EKD mehrere Beschwerden von Beschäftigten, die sich gegen den Betrieb eines landeskirchlichen Intranets richteten. Bemängelt wurde dabei insbesondere, dass die Nutzenden bei der Registrierung dazu aufgefordert wurden, ihr Geburtsdatum sowie ihre private Adresse anzugeben. Bei diesen Angaben handelte es sich um **Pflichtangaben**, ohne die eine Registrierung nicht möglich war. Darüber hinaus bemängelten die Beschäftigten, dass seitens der verantwortlichen Stelle **nicht darüber informiert** wurde, zu welchem **Zweck** die verschiedenen personenbezogenen Daten erhoben wurden.

Im Rahmen der Sachverhaltsaufklärung konnte die verantwortliche Stelle **keine Rechtsgrundlage** für die Erhebung des Geburtsdatums sowie der privaten Adresse der Beschäftigten benennen. Die Erhebung dieser personenbezogenen Daten war **zur Nutzung des Intranets** auch **nicht erforderlich**.

Der BfD EKD stellte daher fest, dass der Prozess der Registrierung **nicht datenschutzkonform** erfolgte. Neben den fehlenden Rechtsgrundlagen waren auch Verstöße gegen den Grundsatz der **Datenminimierung** sowie dem Grundsatz der **Transparenz** gegeben. Die Verstöße wurden beanstandet und auf die Überarbeitung des Registrierungsprozesses sowie auf die Einhaltung der Informationspflichten gegenüber den Beschäftigten hingewirkt.

Fazit: Die Verarbeitung privater Kontaktdaten im Beschäftigungsverhältnis ist nur bei Vorliegen der Voraussetzun-

gen des § 49 DSG-EKD zulässig. Zusätzlich sind die Grundsätze der Verarbeitung nach § 5 DSG-EKD zu berücksichtigen.

Speicherung privater Handynummern

In einigen Beratungsanfragen wurde gefragt, ob eine Einrichtung die private Handynummer ihrer Mitarbeitenden speichern darf.

Nach **§ 49 Abs. 1 DSG-EKD** dürfen personenbezogene Daten von Beschäftigten nur verarbeitet werden, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Beschäftigtenverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch für Zwecke der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

Zur **Durchführung des Arbeitsverhältnisses** bzw. zur Personalplanung ist es **nicht erforderlich**, dass der Arbeitgeber die **privaten Kontaktdaten** der Beschäftigten (insbesondere private Festnetznummer, Handynummer und E-Mail-Adresse) kennt und verarbeitet. Als erforderlich zur Durchführung des Arbeitsverhältnisses gelten z. B. die Adresse, Kontoverbindung und Rentenversicherungsnummer der Mitarbeitenden. Soweit der Arbeitgeber zum Beispiel die private Handynummer vorhalten möchte – um die Mitarbeitenden in Notfällen zu informieren – muss eine **Einwilligung** der Mitarbeitenden für die Datenverarbeitung eingeholt werden. In Fällen, in denen vertraglich eine vergütete Rufbereitschaft vereinbart ist und keine dienstlichen Geräte zur Verfügung gestellt werden, kann der Arbeitgeber den Beschäftigten als milderes gleich wirksames Mittel beispielsweise einen „Pieper“ zur Verfügung stellen, mit dem er die Mitarbeitenden im Einsatzfall erreichen kann. Auch insoweit wird man nicht davon ausgehen können, dass die Verarbeitung der privaten Kontaktdaten zwingend notwendig ist. Eine Speicherung der privaten Telefon- bzw. Handynummer setzt daher immer eine Einwilligung der Mitarbeitenden voraus.

Auf Bitten der Mitarbeitenden sind die entsprechenden Kontaktdaten **unverzüglich zu löschen**.

Fazit: Die Verarbeitung privater Telefon- und Handynummern von Beschäftigten durch den Arbeitgeber ist zur Durchführung des Beschäftigungsverhältnisses nicht erforderlich. Eine Verarbeitung solcher Daten ist lediglich auf der Grundlage einer Einwilligung zulässig. Im Beschäftigungsverhältnis werden an die Einwilligung aufgrund des Über- Unterordnungsverhältnisses erhöhte Anforderungen gestellt.

Weitergabe einer Kündigung

Im Rahmen einer Beschwerde stellte sich heraus, dass ein leitender Angestellter Informationen über die Kündigung einer Beschäftigten an Bewerberinnen und Bewerber weitergegeben hat.

Die Weitergabe der Information über die Kündigung und die Nutzung der Kontaktdaten der Bewerbenden war nicht – wie in § 49 Abs. 1 DSG-EKD gefordert – zur Begründung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses erforderlich und stellt eine Verletzung des Schutzes personenbezogener Daten dar. Es liegt sowohl eine **Datenschutzverletzung gegenüber der Beschäftigten als auch gegenüber den Bewerbenden** vor. Auch hätte die Verarbeitung der personenbezogenen Daten ausschließlich durch die Personalabteilung erfolgen dürfen. Eine eigenmächtige Kontaktaufnahme mit Bewerbenden unter Nennung von personenbezogenen Daten Dritter überschreitet die Zuständigkeit von leitenden Angestellten. Der Datenschutzverstoß war der verantwortlichen Stelle auch zuzurechnen.

Um zukünftig vergleichbare Vorfälle auszuschließen, hat die verantwortliche Stelle zwischenzeitlich festgelegt, dass die **Bearbeitung von Personalfällen** ausschließlich durch die **Personalabteilung** erfolgen darf. Zum Schutz personenbezogener Daten wurde den in der Personalabteilung tätigen Personen die unbefugte Verarbeitung von personenbezogenen Daten untersagt. Zu Nachweiszwecken liegt für alle Beschäftigten eine **schriftliche Verpflichtung auf das Datengeheimnis** vor. Ergänzend erfolgt regelmäßig eine **Schulung** zu aktuellen datenschutzrechtlichen Themen.

Fazit: Beschäftigtendaten sind aufgrund ihrer Sensibilität vor dem unberechtigten Zugriff durch Dritte zu schützen. Dies ist durch technische und organisatorische Maßnahmen sicherzustellen.

Übermittlung an Gläubiger und Kreditinstitute

Beschäftigtendaten dürfen nach § 49 Abs. 1 DSG-EKD verarbeitet werden, soweit dies zur Durchführung eines Beschäftigungsverhältnisses erforderlich ist. Dazu gehört in der Regel auch, den **Namen**, die **Kontoverbindung** und den **Verdienst** zum Zweck der Überweisung des Arbeitseinkommens dem jeweiligen **Kreditinstitut der Beschäftigten** als Dritten gegenüber **offenzulegen**. Es kann aber auch Situationen geben, in denen die zulässige **Offenlegung** von Beschäftigtendaten **gegenüber Dritten nicht** ohne weiteres **ersichtlich** ist.

Dies ist insbesondere in Fällen gegeben, in denen Gläubiger von Beschäftigten (Schuldner) gegen deren Arbeitgeber (Drittschuldner) in einem **Pfändungs- und Überweisungsbeschluss** die Pfändung des Arbeitseinkommens erwirken. Der Pfändungsbeschluss führt dazu, dass die Beschlagnahme des Arbeitseinkommens des Beschäftigten gegen den Arbeitgeber verfügt wird und dem Arbeitgeber die Leistung an den Beschäftigten verboten wird. Der Überweisungsbeschluss gewährt dem Gläubiger das Recht der Einziehung der Forderung beim Arbeitgeber.

Darüber hinaus muss der Arbeitgeber dem Gläubiger auf Verlangen über die in § 840 Zivilprozessordnung (ZPO) genannten Aspekte im Rahmen der sogenannten **Drittschuldnererklärung** Auskunft geben. Dazu ist der Arbeitgeber verpflichtet, auch wenn die Auskunft personenbezogene Daten des Beschäftigten enthält. Insofern stellt § 840 ZPO eine Rechtsgrundlage im Sinne von § 9 Abs. 1 Nr. 2 DSG-EKD für die Offenlegung von personenbezogenen Daten durch den Arbeitgeber an den Gläubiger im Zusammenhang mit der Drittschuldnererklärung dar. Kommt der Drittschuldner seiner Auskunftspflicht nicht, unvollständig oder zu spät nach oder gibt er eine falsche Erklärung ab, haftet er dem Gläubiger gegenüber für den daraus entstandenen Schaden.

Rückblick: Corona-Regelungen in kirchlichen und diakonischen Einrichtungen

Den kirchlichen und diakonischen Einrichtungen wurden während der Corona-Pandemie – im Vergleich zu der Zeit davor – einige **neue gesetzliche Verpflichtungen** auferlegt, die mit der Verarbeitung von Gesundheitsdaten der Beschäftigten im Zusammenhang mit der Covid-19 Infektion einhergingen. Bei den unterschiedlichen gesetzlichen Regelungen, die eine Verarbeitung von Gesundheitsdaten für festgelegte Zwecke ausnahmsweise erlaubten, handelte es sich schwerpunktmäßig um Angaben zum Impf- und Serostatus der Beschäftigten oder zu deren Infektionsrisiko.

Mit der Änderung des Infektionsschutzgesetzes (IfSG) im September 2021 trat in **§ 36 Abs. 3 IfSG** (seit 30. Juni 2022 außer Kraft) die erste Regelung in diesem Zusammenhang für bestimmte, im Gesetz ausdrücklich genannte Einrichtungen in Kraft. Neben bestimmten diakonischen Einrichtungen fielen auch Kindertagesstätten und Schulen in den Anwendungsbereich. Auf Basis dieser Rechtsgrundlage konnten Einrichtungen **personenbezogene Daten von Beschäftigten über deren Impf- und Serostatus** in Bezug auf die Covid-19 Infektion verarbeiten, um über die Begründung eines Beschäftigungsverhältnisses oder über die Art und Weise einer Beschäftigung zu entscheiden. Dabei kam es bei der Anwendung der neuen Rechtsgrundlage teilweise zu der fehlerhaften Auffassung, dass hierzu Fotokopien der Dokumente der Mitarbeitenden anzufertigen seien, um der Rechenschaftspflicht nachkommen zu können. Da § 36 IfSG aber von personenbezogenen Daten über den Status der Mitarbeitenden spricht, ergab sich aus dem datenschutzrechtlichen Prinzip der Erforderlichkeit, dass Aufzeichnungen zu dem Vorliegen der entsprechenden Dokumente ausreichten.

Seit November 2021 regelte **§ 28b Abs. 1 IfSG** (seit 24. März 2022 außer Kraft) die **Vorlagepflicht von 3G-Nachweisen**, die zum Betreten aller Arbeitsstätten deutschlandweit notwendig waren. Auch hier ergaben sich in der anfänglichen Umsetzungsphase zahlreiche datenschutzrechtliche Fragen und Probleme. Genügte als Nachweis für Arbeitgeber grundsätzlich die Vorlage eines aktuellen 3G-Dokumentes, wurde vielerorts die Vorlage des Impfausweises per E-Mail gefordert, um den Verpflichtungen der Arbeitgeber nachkommen zu können. Dieses häufig als unverschlüsselte E-Mail angeforderte Dokument enthielt in der Regel Daten, die über das gesetzlich geforderte Maß hinausgingen. Es wurden daher Daten verarbeitet, für die keine Rechtsgrundlage gegeben war und die nicht erforderlich waren. Des Weiteren führte die Regelung in der Praxis vielfach dazu, dass beim Betreten der Arbeitsstätte zahlreichen Mitarbeitenden gegenüber offengelegt wurde, wer welches

3G-Dokument vorhält. Mitarbeitenden, die sich aus verschiedenen Gründen gegen eine Impfung entschieden hatten, wurden daher teilweise stigmatisiert. Da dieses Thema sehr präsent in Politik und Medien lanciert wurde, war es in manchen Arbeitsstätten schwer, die Persönlichkeitsrechte aller Beschäftigten adäquat zu schützen.

Einhergehend mit der Vorlagepflicht von 3G-Nachweisen für die Beschäftigten waren Arbeitgeber nach **§ 28b Abs. 3 IfSG** (seit 24. März 2022 außer Kraft) dazu verpflichtet, personenbezogene Daten der Beschäftigten einschließlich Daten zum Impf-, Sero- und Teststatus in Bezug auf die Covid-19 Infektion zu Dokumentationszwecken zu verarbeiten (**Dokumentationspflicht**). Zur Erfüllung dieser Pflicht mussten die geimpften und genesenen Beschäftigten dem Arbeitgeber **einmalig** ihren Impf- oder Genesenennachweis **vorlegen**, um die Arbeitsstätte betreten zu können. Die Arbeitgeber durften die Vorlage des Nachweises in einer **namentlich geführten Liste** vermerken und auch die Dauer der Befristung dokumentieren. Beschäftigte, die keinen Impf- oder Genesenennachweis vorlegten, konnten die Arbeitsstätte nur nach Vorlage eines negativen Testergebnisses betreten. In diesem Fall durfte der Arbeitgeber den Namen des Beschäftigten sowie die Gültigkeit des Tests vermerken. Zugleich bestand für die Beschäftigten die Pflicht, während ihrer Anwesenheit in der Arbeitsstätte Impf-, Genesenen- oder Testnachweise **für Kontrollen** durch die zuständigen Behörden **verfügbar** zu halten. Um nicht ständig den entsprechenden Nachweis mit sich führen zu müssen, bestand alternativ die Möglichkeit, die entsprechenden Nachweise in einem verschlossenen und mit dem Namen versehenen Umschlag beim **Arbeitgeber** für eventuelle Kontrollen durch die zuständigen Behörden zu **hinterlegen**. Dabei war jedoch zu beachten, dass mit der Hinterlegung die Verarbeitung von Gesundheitsdaten der Beschäftigten, die den Impf-, Genesenen- oder Testnachweisen entnommen werden konnten, verbunden war und daher eine Rechtsgrundlage für die weitere Verarbeitung dieser Daten erforderlich war. Als Rechtsgrundlage kam lediglich die **Einwilligung** der betroffenen Person in Betracht. Da im Beschäftigtenverhältnis ein Über-Unterordnungsverhältnis besteht, sind an die **Freiwilligkeit** solcher Einwilligungen stets besondere Anforderungen zu stellen. Verantwortliche Stellen müssen den Beschäftigten eine echte Wahlmöglichkeit geben. Ein Indiz für die Freiwilligkeit besteht dann, wenn Beschäftigte einen rechtlichen oder wirtschaftlichen Vorteil erhalten. Ob der Entfall der Mitführungspflicht als rechtlicher oder wirtschaftlicher Vorteil angesehen werden kann, ist umstritten. Zumindest war den Beschäftigten zur Wahl zu stellen, ob sie den Nachweis selbst mitführen oder bei dem Arbeitgeber hinterlegen. Darüber hinaus kann die Einwilligung immer nur zweckgebunden erteilt werden. Der Zweck der Hinterlegung war, dem Arbeitgeber die Vorlage der nach § 28b IfSG geforderten Nachweise gegenüber einer kontrollierenden Behörde zu ermöglichen, ohne dass die Beschäftigten den Nachweis stets mit sich führen mussten. Sofern die genannten Voraussetzungen eingehalten und die Beschäftigten zusätzlich auf das jederzeit bestehende **Widerrufsrecht** hingewiesen wurden, war eine Hinterlegung des geforderten Nachweises beim Arbeitgeber auf der Grundlage einer schriftlichen Einwilligung zulässig.

Mit Inkrafttreten der sogenannten **einrichtungsbezogenen Impfpflicht** zum 11. Dezember 2021 nach **§ 20a IfSG** (seit 31. Dezember 2022 außer Kraft) war eine Differenzierung zwischen geimpften, genesenen und getesteten Personen nicht mehr vorzunehmen. In **Gesundheitseinrichtungen** war mit dieser Regelung eine Weiter- oder Neubeschäftigung nur noch nach **Vorlage eines entsprechenden Immunitätsnachweises** – spätestens bis zum 15. März 2022 – möglich. Danach konnten nur noch medizinische Kontraindikationen einen Verzicht auf die Impfung rechtfertigen. Datenschutzrechtlich schaffte § 20a IfSG damit zum einen die Rechtsgrundlage zur Verarbeitung von Immunitätsnachweisen der Mitarbeitenden. Zum anderen schaffte § 20a IfSG für die betroffenen Einrichtungen eine **Offenlegungsbefugnis bzw. –verpflichtung gegenüber den zuständigen Gesundheitsämtern**, deren Nichteinhaltung mit Bußgeld bewährt war. Legten Mitarbeitende der Einrichtungen ihren Immunitätsnachweis bis zum Ablauf des 15. März 2022 nicht vor oder bestanden Zweifel an der Echtheit oder inhaltlichen Richtigkeit der Dokumente, mussten die Einrichtungen die zuständigen Gesundheitsämter darüber benachrichtigen und personenbezogene Daten der Mitarbeitenden zur Verfügung stellen. Diese Daten sollten es den Gesundheitsämtern ermöglichen, die Mitarbeitenden zu identifizieren und mit diesen Kontakt aufzunehmen. Hinsichtlich der Nachweise hatten die Einrichtungen nunmehr die Verpflichtung, eine Plausibilitätskontrolle vorzunehmen. Nach dem Geset-

zeswortlaut war auch in diesem Fall nicht vorgesehen, Immunitätsnachweise der Mitarbeitenden zu kopieren und zu archivieren. Auch hier sollte die Vorlage genügen. Im Idealfall nur gegenüber einem dafür bestimmten Personenkreis, der zur Verarbeitung von Gesundheitsdaten geeignet war. Gemäß § 20a IfSG waren alle in den Einrichtungen **Tätigen den Gesundheitsämtern zu melden**. Aufgrund der Regelung kam es dazu, dass beispielsweise auch Mitarbeitende, die sich in Elternzeit befanden oder in einem abgeschlossenen Verwaltungsgebäude tätig waren, gemeldet wurden. Erhoben diese Mitarbeitende teilweise den Einwand, sie unterfielen der Regelung – mangels Kontakt zu vulnerablen Gruppen – nicht, war dies für die Einrichtungen schwer zu berücksichtigen, da die Regelung hier gerade keine eindeutige Differenzierung vornahm. Insoweit konnte der Einwand der Beschäftigten dann tatsächlich erst durch die Gesundheitsämter geprüft werden. Erst dort war die Frage zu entscheiden, ob gegen die gemeldeten Mitarbeitenden mangels Vorlage eines Immunitätsnachweises ein Beschäftigungsverbot zu verhängen war. Letztlich war es wichtig, darauf zu achten, dass in keinem Fall Immunitätsnachweise an das Gesundheitsamt übermittelt wurden. Auch nicht, wenn Zweifel an der Echtheit oder an der inhaltlichen Richtigkeit bestanden. Im Ganzen bleibt in Bezug auf die Abfrage des Impfstatus im Rahmen der einrichtungsbezogenen Impfpflicht festzuhalten, dass es zu einer **Vielzahl von Beschwerden von Beschäftigten** gekommen ist. Die Petentinnen und Petenten rügten insbesondere, dass sie von ihrem Arbeitgeber aufgefordert wurden einen Impfnachweis zu erbringen. Inhalt einiger Beschwerden war auch die Anfertigung und Aufbewahrung der vorgelegten Immunitätsnachweise durch die verantwortliche Stelle. Wegen einer fehlenden Rechtsgrundlage oder Einwilligung der Petentinnen und Petenten wurde in mehreren Fällen festgestellt, dass die Anfertigung und die Aufbewahrung von Kopien der Immunitätsnachweise – unter Berücksichtigung des Grundsatzes der Datensparsamkeit und des besonderen Schutzes von Gesundheitsdaten – nicht datenschutzkonform gewesen sind.

Im Fall von **quarantänebedingten Ausfällen** hatte sich der Gesetzgeber in **§ 56 IfSG** entschieden, den Einrichtungen aufzuerlegen, dass diese in Vorleistung für die **Erstattungszahlungen** gehen müssen, wenn Mitarbeitende wegen behördlich angeordneter Isolation nicht ihrer Beschäftigung nachkommen konnten. Dies betraf nicht nur den Gesundheitsbereich, sondern alle Arbeitsstätten. Diese Entschädigung wurde jedoch anschließend an die Einrichtungen nur dann ausgezahlt, wenn die Mitarbeitenden eine Schutzimpfung im Sinne des § 20a IfSG nachweisen konnten. In diesen Fällen wurde für die Erstattungszahlung tatsächlich die Übersendung von Immunitätsnachweisen in Fotokopie durch die Einrichtungen verlangt. Eine Direkterhebung bei den Mitarbeitenden war grundsätzlich nicht vorgesehen. Insoweit war die zweckgebundene Verarbeitung durch die Einrichtung erforderlich. Unterlagen sollten nach **Zweckerreichung** umgehend **gelöscht** werden.

Fazit: Während der Corona-Pandemie haben die neuen Regelungen zum Umgang mit Beschäftigtendaten auch in Kirche und Diakonie viele rechtliche Fragen aufgeworfen, die in der praktischen Umsetzung der Regelungen nicht immer datenschutzkonform gelöst wurden.

Digitale Kommunikation in Videokonferenzen

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

Ist Zoom datenschutzkonform einsetzbar?

Wie im Berichtszeitraum 2019/2020 gab es auch im aktuellen Berichtszeitraum mehrere Anfragen, aber auch Beschwerden zur Nutzung des Videokonferenzsystems Zoom. Insbesondere in Bezug auf den Rahmenvertrag, den die Wirtschaftsgesellschaft der Kirchen in Deutschland mbH (WGKD) mit dem Dienstleister „Connect4Video“ geschlossen hat, erreichten den BfD EKD eine Reihe von Anfragen zur datenschutzrechtlichen Einschätzung von Zoom.

Allgemein ist bei der Nutzung von Zoom zu beachten, dass dabei **verschiedene personenbezogene Daten der Nutzenden** erhoben und verarbeitet werden. Dazu gehören neben den Protokoll- und Metadaten (z. B. Benutzername, E-Mail-Adresse und IP-Adresse) auch die Inhaltsdaten. Welche personenbezogenen Daten erhoben und verarbeitet werden und was mit den Daten geschieht, ist für die Nutzenden **kaum nachzuvollziehen**. Hinzu kommt, dass Zoom seinen Hauptsitz und

seine Rechenzentren in den USA hat, sodass davon auszugehen ist, dass bei der Nutzung von Zoom personenbezogene Daten **in die USA übermittelt** werden. Dies hat zur Folge, dass ohne einen dazwischen geschalteten Dienstleister alle personenbezogenen Daten der Nutzenden ungefiltert in die USA übermittelt und dort verarbeitet werden. Mit der Übermittlung der personenbezogenen Daten der Nutzenden in die USA sind **Risiken** verbunden, die die verantwortliche Stelle bei der Entscheidung, welches Videokonferenzsystem genutzt werden soll, berücksichtigen muss. Im Rahmen der Beratungsanfragen sowie im Zusammenhang mit den Beschwerdeverfahren hat der BfD EKD auf die bestehenden Risiken, die mit der Nutzung von Zoom für die personenbezogenen Daten der Nutzenden entstehen, hingewiesen und dabei zwischen den aktuell verfügbaren Betriebsformen von Zoom differenziert.

Zunächst ist es möglich, **Zoom in „Reinform“**, das heißt direkt und ohne einen dazwischen geschalteten Dienstleister, zu verwenden. In diesem Fall werden sämtliche personenbezogene Daten – also sowohl Inhalts- als auch Verbindungs- bzw. Metadaten – in die USA übermittelt und auf dortigen Servern verarbeitet. Dabei ist zu berücksichtigen, dass es sich bei den USA um ein sogenanntes Drittland im Sinne des § 4 Nr. 18 DSG-EKD handelt. Ein Drittland ist ein Staat, in dem die DSGVO keine Anwendung findet. Aufgrund dessen werden an Datenübermittlungen in Drittländer besonders hohe Anforderungen gestellt. **Datenübermittlungen in Drittländer** unterliegen gemäß § 10 DSG-EKD besonderen rechtlichen Anforderungen. Gemäß § 10 Abs. 1 DSG-EKD muss die EU-Kommission entweder ein **angemessenes Datenschutzniveau** in dem jeweiligen Drittland festgestellt haben oder es müssen **Standarddatenschutzklauseln** als geeignete Garantien verwendet werden. Sofern keine dieser Alternativen vorliegt, ist eine Datenübermittlung in Drittländer nur zulässig, wenn sie z. B. durch eine **Einwilligung** der betroffenen Personen legitimiert ist. Diese Anforderungen sind bei der direkten Nutzung von Zoom nicht erfüllt. Es ist keine Rechtsgrundlage für die Übermittlung von personenbezogenen Daten in die USA gegeben. Mit dem „Schrems II“-Urteil des EuGH vom 16. Juli 2021 wurde das sogenannte EU-US Privacy Shield-Abkommen, das bis zu diesem Zeitpunkt als Rechtsgrundlage gemäß § 10 Abs. 1 Nr. 1 DSG-EKD für die Datenübermittlung in die USA herangezogen werden konnte, für ungültig erklärt. Die Datenübermittlung kann ohne weitere **technische und organisatorische Maßnahmen** gegenwärtig auch nicht auf Standarddatenschutzklauseln gemäß § 10 Abs. 1 Nr. 2 DSG-EKD gestützt werden, da in den USA kein angemessenes Datenschutzniveau besteht und die in den Standarddatenschutzklauseln festgelegten Garantien nicht eingehalten werden können. Auch die in § 10 Abs. 2 DSG-EKD genannten Rechtsgrundlagen liegen bei der direkten Nutzung von Zoom in der Regel nicht vor. So werden beispielsweise an eine wirksame **Einwilligung** der Nutzenden hohe Anforderungen gestellt. Eine Einwilligung der Nutzenden wäre nur dann wirksam, wenn diese im Vorfeld ausführlich über die bestehenden möglichen Risiken, die mit einer Datenübermittlung in die USA verbunden sind, aufgeklärt worden sind. Da momentan erhebliche Bedenken bezüglich des in den USA vorhandenen Datenschutzniveaus bestehen, kann diese Variante nicht **datenschutzkonform** eingesetzt werden.

Neben der direkten Nutzung ist es möglich, Zoom über den deutschen Dienstleister **Connect4Video** zu verwenden. Durch den dazwischen geschalteten Dienstleister wird verhindert, dass die **Inhaltsdaten** in die USA übermittelt werden. Stattdessen werden diese auf in Deutschland befindlichen Servern von Connect4Video verarbeitet. Die **Metadaten** werden jedoch weiterhin in die USA übermittelt. Da auch Metadaten personenbezogene Daten sein können, bestehen an dieser Stelle vergleichbare Risiken für den Schutz der personenbezogenen Daten wie bei der direkten Nutzung von Zoom. Lediglich die Inhaltsdaten sind besser geschützt. Insofern kann auch diese Variante **nur als bedingt datenschutzkonform** eingestuft werden.

Die wohl datenschutzfreundlichste Variante ist die Nutzung von Zoom über den **Rahmenvertrag, den die WGKD** zwischenzeitlich mit dem deutschen Dienstleister Connect4Video abgeschlossen hat. In dem Rahmenvertrag ist geregelt, dass sämtliche personenbezogene Daten – sowohl Inhaltsdaten als auch Metadaten – der an den Videokonferenzen Teilnehmenden auf **Rechenzentren in Deutschland** verarbeitet werden. Es werden keine personenbezogenen Daten – auch keine Metadaten – in die USA oder ein anderes Drittland übermittelt. Die **Inhaltsdaten** werden auf Rechenzentren des deutschen Dienstleisters Connect4Video verarbeitet. Die **Metadaten** – die auch personenbezogen sein können – verblei-

ben dagegen auf deutschen Servern von Zoom mit Standort Frankfurt am Main. Obwohl keine personenbezogenen Daten in die USA übermittelt werden, besteht jedoch hinsichtlich der Verarbeitung der Metadaten auf deutschen Servern von Zoom aufgrund des sogenannten **CLOUD-Acts** weiterhin ein Risiko für den Schutz der personenbezogenen Daten der an den Videokonferenzen Teilnehmenden. Der CLOUD-Act ermöglicht den US-amerikanischen Behörden unter bestimmten Voraussetzungen auf die in Deutschland gespeicherten Daten zuzugreifen. Auch wenn davon wohl nur in wenigen Fällen Gebrauch gemacht wird, reicht allein die Möglichkeit aus, um ein Risiko für die verarbeiteten personenbezogenen Daten zu bejahen. Zwar werden die personenbezogenen Daten bei der Nutzung von Zoom über den Rahmenvertrag der WGKD besser geschützt als bei den anderen beiden Varianten, aber dennoch besteht auch bei dieser Variante ein **Risiko für die Rechte der betroffenen Personen**, also den Teilnehmenden an den Videokonferenzen. Dieses Risiko kann nicht vollständig ausgeschlossen werden. Sofern eine verantwortliche Stelle trotz der bestehenden Risiken Zoom einsetzen möchte, muss die verantwortliche Stelle prüfen, ob sie das bestehende Risiko **vertreten** kann und ob das bestehende Risiko durch weitere **technische und organisatorische Maßnahmen** verringert werden kann. Die Prüfung erfolgt im Rahmen einer **Risikobewertung** bzw. einer **Datenschutz-Folgenabschätzung**.

Fazit: Zum Schutz der personenbezogenen Daten empfiehlt der BfD EKD ein Videokonferenzsystem einzusetzen, das von einem deutschen oder europäischen Anbieter betrieben wird und bei dem die personenbezogenen Daten ausschließlich in Deutschland oder in der EU verarbeitet werden.

Einsatz von Zoom im Unterricht an Schulen

Den BfD EKD erreichte im Berichtszeitraum eine Beschwerde von Eltern, deren Kinder ein evangelisches Gymnasium besuchen. Inhalt der Beschwerde war die Umsetzung der **digitalen Unterrichtsgestaltung** während der Pandemiezeit. In der betroffenen Schule wurde zur Durchführung von Online-Unterricht das Videokonferenzsystem **Zoom in der direkt vom Hersteller** bereitgestellten Version eingesetzt. In der Anfangszeit der Nutzung von Zoom kam es zu Störungen durch fremde Personen mit Einblendungen unerwünschter Inhalte. Daraufhin wurden die Schülerinnen und Schüler verpflichtet, als Sicherheitsmaßnahme ihre Kamera über die gesamte Unterrichtszeit aktiviert zu lassen. Die Eltern fühlten sich in Bezug auf die getroffenen Datenschutzvorgaben und die geltenden IT-Sicherheitsmaßnahmen **nicht ausreichend informiert**. Sie befürchteten beispielsweise, dass unerlaubt Bild- und Videoaufnahmen gemacht und unkontrolliert im **Internet veröffentlicht** werden könnten.

Die Schule hat sowohl durch die **direkte Nutzung von Zoom** als auch im Rahmen der **Durchführung** des digitalen Unterrichts gegen datenschutzrechtliche Vorschriften **verstoßen**. Die direkte **Nutzung von Zoom** ist nicht datenschutzkonform möglich. Für die damit in Zusammenhang stehende Verarbeitung von personenbezogenen Daten der Schülerinnen und Schüler sowie der Lehrenden lag **keine Rechtgrundlage** vor. Auch eine **wirksame Einwilligung** der betroffenen Personen sowie deren Erziehungsberechtigten war nicht gegeben. Eine Einwilligung wäre nur wirksam gewesen, wenn diese im Vorfeld ausführlich über die bestehenden möglichen Risiken, die mit einer **Datenübermittlung in die USA** verbunden sind, aufgeklärt worden wären. Dies ist vorliegend nicht geschehen. Auch die zugrundeliegende **Freiwilligkeit** einer Einwilligung ist fraglich, da bei einer Nichteinwilligung die betroffenen Schülerinnen und Schüler vom digitalen Unterricht ausgeschlossen worden wären, was eine Benachteiligung darstellt. Im Übrigen war die Nutzung von Zoom **weder verhältnismäßig noch erforderlich**. Es gibt andere Videokonferenzsysteme, die datenschutzfreundlicher gestaltet sind und ihre Rechenzentren in Deutschland bzw. zumindest in einem Mitgliedsstaat der EU haben. Weiterhin wäre für die Nutzung von Zoom ein **Vertrag zur Auftragsverarbeitung** nach § 30 DSG-EKD abzuschließen gewesen und es hätte im Vorfeld eine **Datenschutz-Folgenabschätzung** durchgeführt werden müssen. Beides ist vorliegend nicht geschehen.

Darüber hinaus wurde der digitale Unterricht **nicht datenschutzkonform** durchgeführt. Den im Rahmen des Beschwerdeverfahrens vorgelegten Materialien der Schule zur Durchführung von Videokonferenzen ließ sich entnehmen, dass den Schülerinnen und Schülern die **dauerhafte Aktivierung der Kamera** während des Unterrichts vorgeschrieben wurde. Diese Datenverarbeitung wurde auf eine Einwilligung gestützt. Diesbezüglich ist zu beachten, dass eine verpflichtende Teilnahme

der Schülerinnen und Schüler ohne Bild und Ton mit dem Bildungs- und Erziehungsauftrag der Schule – also der Aufgabenerfüllung nach § 6 Nr. 3 DSG-EKD – begründet werden kann. Wenn aber Bild und Ton der Schülerinnen und Schüler erfasst werden, stellt dies einen tiefgreifenden Grundrechtseingriff dar, welcher einer gesonderten Rechtsgrundlage bedarf. Bei Video- und Tonübertragungen aus dem **häuslichen Umfeld** ist zu berücksichtigten, dass dieser Bereich nach Art. 13 Grundgesetz (GG) **besonders geschützt** ist. Hier käme tatsächlich nur eine **Einwilligung** nach § 6 Nr. 2 DSG-EKD in Betracht. Eine gesetzliche Rechtsgrundlage besteht nicht. Allerdings sind Einwilligungen wegen des Über- und Unterordnungsverhältnisses zwischen der Schule und den Schülerinnen und Schülern problematisch. Der **Freiwilligkeit** einer solchen Einwilligung kann ein sozialer Druck seitens der Mitschülerinnen und Mitschüler entgegenstehen. Dabei ist außerdem zu berücksichtigen, dass die Schülerinnen und Schüler rechtlich einen **Anspruch auf Erziehung und Bildung** haben. Die Erfüllung dieses Rechts darf – mit Blick auf die erforderliche Freiwilligkeit – nicht davon abhängig gemacht werden, dass eine Einwilligung erteilt wird. Deswegen muss den Schülerinnen und Schülern, die ihr Videobild und den Ton nicht übertragen möchten, die Teilnahme am Unterricht trotzdem ermöglicht oder ein vergleichbares Bildungs- und Erziehungsangebot unterbreitet werden. Sonst wäre eine Einwilligung datenschutzrechtlich nicht wirksam. Zudem muss es den Schülerinnen und Schülern auch nach Erteilung der Einwilligung freigestellt sein, die eigene Kamera oder das Mikrofon auszuschalten, denn datenschutzrechtlich ist jede Einwilligung mit Wirkung für die Zukunft widerrufbar. Auf die Möglichkeit des **Widerrufs** muss im Rahmen der Einwilligung explizit hingewiesen werden. Eine kurze **Aktivierung der Kamera** zu Beginn und zum Ende einer Unterrichtsstunde kann unter Umständen datenschutzkonform sein. Mit der kurzen Aktivierung der Kamera wird ein **legitimer Zweck** – die Kontrolle der Anwesenheit zur Erfüllung der Schulpflicht – verfolgt, wenn dies nicht auf andere Art und Weise möglich ist. Dies gilt aber nur, wenn ein datenschutzfreundliches Videokonferenzsystem verwendet wird und die Datenverarbeitung grundsätzlich gesetzeskonform erfolgt. Andere ebenso wirksame Möglichkeiten der Anwesenheitskontrolle müssen im Rahmen der **Erforderlichkeitsprüfung** vorrangig berücksichtigt werden.

Im Rahmen der Sachverhaltsaufklärung stellte sich im Übrigen heraus, dass der Schulträger keine Kenntnis vom Einsatz des Videokonferenzsystems Zoom hatte. Eigentlich stand den Schulen als Werkzeug für den digitalen Unterricht die **Schul-Cloud** des Bundeslandes zur Verfügung. In den Anfangszeiten der Corona-Pandemie war der Bedarf an dem Tool jedoch so hoch, dass der Online-Unterricht nicht zufriedenstellend durchgeführt werden konnte. Deshalb suchte sich die Schule eigenmächtig ein alternatives, schnell nutzbares Werkzeug zur Erfüllung ihrer Aufgaben und entschied sich für Zoom.

Die Durchführung des Online-Unterrichts mit Zoom wurde durch den BfD EKD beanstandet. Der Schulträger ergriff ebenfalls Maßnahmen und untersagte nach Bekanntwerden des Sachverhaltes sofort die datenschutzwidrige Nutzung von Zoom. Darüber hinaus unterstützte der BfD EKD den Schulträger bei der Auswahl einer datenschutzkonformen Lösung als Ergänzung zur Schul-Cloud.

Fazit: Bei der Nutzung von Videokonferenzsystemen ist darauf zu achten, dass datenschutzfreundliche Voreinstellungen getroffen werden. So sollten das Mikrofon und die Kamera bei der Anmeldung stets deaktiviert sein, sodass die Nutzenden selbst entscheiden können, ob und wann sie das Mikrofon und die Kamera aktivieren.

Online-Beratungsgespräche

Während der Corona-Pandemie durften Beratungsstellen zeitweise keine persönlichen Vor-Ort-Beratungen für Menschen in Lebenskrisen durchführen. Zur Erfüllung ihrer Aufgaben und zur Deckung des Beratungsbedarfs erkundigten sich im Berichtszeitraum daher verschiedene Beratungsstellen nach einem datenschutzkonformen Einsatz von Videokonferenzsystemen bei der Durchführung von Beratungsgesprächen.

Bei der datenschutzrechtlichen Bewertung war zu berücksichtigen, dass Beratungen in der Regel durch **Berufsgeheimnisträger** erfolgen und die Gesprächsinhalte **höchstpersönliche** und **sensible Informationen**, die als besondere Kategorien personenbezogener Daten besonders schützenswert sind, umfassen. Aufgrund dessen wurde den Beratungsstellen empfohlen, vor dem Einsatz eines konkreten Videokonferenzsystems

eine **Datenschutz-Folgenabschätzung** nach § 34 DSG-EKD durchzuführen.

Allgemein ist bei der Durchführung einer Datenschutz-Folgenabschätzung zu beachten, dass diese **objektiv** und **ergebnisoffen** zu erfolgen hat. Auf jeder Stufe der Prüfung kann die verantwortliche Stelle zu dem Ergebnis kommen, dass die Verarbeitung nicht datenschutzkonform durchführbar ist. Mit den Verarbeitungsvorgängen darf dann nicht begonnen werden. Eine Datenschutz-Folgenabschätzung folgt einem gesetzlich vorgeschriebenen Vorgehen und beginnt grundsätzlich mit einer **systematischen Beschreibung der geplanten Verarbeitungsvorgänge**. Dabei muss die Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Anbahnung, Durchführung und Beendigung einer Beratung über einen Videokonferenzdienst betrachtet werden. Dazu gehört beispielsweise, dass die Beratungsstelle einen Beratungstermin in dem Videokonferenzdienst anlegt und anschließend die Kontaktdaten der zu beratenden Personen zur Übermittlung der Zugangsdaten verarbeitet. Die zu Beratenden müssen sich zur Teilnahme an der Besprechung beim Videokonferenzdienst einwählen. Im Rahmen der Einwahl werden **Telemetrie-, Meta- und Verbindungsdaten** von dem Videokonferenzdienst neben den **Video**- und **Audiodaten** im Auftrag der Beratungsstelle verarbeitet.

Der systematischen Beschreibung der geplanten Verarbeitungsvorgänge folgt in einem weiteren Schritt die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge. Die **Bewertung der Notwendigkeit und Verhältnismäßigkeit** der Verarbeitungsvorgänge umfasst immer die Prüfung von datenschutzfreundlicheren Alternativen.

Auf der Grundlage der Datenströme müssen die **Risiken für die Rechte und Freiheiten der betroffenen Personen bewertet** werden. Ein Risiko wird definiert als die Möglichkeit des Eintritts eines Ereignisses, das einen Schaden für die Freiheiten und Rechte betroffener Personen darstellt oder zu einem solchen für eine oder mehrere natürliche Personen führen kann. Die Bewertung von Risiken gliedert sich in zwei zusammenhängende Aspekte, nämlich die Bewertung eines Lebenssachverhalts als risikohaft und der Folgen bei Eintritt des Risikos. Insoweit hat das mögliche Risiko zwei Dimensionen: **Schadenshöhe** und **Eintrittswahrscheinlichkeit**. Es ist die Möglichkeit des **Eintritts eines schadensverursachenden Ereignisses** zu prüfen.

Eine Bewertung von Risiken bedeutet für den Einsatz von Videokonferenzdiensten in Beratungsstellen, dass anhand des **Lebenssachverhalts** und der **Datenströme** geprüft werden muss, wie und wodurch Informationen über die zu Beratenden an Unbefugte gelangen und welche **negativen Folgen** sich daraus für die zu Beratenden ergeben können. So ist beispielsweise zu prüfen, wie hoch das Risiko ist, dass Familienangehörige oder sonstige Dritte durch eine Kontaktaufnahme durch die Beratungsstelle über die vereinbarte Beratung der betroffenen Person informiert werden können.

Die verantwortliche Stelle muss auf der Grundlage der **erkannten Risiken** und der drohenden **Folgen** im Hinblick auf Schadenshöhe und Eintrittswahrscheinlichkeit für die betroffenen Personen prüfen, welche technischen und organisatorischen **Abhilfemaßnahmen** erforderlich sind. Hierzu stellt sie jeweils den erkannten Risiken in Frage kommende Abhilfemaßnahmen gegenüber. Abhilfemaßnahmen können beispielsweise die **Verschlüsselung** oder die **Pseudonymisierung** von personenbezogenen Daten sein.

Die verantwortliche Stelle muss sich darüber im Klaren sein, dass bestimmte Risiken mit den zur Verfügung stehenden Abhilfemaßnahmen nicht bewältigt werden können. Aus diesem Grund müssen die ausgewählten Abhilfemaßnahmen immer auch auf ihre **tatsächliche Wirksamkeit** überprüft werden. Noch an dieser Stelle kann die verantwortliche Stelle zu dem Ergebnis kommen, dass ein voraussichtlich hohes Risiko für die Rechte der betroffenen Personen besteht, das auch nicht durch Abhilfemaßnahmen minimiert werden kann. Mit der Verarbeitung darf in diesem Fall nicht begonnen werden.

Sofern die Beratungsstelle nach der Durchführung der Datenschutz-Folgenabschätzung zu dem Ergebnis gelangt, dass die mit dem Einsatz des konkreten Videokonferenzdienstes verbundenen Risiken für den Schutz personenbezogener Daten **vertretbar** sind, kann mit den damit verbundenen Verarbeitungsvorgängen begonnen werden. Die Datenschutz-Folgenabschätzung muss jedoch im Sinne des **Plan-Do-Check-Act-Zyklus** regelmäßig, idealerweise jährlich, erneut durchlaufen werden. Mit der Zeit ändern sich die Technik oder die

datenschutzrechtlichen Anforderungen. In den Markt können neue Anbieter eintreten, die mit ihren Diensten die Anforderungen besser erfüllen und damit die Erforderlichkeit und die Notwendigkeit des bisherigen Anbieters in Frage stellen.

Fazit: Vor dem Einsatz eines Videokonferenzsystems ist im Rahmen einer Datenschutz-Folgenabschätzung zu prüfen, welche personenbezogenen Daten verarbeitet werden und wie hoch das Risiko für den Schutz der personenbezogenen Daten ist. Es sind technische und organisatorische Maßnahmen zu ergreifen, um das Risiko möglichst gering zu halten.

Kameras überall?!

Die Videoüberwachung öffentlicher und nichtöffentlicher Bereiche wird in kirchlichen und diakonischen Einrichtungen immer häufiger eingesetzt. Der Themenkomplex bringt vielseitige datenschutzrechtliche Fragen und Probleme mit sich, mit denen sich der BfD EKD im Berichtszeitraum im Rahmen von Datenschutzbeschwerden und Beratungsanfragen intensiv beschäftigt hat.

Entstehen bei einer Videoüberwachung biometrische Daten?

Seit der Novellierung der Datenschutzgesetze im Jahr 2018 fallen biometrische Daten unter die besonderen Kategorien personenbezogener Daten. Im Zusammenhang mit der Videoüberwachung ergab sich daher die Frage, ob das Thema Videoüberwachung **nun grundsätzlich nach § 13 DSG-EKD** zu beurteilen ist, da dabei **biometrische Daten** und somit besondere Kategorien personenbezogener Daten verarbeitet werden können.

Tatsächlich eignen sich Lichtbilder und auch Videoaufzeichnungen zur Identifizierung von Personen, sodass der Anwendungsbereich eröffnet wäre. Dazu muss aber noch der Umstand treten, dass durch die verantwortliche Stelle auch tatsächlich solche Identifizierungen durchgeführt werden. Dies wäre der Fall, wenn Gesichtserkennungssoftware eingesetzt und Daten tatsächlich ausgewertet werden. Fehlt es an einer solchen Verarbeitung, fallen Videoaufzeichnungen nicht in den Anwendungsbereich des § 13 DSG-EKD, sondern sind an den grundsätzlichen Maßstäben (in der Regel § 52 DSG-EKD) zu messen. Ähnliches gilt auch für andere besondere Kategorien personenbezogener Daten, wie **Gesundheitsdaten**. Auch hier ist eine enge Auslegung des § 13 DSG-EKD angezeigt, da sonst beispielsweise Brillenträger auf der Videoüberwachung bereits den Anwendungsbereich eröffneten. Soweit die Videoüberwachung die Erhebung sensibler Daten **nicht bezweckt** und auch **keine Auswertungsabsicht** bezüglich dieser Daten besteht, entfaltet die Videoüberwachung nach dieser Ansicht keine Gefahr für die Rechte und Freiheiten der betroffenen Personen.

Überwachungskameras auf einem Kita-Gelände

Das Instrument der Videoüberwachung gewinnt auch in kirchlichen und diakonischen Einrichtungen immer mehr an Bedeutung. Nicht immer werden dabei im Vorfeld die Anforderungen, die das EKD-Datenschutzgesetz an eine rechtmäßige Videoüberwachung stellt, in ausreichendem Maße berücksichtigt. So erreichte den BfD EKD im Berichtszeitraum eine Beschwerde, die sich gegen eine Videoüberwachung im Umfeld einer Kindertageseinrichtung richtete.

In der Vergangenheit war diese Kindertageseinrichtung mehrfach das **Ziel von Einbruchdiebstählen** geworden. Aus diesem Grund fasste die Trägerin der Kindertageseinrichtung den Entschluss, das Gelände der Kindertageseinrichtung mit mehreren Überwachungskameras auszustatten. Im Rahmen der Bearbeitung der Beschwerde hat der BfD EKD festgestellt, dass die Videoüberwachung an mehreren Stellen **nicht datenschutzkonform** erfolgt ist.

Vor dem Einsatz der Videokameras im Außenbereich der Kindertageseinrichtung hätte aufgrund des voraussichtlich hohen Risikos für die Rechte natürlicher Personen eine **Datenschutz-Folgenabschätzung** gemäß § 34 DSG-EKD durchgeführt werden müssen.

Das **hohe Risiko** ergab sich zum einen daraus, dass Videokameras von einem US-amerikanischen Anbieter ausgewählt wurden, bei deren Nutzung nicht ausgeschlossen werden konnte, dass **personenbezogene Daten in die USA übermittelt** werden. So wurde beispielsweise vorab nicht geklärt, ob die Bewegungserken-

nung auf den Servern des Dienstleisters verarbeitet wird und ob der Dienstleister eigene Zwecke bei der Verarbeitung verfolgt. Auch wurde nicht berücksichtigt, dass bei der Nutzung der zu den Videokameras gehörenden App personenbezogene Daten des Nutzenden der App verarbeitet und in die USA übermittelt werden. Dieses Risiko hätte vor der Nutzung der Videokameras sowie der dazugehörigen App betrachtet und bewertet werden müssen. Zum anderen folgte das hohe Risiko für die Rechte natürlicher Personen daraus, dass vor allem **Kinder** und **Beschäftigte** der Kindertageseinrichtung von der Verarbeitung der personenbezogenen Daten betroffen waren. Die personenbezogenen Daten von **Kindern** sowie von **Beschäftigten** unterliegen einem besonderen Schutz**.** Die Trägerin der Kindertageseinrichtung hätte daher besonders sorgfältig prüfen müssen, ob eine Verarbeitung dieser personenbezogenen Daten tatsächlich zulässig und erforderlich ist.

Im Rahmen der Datenschutz-Folgenabschätzung hätte die Trägerin prüfen müssen, ob und welche personenbezogenen Daten durch die Verwendung der Videokameras und durch die Nutzung der App in die USA übermittelt werden, auf welche **Rechtsgrundlage** die Übermittlung gestützt werden kann, welche **Risiken** dadurch für die von der Verarbeitung betroffenen Personen entstehen und welche **technischen und organisatorischen Maßnahmen** zum Schutz der personenbezogenen Daten hätten getroffen werden müssen. Auch wäre zu berücksichtigen gewesen, ob der mit der Videoüberwachung verfolgte Zweck nicht auch durch **mildere gleichwirksame Mittel** hätte erreicht werden können.

Vor dem Einsatz der Videokameras hat die Trägerin der Kindertageseinrichtung nicht geprüft, ob und welche personenbezogenen Daten durch die Videoüberwachung in die **USA übermittelt** werden und ob für eine Übermittlung dieser Daten eine **Rechtsgrundlage** gegeben ist. Auch die **Risiken**, die mit der Videoüberwachung verbunden sind, wurden im Vorfeld nicht berücksichtigt.

Darüber hinaus wurden **keine ausreichenden technischen und organisatorischen Maßnahmen** zum Schutz der personenbezogenen Daten getroffen. Das von der Trägerin ausgewählte System war in erster Linie für den Privatgebrauch gedacht und verfügte beispielsweise nicht über eine Anbindungsmöglichkeit an polizeiliche Alarmzentralen. Aus diesem Grund wurde die zu dem System gehörende App auf dem **privaten Smartphone** der Kita-Leitung installiert, auf dem rund um die Uhr ein entsprechender Alarm ausgelöst wurde, sobald die Videokameras eine Bewegung aufgenommen haben. Unabhängig davon, dass es bereits aus **Sicht des Arbeitsschutzes** bedenklich erscheint, dass die Leitung einer Kindertageseinrichtung jederzeit – auch außerhalb der Dienstzeit – den Einbruchschutz überwachen muss, so war darin auch ein Verstoß gegen **§ 27 Abs. 1 DSG-EKD** zu sehen. Gemäß § 27 Abs. 1 DSG-EKD hat die verantwortliche Stelle geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Auswahl der technischen und organisatorischen Maßnahmen sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Durch die Nutzung der App auf dem privaten Smartphone wurden personenbezogene Daten der Kita-Leitung verarbeitet und in die USA übermittelt. Dies hätte durch die Nutzung dienstlicher Endgeräte verhindert werden müssen. Aus welchem Grund keine dienstlichen Endgeräte zur Verfügung gestellt wurden, hat die Trägerin weder begründet noch dokumentiert.

Die Videoüberwachung war vorliegend auch **nicht verhältnismäßig**. So waren Videokameras auch zu Zeiten aktiv, zu denen sich noch Beschäftigte und Kinder auf dem Gelände aufgehalten haben. Da die Videoüberwachung jedoch zum Zweck der Verhinderung von Einbrüchen installiert wurde und Einbrüche in der Regel zu Zeiten stattfinden, in denen sich niemand auf dem Gelände aufhält, war es **nicht erforderlich**, dass die Videokameras bereits während der Arbeits- und Betreuungszeit aktiv waren. Zum Schutz der personenbezogenen Daten der Kinder und der Beschäftigten wäre es ausreichend gewesen, die Videokameras erst dann einzuschalten, wenn alle Kinder und alle Beschäftigte das Gelände der Kindertageseinrichtung verlassen haben.

Ein weiterer datenschutzrechtlicher Verstoß wurde aufgrund der **Verletzung der Informationspflichten** nach § 52 Abs. 2 DSG-EKD festgestellt. So wurden weder die Beschäftigten und die Erziehungsberechtigten noch die allgemeine Öffentlichkeit über die Tatsache und den Umfang der Videoüberwachung hinreichend informiert.

Zwar hat die Kindertageseinrichtung durch **Hinweisschilder** auf den Umstand der Videoüberwachung hingewiesen, diese enthielten aber nicht den gesetzlich vorgeschriebenen Inhalt. Auch andere Informationswege wurden nicht genutzt.

Aufgrund der Vielzahl der Verstöße gegen datenschutzrechtliche Bestimmungen hat der BfD EKD auf die Deinstallation der Videokameras hingewirkt und die Verstöße beanstandet.

Fazit: Vor der Installation einer Videoüberwachung muss die kirchliche Stelle vorab prüfen, ob die Videoüberwachung zu einem legitimen Zweck erfolgt und ob nicht auch mildere gleichwirksame Mittel in Betracht kommen. Auch muss im Vorfeld eine Datenschutz-Folgenabschätzung gemäß § 34 DSG-EKD durchgeführt und dokumentiert werden.

Kameras in den Räumen einer Kita versteckt

Aus einer Kindertageseinrichtung erreichte den BfD EKD die Meldung, dass ein Mitarbeiter ohne Wissen der Kita-Leitung Kameras in der Einrichtung installiert hatte. Der Mitarbeiter war in der Vergangenheit zuständig für die Installation und Wartung der in der Kita genutzten IT-Technik. Für die Konfiguration benutzte er seine private E-Mail-Adresse.

Im Zuge der Erneuerung der vorhandenen IT-Technik wurden die **versteckten Kameras** gefunden. Eine Kamera befand sich im Gruppenraum des Mitarbeiters in einem Plüschtier, eine weitere war in der Küche angebracht. Zum Zeitpunkt der Entdeckung waren die Kameras nicht mehr in Betrieb. Durch eine Fachfirma wurde mittels forensischer Untersuchungen versucht, Aufschluss über eventuelle Datenspeicherungen zu erhalten. Bei einer Kamera konnten Fragmente aus dem Speicherchip wiederhergestellt werden. Darunter befanden sich auch einige Sequenzen mit Kindern. Eine **Identifikation der Kinder** auf diesen Aufnahmen konnte **trotz der geringen Auflösung** nicht ausgeschlossen werden.

Gegen den Mitarbeiter wurden straf- und arbeitsrechtliche Maßnahmen eingeleitet. Außerdem wurden die **sorgeberechtigten Personen der Kita-Kinder informiert** und ein Elternabend zu diesem Thema einberufen.

Fazit: Die Installation und Wartung von IT-Technik darf generell nur durch vertrauenswürdiges Fachpersonal auf Basis einer vertraglichen Grundlage erfolgen. Dabei dürfen keinesfalls private Accounts oder andere private Ressourcen in Anspruch genommen werden.

Videoüberwachung auch in nichtöffentlichen Bereichen erlaubt?

Die häufigste Form der Videoüberwachung ist die Überwachung öffentlich zugänglicher Bereiche, deren datenschutzrechtliche Zulässigkeit in § 52 DSG-EKD geregelt ist. Was ist aber, wenn Räume oder Bereiche überwacht werden sollen, die nicht öffentlich zugänglich sind und wann liegen solche Bereiche vor?

Von **öffentlich zugänglichen Bereichen** ist auszugehen, wenn diese von einem unbestimmten Personenkreis, der nur nach allgemeinen Merkmalen abzugrenzen ist, betreten und genutzt werden können. Des Weiteren müssen diese Bereiche auch ihrem Zweck nach dazu bestimmt sein, von einem unbestimmten Personenkreis betreten werden zu können. Dies muss sich entweder aus dem erkennbaren Willen der verantwortlichen Stelle oder einer entsprechenden Widmung des Bereiches ergeben. Letztlich kommt es auf die tatsächlich vorhandenen Nutzungsmöglichkeiten durch die Allgemeinheit an, wobei Eigentumsverhältnisse unerheblich sind. Öffentlich zugängliche Bereiche können im Übrigen auch dann vorliegen, wenn das Betreten erst nach Passieren eines Schalters oder nach dem Kauf eines Tickets möglich ist. Knüpft die Nutzungsmöglichkeit jedoch an differenzierende individuelle Voraussetzungen an und ist nur ein bestimmter Personenkreis zum Betreten bestimmt, handelt es sich um einen nichtöffentlichen Bereich im datenschutzrechtlichen Sinne.

Welche Möglichkeiten bestehen, wenn eine Videoüberwachung **im nichtöffentlich zugänglichen Bereich** stattfinden soll?

Ob eine Videoüberwachung nichtöffentlich zugänglicher Bereiche datenschutzrechtlich zulässig ist, kann nicht anhand von § 52 DSG-EKD beurteilt werden. § 52 DSG-EKD regelt die Zulässigkeit der Videoüberwachung ausschließlich für öffentlich zugängliche Bereiche. Da es keine spezielle Rechtsgrundlage für die Videoüberwachung nichtöffentlich zugänglicher Bereiche gibt, ist auf § 6 DSG-EKD und konkret auf **§ 6 Nr. 4 in Verbindung mit**

§ 6 Nr. 8 DSG-EKD zurückzugreifen. Dabei ist insbesondere zu prüfen, ob die mit der Videoüberwachung zusammenhängende Verarbeitung von personenbezogenen Daten zur Wahrung der **berechtigten Interessen der verantwortlichen Stelle sowie von Dritten erforderlich** ist. Weiterhin ist im Rahmen einer Interessenabwägung festzustellen, ob schutzwürdige Interessen der betroffenen Person an der Unterlassung der Videoüberwachung die Interessen der verantwortlichen Stelle an der Vornahme der Videoüberwachung überwiegen. Hier sind sowohl Rechte von Beschäftigten als auch von betroffenen Dritten relevant.

Eine Videoüberwachung nichtöffentlich zugänglicher Bereiche ist für unterschiedliche **Zwecke** denkbar. Von Bedeutung sind insbesondere solche Konstellationen, bei denen **Dritte**, die Dienstleistungen diakonischer Einrichtungen wahrnehmen, vor **Eigengefährdungen geschützt** werden müssen. Neben den Interessen der verantwortlichen Stelle können hier auch rechtliche Verpflichtungen wie **Obhuts- oder Fürsorgepflichten** im Raum stehen, die der verantwortlichen Stelle vertraglich oder gesetzlich auferlegt sind. Um diese wahrnehmen und Gefahrsituationen effektiver entgegentreten zu können, kann eine Videoüberwachung beispielsweise in **stationären Jugendhilfeeinrichtungen** für suizidgefährdete Jugendliche in Betracht kommen. Hier ist eine entsprechende **Einzelfallprüfung** vorzunehmen. Ausgangspunkt ist, dass es kein gleichwirksames milderes Mittel als die Videoüberwachung gibt. Bauliche Besonderheiten oder Personalmangel können in diesen Fällen nicht zur Begründung herangezogen werden. **Sozialräume** sind grundsätzlich aufgrund des erheblichen Eingriffs in das Persönlichkeitsrecht von der Überwachung ausgeschlossen.

Sofern die Videoaufzeichnungen für einen genau bestimmten Zeitraum gespeichert werden sollen, ist zu prüfen, ob die **Speicherung** und damit eine weitere Verarbeitung von personenbezogenen Daten datenschutzrechtlich zulässig und verhältnismäßig ist. Die getroffenen Maßnahmen sind zu dokumentieren und die betroffenen Personen gemäß §§ 17 ff. DSG-EKD transparent zu **informieren**. Soweit bei der Videoüberwachung nichtöffentlich zugänglicher Bereiche besondere Kategorien personenbezogener Daten verarbeitet werden, ist bei der Prüfung der Rechtmäßigkeit zusätzlich § 13 DSG-EKD zu berücksichtigen.

Fazit: Der Einsatz von Videoüberwachung ist auch in Bereichen möglich, die nichtöffentlich zugänglich sind. Dies bedarf wegen der Eingriffsintensität einer Datenschutz-Folgenabschätzung, ist aber in Einzelfällen datenschutzkonform möglich, soweit entsprechende Prüfungen und Dokumentationen durchgeführt wurden.

Einsatz von Kamera-Attrappen

Im Berichtszeitraum wurde die Frage gestellt, wie der Einsatz von Kamera-Attrappen datenschutzrechtlich zu bewerten ist. Zunächst gilt, dass beim Einsatz von Kamera-Attrappen **datenschutzrechtliche Vorschriften nicht zur Anwendung** kommen, da tatsächlich **keine personenbezogenen Daten** erhoben werden.

Wegen des vermeintlich andauernden Überwachungsdrucks können Kamera-Attrappen aber – abhängig von den Umständen des Einzelfalls – einen **Eingriff** in das aus Art. 2 GG hergeleitete **allgemeine Persönlichkeitsrecht** darstellen. Dies ist insbesondere dann anzunehmen, wenn nicht erkannt werden kann, ob tatsächlich eine bloße Attrappe oder – gegebenenfalls nach äußerlich nicht wahrnehmbarer technischer Veränderung – eine funktionsfähige Kamera betrieben wird. Aus dem Eingriff in das allgemeine Persönlichkeitsrecht können betroffene Personen gegebenenfalls weitere Ansprüche geltend machen. Eine Beeinträchtigung der Persönlichkeitsrechte kann ausgeschlossen werden, wenn für die Betroffenen nach entsprechender Information feststeht, dass es sich um eine Attrappe handelt. Dies wird nur in Geschäftsräumen mit geringer Kundenfrequenz möglich sein, wenn eine Attrappe zum Diebstahlsschutz installiert wird.

Fazit: Auch wenn Kamera-Attrappen datenschutzrechtlich nicht relevant sind, ist beim Einsatz Vorsicht geboten.

Datensicherheit, Verschlüsselung und Cookies

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

Sicherheitslücken und Cyberangriffe

In einem bisher nicht gekannten Ausmaß wurden kirchliche und diakonische Einrichtungen im Berichtszeitraum zum Ziel von Cyberangriffen. Bei diesen Angriffen wurden mit unterschiedlichen Methoden (unter anderem Verschlüsselungs- und Datendiebstahlstrojanern) entweder die **Verfügbarkeit und Integrität der IT-Systeme direkt bedroht oder mit den erbeuteten personenbezogenen Daten wirtschaftliche oder sonstige Schäden bei den Betroffenen erzeugt** (Identitätsdiebstahl). Einfallstor für die zum großen Teil automatisierten Angriffe, die von überall auf der Welt gestartet werden, sind oftmals Sicherheitslücken in einer unzureichend gesicherten IT-Infrastruktur.

In diesem Zusammenhang hat der BfD EKD die kirchlichen und diakonischen Einrichtungen zu den aktuellen Risiken und Gefahren beraten und sensibilisiert und Datenpannenmeldungen bearbeitet. Das Ziel des BfD EKD ist bei seinem beratenden und aufsichtlichen Handeln zu helfen, **zukünftige Datenschutzverletzungen** nach Möglichkeit zu verhindern und **im Schadensfall die notwendigen Konsequenzen zu ziehen**. Im Folgenden werden exemplarisch drei Fälle zu diesem Themenkomplex dargestellt:

„Hafnium“

Anfang März 2021 veröffentlichte Microsoft ein **außerplanmäßiges Sicherheitsupdate** zu vier Schwachstellen im häufig eingesetzten E-Mail-Programm **Exchange Server**. Betroffen waren die Versionen 2010 bis 2019.

Bereits im Januar 2021 hatten taiwanesische Sicherheitsforscher Microsoft auf die Schwachstellen und deren Ausnutzbarkeit für Cyberangriffe hingewiesen. Schon Ende Januar 2021 wurden Exchange Server weltweit durch die Hacker-Gruppe „Hafnium“ angegriffen. Ab Februar 2021 waren **Massenscans** durch Cyberkriminelle **nach verwundbaren Exchange Servern** erkennbar. Dennoch wurden erst im März 2021 die ersten Sicherheitspatchs ausgerollt. Zu diesem Zeitpunkt waren weltweit bereits **viele tausend Server kompromittiert**. Mit der Veröffentlichung vom 3. März 2021 startete eine beispiellose massenhafte Infektion aller per Internet erreichbaren und nicht aktualisierten Exchange Server. Administratoren hatten kaum eine Chance, zeitnah zu reagieren, zumal die ersten Patchs nicht einfach zu installieren waren.

Der Warnung des BSI mit der **höchsten Warnstufe „Rot“** vom 9. März 2021 schloss sich der BfD EKD am 11. März 2021 an und empfahl allen kirchlichen und diakonischen Stellen, unverzüglich die betroffenen Server auf **Kompromittieren** (d. h. Infektion mit Schadsoftware) **zu prüfen**, die empfohlenen **Sicherheitsupdates** unverzüglich einzuspielen und gegebenenfalls die Systeme **neu aufzusetzen**. Vom Hersteller und vom BSI wurden **Hinweise** und **Anleitungen** dazu veröffentlicht, wie eine erfolgte Infektion zu erkennen ist, welches Patch-Level die Installation aktuell aufweist und wie das Sicherheitsupdate zu erfolgen hat. Die Überprüfung, ob ein Exchange Server aktuell auf einem sicheren Stand ist, kann allerdings auch von außen über die Internet-Schnittstellen (über die die E-Mails von extern empfangen werden) erfolgen. Potenzielle Angreifer hatten und haben also die Möglichkeit, die Angreifbarkeit der Installationen mit einfachen Mitteln und sogar automatisiert abzufragen.

Wegen der enormen Zahl der betroffenen Installationen hat der BfD EKD die verantwortlichen Stellen angewiesen, die **Meldung einer Datenschutzverletzung** nach § 32 DSG-EKD nicht vorzunehmen, wenn lediglich eine initiale Infektion des Servers feststellbar war. Eine Meldung sollte erst dann erfolgen, wenn es tatsächlich zu nicht berechtigten Datenabflüssen oder sonstigen Schäden gekommen war. Leider gab es im Nachlauf mindestens einen Fall in einer kirchlichen Einrichtung, in dem die Sicherheitsupdates über Monate hinweg nicht eingespielt wurden und in der es Anfang 2022 einen Verschlüsselungsangriff gab, der durch rechtzeitiges Einspielen der Updates hätte verhindert werden können.

Fazit: Im Augenblick der Bekanntgabe einer Sicherheitslücke in einer weit verbreiteten Software ist mit einem explosionsartigen Ansteigen der Angriffsversuche auf diese Schwachstelle zu rechnen. Cyberkriminelle arbeiten inzwischen hoch automatisiert und scannen die verwundbaren Systeme weltweit. Ein permanentes Beobachten und Auswerten aller verfügbaren Informationen, ein schnelles Reagieren und das Durchführen einer gründlichen Risikoanalyse sind unbedingt notwendig. Die Sofortmaßnahmen können auch das vorübergehende Offline-Setzen bestimmter Dienste einschließen.

Die Prozesse des Patch-Managements sollten sowohl geplante als auch ungeplante Update-Aktionen abdecken.

„Log4Shell/Log4j“
Im Dezember 2021 wandte sich das BSI an die deutsche IT-Öffentlichkeit mit einer dringenden Warnung vor der soeben entdeckten **Schwachstelle** „Log4Shell“ in der weit verbreiteten **Java-Bibliothek** „Log4j“. Das BSI bewertete die Bedrohungslage als kritisch und empfahl, alle betroffenen Anwendungen bis zu einem Update durch den Hersteller zunächst **außer Betrieb** zu nehmen. Durch die Sicherheitslücke war es potenziellen Angreifern möglich, auf den betroffenen Servern **Schadsoftware zu installieren**, die dann zu einem späteren Zeitpunkt weitere Schadsoftware wie z. B. Verschlüsselungs- und Erpressungstrojaner nachgeladen hätte. International wurden schnell Fälle bekannt, in denen die Sicherheitslücke bereits zur Verseuchung von Servern mit Schadsoftware ausgenutzt worden war.

Der BfD EKD reagierte umgehend und empfahl am 13. Dezember 2021 allen kirchlichen und diakonischen Einrichtungen, die selbst Server betreiben oder bei einem Dienstleister nutzen, sich unverzüglich über die möglichen **Abhilfemaßnahmen** zu informieren und sofort alle notwendigen Schritte einzuleiten.

Die erste Aufgabe für die verantwortliche Stelle war, mit dem Softwarehersteller abzuklären, ob die fragliche Java-Bibliothek eingesetzt wird und – falls ja – wann der Hersteller ein **Update seines Produktes** ausliefern kann, welches die Bibliothek in einer neuen, nicht mehr von der Sicherheitslücke betroffenen Version verwendet. Danach musste die verantwortliche Stelle entscheiden, ob in dem Zeitraum bis zur Beseitigung der Schwachstelle die betroffene Software besser außer **Betrieb** bleiben sollte oder ob das Risiko eines Betriebes vertretbar war, beispielsweise, weil die Systeme nicht „von außen“ (d. h. über eine Internetverbindung) erreichbar waren.

Fazit: Durch die Industrialisierung der Softwareerstellung ist die Gefahr des Auftretens von flächendeckend verbreiteten Schwachstellen enorm gestiegen. Die Kommunikation mit den Softwareherstellern ist wichtig, um die „Lieferketten“ der Hersteller zu verstehen. Sobald ein Hersteller zu seinen Produkten ein Update zur Verfügung stellt, zumal wenn dies mit einem Hinweis auf akut entdeckte Sicherheitslücken verknüpft ist, sollten diese – nach Verifizierung der Information z. B. über das BSI – umgehend installiert werden.

Verschlüsselung und angedrohte Offenlegung bei einem Dienstleister
Von einem vollendeten und erfolgreichen Cyberangriff waren im Januar 2022 direkt und indirekt zehntausende kirchliche und diakonische Mitarbeitende betroffen, als die **IT-Systeme eines** versicherungsmathematischen **Dienstleisters durch** einen **Erpressungsangriff verschlüsselt** wurden. Zusätzlich wurden vom Angreifer **mehrere Gigabyte Daten abgezogen**, mit deren Veröffentlichung der Erpresser drohte.

Der Dienstleister ermittelt für Pensionskassen und sonstige Einrichtungen der Altersvorsorge die gesetzlich vorgeschriebenen Rückstellungen und bilanziellen Buchungen. Auch **viele kirchliche und diakonische Arbeitgeber und Zusatzversorgungskassen beauftragen** diesen **Dienstleister** mit der Ermittlung der korrekten Bewertung der aufgelaufenen Ansprüche der versicherten Personen. Dazu werden regelmäßig Datensätze mit personenbezogenen Daten der Versicherten an den Dienstleister übermittelt.

Nachdem der Dienstleister seine (kirchlichen) **Kunden** über den Angriff, den unberechtigten Datenabfluss und den potenziellen Datenverlust durch Verschlüsselung **informiert** hatte, ergab sich für die kirchlichen und diakonischen Stellen die Frage, ob die **betroffenen Personen nach § 33 DSG-EKD zu informieren** waren. Diese Benachrichtigung der betroffenen Personen ist immer dann gesetzlich vorgeschrieben, wenn durch die Datenschutzverletzung ein voraussichtlich **hohes Risiko** für die persönlichen Rechte der betroffenen Personen besteht (§ 33 Abs. 1 DSG-EKD). Eine nähere Betrachtung der betroffenen Datensätze zeigte, dass in vielen Fällen **nicht erforderliche personenbezogene** Daten an den Dienstleister **übertragen** wurden. So ist es für den Zweck der korrekten bilanziellen Bewertung von Rentenansprüchen nicht erforderlich, den **Klarnamen der Versicherten** zu übermitteln. Vielmehr reicht für diesen Zweck eine Identifizierbarkeit

durch eine (Personal-) Nummer völlig aus. Bei Verwendung der Personalnummer und Vermeidung des Klarnamens war der Datensatz dann aber hinreichend **pseudonymisiert**, da nicht davon auszugehen war, dass der Angreifer im Besitz einer Personalliste mit Personalnummern und Namen der Beschäftigten war. Gerade die unnötigen identifizierenden Klardaten in den Datensätzen führten dazu, dass in diesen Fällen ein hohes Risiko für die betroffenen Personen vorlag und diese betroffenen Personen insofern benachrichtigt werden mussten. In den Fällen, in denen die Datensätze hinreichend pseudonymisiert waren, war hingegen kein hohes Risiko zu erkennen, sodass auch keine Benachrichtigungspflicht bestand.

Fazit: Auch bei der zulässigen Übermittlung von personenbezogenen Daten ist die Zweckbindung und das Prinzip der Datenminimierung zu beachten. Auch ohne vollständige Anonymisierung reduziert bereits jede Verwendung von Pseudonymen das Risiko eines Schadeneintritts und für die betroffenen Personen das Risiko, Opfer einer Datenschutzverletzung zu werden.

IT-Angriffe mit Ransomware

Im Berichtszeitraum gab es mehrere Datenpannenmeldungen, die den Befall der IT-Systeme von kirchlichen oder diakonischen Stellen oder auch von deren IT-Dienstleistern mit Ransomware betrafen. Bei Ransomware handelt es sich um Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder das ganze Computersystem verhindern kann. In allen Fällen zeigten sich bei den kirchlichen und diakonischen Stellen die typischen Auswirkungen eines solchen **Verschlüsselungstrojaners**. Es wurden umfangreiche – teils vollständig vorhandene – Datenbestände inklusive der Datensicherungen unbefugt ausgelesen und verschlüsselt. In hinterlegten Textdateien wurde die Entschlüsselung von den Angreifern gegen Zahlung eines Lösegeldes angeboten. Im Falle einer Nichtzahlung wurde gedroht, die erbeuteten Daten im Internet zu veröffentlichen.

Die **technischen Gründe für den Virenbefall** waren bei den kirchlichen und diakonischen Stellen unterschiedlich. In einem Fall wurde zum Beispiel eine vorhandene php-Sicherheitslücke in Verbindung mit einer offenen Zugriffsmöglichkeit aus dem Internet auf einem auch aus dem Internet erreichbaren Datenspeicher, sogenanntes NAS (Network Attached Storage) ausgenutzt. In einem anderen Fall wurde ein Phishing-Angriff mit einem E-Mail-Anhang festgestellt. In einigen Fällen konnte der konkrete Grund für den Virenbefall nicht mehr ermittelt werden. Entsprechend der Empfehlung des BSI bezüglich eines Ransomware-Angriffs rät auch der BfD EKD den betroffenen Einrichtungen, auf keinen Fall auf Lösegeldforderungen einzugehen. Befallene Systeme müssen vollständig **neu aufgesetzt** und **eingerichtet** werden.

Um gegen IT-Angriffe mit Ransomware zukünftig besser geschützt zu sein, rät der BfD EKD die folgenden IT-Managementkonzepte zu erarbeiten und umzusetzen:

- **Datensicherungskonzept zur Backup-Strategie:** Für eine Neueinrichtung der IT-Systeme sind funktionierende Datensicherungen essenziell. Als Vorbeugung vor einem kompletten Datenverlust durch Ransomware sind Datensicherungen immer räumlich getrennt von den Livedaten aufzubewahren, damit sie nicht selbst durch die Schadsoftware unbrauchbar werden. Speichermedien für die Datensicherung sollten nur während der Datensicherung und Datenwiederherstellung mit dem Netz der kirchlichen oder diakonischen Einrichtung oder dem Livesystem verbunden werden. Es sollte auch regelmäßig getestet werden, ob der Prozess einer Datenwiederherstellung fehlerfrei durchgeführt werden kann.

- **Update-/Patchmanagement:** Alle vorhandenen Systeme sind aktuell zu halten. Vorhandene Updates und Sicherheitspatchs sind nach Veröffentlichung durch die Hersteller unverzüglich zu installieren, um Angriffe durch die Ausnutzung bereits behobener Sicherheitslücken zu verhindern. Virenschutzprogramme sind zu aktivieren. Auch hier sind regelmäßige Updates (mindestens täglich!) erforderlich.

- **Berechtigungskonzept:** Berechtigungen für das Ausführen von Software und den Zugriff auf Daten müssen restriktiv erfolgen. Nutzer dürfen nur die Zugriffsberechtigungen auf Programme und Daten erhalten, die sie wirklich benötigen. Administrato-

ren-Accounts sollten nur für Administrationstätigkeiten verwendet werden.

- **Mitarbeitendensensibilisierung:** Regelmäßige Schulungen der Beschäftigten sind unerlässlich. E-Mails mit Schadsoftware in Verbindung mit dem unachtsamen Verhalten der Mitarbeitenden sind das Haupteinfallstor für Schadsoftware. Es sollten keine E-Mails und Anhänge von unbekannten oder unseriösen Absendern geöffnet oder auf Links in diesen E-Mails und deren Anhängen geklickt werden.

Gefahr durch Phishing E-Mails

Bei kirchlichen und diakonischen Stellen sind im Berichtszeitraum vermehrt Phishing E-Mails eingegangen. Unter einer Phishing E-Mail versteht man Versuche, sich über gefälschte E-Mails als vertrauenswürdiger Absender in einer elektronischen Kommunikation auszugeben. Ziel ist es, an persönliche Daten der E-Mail Empfangenden zu gelangen oder die Empfangenden zur Ausführung einer schädlichen Aktion zu bewegen. In der Folge werden dann beispielsweise Kontoplünderungen oder Identitätsdiebstähle begangen oder eine Schadsoftware installiert.

Im konkreten Fall wurde ein Mitarbeiter einer kirchlichen Stelle im Rahmen einer E-Mail dazu aufgefordert, die **Zugangsdaten für seinen dienstlichen E-Mail-Account** wegen angeblicher Wartungsarbeiten **preiszugeben**. Der Inhalt und das Aussehen der E-Mail machten einen professionellen Eindruck, sodass nicht ohne weiteres zu erkennen war, dass es sich bei der **E-Mail** um eine **Fälschung** handelte. Hinter der E-Mail-Adresse verbarg sich nicht der angegebene Adressat, sondern ein Server, der den von dem Mitarbeiter eingegebenen Benutzernamen und das Kennwort sofort speicherte. Mithilfe dieser Zugangsdaten wurden anschließend eine Vielzahl von E-Mails verschickt, wodurch bei den Empfangenden der Eindruck entstand, die E-Mail würde von dem Mitarbeiter der kirchlichen Stelle stammen. Tatsächlich enthielten die E-Mails einen Link, bei dessen Anklicken das jeweilige **Endgerät mit einem Schadcode** infiziert wurde.

Nach dem Erkennen des Vorfalls hat die kirchliche Stelle das **Kennwort** für den E-Mail-Account unverzüglich **geändert** und die **betroffenen Personen** – soweit möglich – **informiert**. Darüber hinaus wurde der Angriff einer zentralen Abwehrstelle für Cybercrime gemeldet.

Fazit: Zunehmend sind professionell gestaltete Phishing E-Mails im Umlauf, die auch den Kontext des E-Mail-Empfangenden widerspiegeln. Kirchlichen und diakonischen Stellen wird empfohlen, die Mitarbeitenden regelmäßig zu sensibilisieren und vor Phishing E-Mails zu warnen.

Verwendung des Telefaxes

Kirchliche und diakonische Stellen haben den BfD EKD im Berichtszeitraum mehrfach um Beratung zur datenschutzrechtlichen Bewertung des Telefaxdienstes und um Unterstützung bei der Neuausrichtung ihrer Kommunikationskanäle gebeten. Staatliche Datenschutzaufsichtsbehörden haben sich im Berichtszeitraum immer wieder dahingehend geäußert, dass die ursprünglich rein analogen Dienste Telefonie und Telefax immer mehr mit einer E-Mail vergleichbar seien. Deshalb seien zur Bewertung der datenschutzrechtlichen Zulässigkeit ähnliche Kriterien wie bei der elektronischen Post anzuwenden und eventuell vorhandene Privilegierungen der Datenübermittlung per Telefax nicht mehr zu rechtfertigen.

Die allgemein zu beobachtende Annäherung von Internet- und Telekommunikationstechnologien hin zu **IP-basierten Anschlüssen** hat auch Auswirkungen auf die Nutzung von Faxgeräten. Die Benutzenden nehmen beim Fax – als auch bei der Telefonie – zwischen analogen/ISDN- und IP-basierten Anschlüssen keine Unterschiede wahr, auch wenn die **technische Umsetzung** grundlegend voneinander abweicht. Wurde beim analogen Fax und auch noch beim digitalen ISDN-Fax eine Verbindung zwischen den beiden kommunizierenden Geräten aufgebaut und flossen Datenströme über diese vermittelte Leitung, so erfolgt die Datenübermittlung bei IP-basierter Kommunikation – wie allgemein im Internet – **„paketvermittelt“**, ohne dass vorher genau bestimmt werden kann, welchen Weg einzelne Datenpakete zwischen den Sendenden und den Empfangenden nehmen werden. Fax over IP erbt damit als IP-basierte Anwendung die Bedrohungen und Gefährdungen des genutzten IP-Netzes. Bei allen Technologievarianten nehmen die Benutzenden aber weiterhin

wahr, dass Fax-Empfangende eine identische Kopie des Originals erhalten.

Tatsächlich erfolgt jedoch eine mehrfache Umwandlung analoger Informationen in digitale Werte und zurück, bevor die Kopie auf der Empfängerseite angekommen ist. Die Anzahl der **Transformierungen** (Codierungen/ Decodierungen) steigt von der reinen analogen Leitungsvermittlung über die Nutzung digitaler Übertragungswege für herkömmliche Endgeräte bis hin zur Nutzung von Software-Lösungen (ohne herkömmliche Faxgeräte) stetig an. Dieser wiederholte Wechsel der Darstellungsform ist den meisten Nutzenden nicht bewusst, verursacht aber **zusätzliche Risiken**. Insbesondere kann jedes digitale Datenpaket prinzipiell in jedem **Vermittlungsknoten** mitgeschnitten und – falls unverschlüsselt – als Klardaten ausgelesen werden. Zusätzlich kommt für die Sendenden die Unsicherheit hinzu, wie die **Daten bei den Empfangenden weiterverarbeitet** werden (z. B. Umwandlung in E-Mails und Weiterversand) und wo die **entgegennehmende Stelle lokalisiert** ist (z. B. im gleichen separaten Subnetz des eigenen Internet-Service-Providers oder aber bei einem Online Fax Service). Sobald die sendenden und die empfangenden Personen von unterschiedlichen Internet-Providern bedient werden, kann ein Routing auch über ausländische Vermittlungsknoten (deren Betreiber nicht dem deutschen Fernmeldegeheimnis unterliegen) nicht ausgeschlossen werden.

Um bei der Nutzung von Telefax-Diensten den Schutz von personenbezogenen Daten gewährleisten zu können, sind **technische und organisatorische Maßnahmen** erforderlich. Aus organisatorischer Sicht ist etwa der Aufstellungsort des Geräts, der Umgang mit Sende- und Empfangsprotokollen sowie die Anrufumleitung und -weiterschaltung entscheidend. Zu den technischen Maßnahmen gehören beispielsweise eine angemessene Zugangs- und Zugriffskontrolle sowie die Verschlüsselung. Bezüglich der Schutzmaßnahmen ist zu beachten, dass mit steigender Sensibilität der personenbezogenen Daten auch die Anforderungen an die einzusetzenden Sicherungsmaßnahmen für deren Übertragung steigen. Sind **besondere Kategorien personenbezogener Daten** betroffen, zu denen unter anderem Gesundheitsdaten gehören, kann eine unverschlüsselte Übertragung das geforderte Sicherheitsniveau nicht mehr gewährleisten, wenn die Übertragung außerhalb eines geschlossenen und gesicherten Netzwerkes stattfindet. Dies ist beispielsweise der Fall, sobald die Kommunikationspartner ihre IP-Anschlüsse von unterschiedlichen Internet Service Providern beziehen. Dies ist der Regelfall bei der Kommunikation mit externen Stellen.

Gerade im **Gesundheitswesen**, dem viele der diakonischen Einrichtungen zuzurechnen sind, gibt es seit mehreren Jahren Entwicklungen zur Digitalisierung des Schriftverkehrs und des Bereithaltens und Austauschens von patientenbezogenen Unterlagen. Bekanntestes Beispiel ist die elektronische Patientenakte (ePA), in der prinzipiell alle Unterlagen des Patienten unter dessen Datenhoheit vorgehalten werden können, damit die an der Behandlung beteiligten Stellen auf diese Unterlagen zugreifen können. Die Basis für die neuen Anwendungen im Gesundheitsbereich ist die Telematikinfrastruktur (TI) der gematik GmbH, die in einer nächsten Version softwarebasiert über ein föderiertes Identitätsmanagement (betrieben etwa durch die Ärztekammern und die Krankenkassen) zugänglich sein soll. Obwohl auch die TI immer mal wieder mit Sicherheitslücken und Datenschutzverletzungen zu kämpfen hat, ist davon auszugehen, dass diese Infrastruktur zumindest im Gesundheitswesen einen wichtigen Beitrag zu einer sicheren und datenschutzkonformen Digitalisierung leistet und leisten wird.

Im Gegensatz zu der Kommunikationsart E-Mail ist für das Telefax bzw. für Voice over IP allgemein **keine** offene, herstellerunabhängige **Verschlüsselungsmethode verfügbar**. Das gilt insbesondere, wenn der Vorgang „Versenden eines Telefaxes“ vom Papier auf der Senderseite bis zum ausgedruckten Bild auf der Empfängerseite gesehen wird. Somit ist die **Ende-zu-Ende-verschlüsselte E-Mail** in allen Fällen eine sichere Alternative zur Übertragung per Telefax. Durch zentral in einer Organisation verwaltete Zusatzprogramme oder Ergänzungen des E-Mail-Servers kann der Anwendende von zusätzlichem Aufwand entlastet werden. Zur Entlastung kommt beispielsweise eine zentrale Zertifikatsverwaltung für alle internen und externen Kommunikationspartner und die Verwendung eines Web-Portals zur TLS-gesicherten Bereitstellung

von Datei-Anlagen für bisher unbekannte Empfänger in Betracht.

Fazit: Bereits vor der Digitalisierung, als das Fax noch als sicheres Kommunikationsmittel galt, bestand immer schon das Risiko, dass Datenströme technisch abgegriffen werden.

Verlust von mobilen Endgeräten

Den BfD EKD erreichten im Berichtszeitraum eine Vielzahl von Datenpannenmeldungen über den Verlust von unverschlüsselten mobilen Endgeräten. So wurde beispielsweise in eine Einrichtung eingebrochen und ein Notebook entwendet. Auf dem Gerät waren personenbezogene Daten von Klienten und Klientinnen, darunter auch Kinder, gespeichert. **Das Notebook und die darauf gespeicherten personenbezogenen Daten** waren **nicht** in ausreichender Weise **vor dem Zugriff durch Unbefugte geschützt**.

Um zukünftig Fällen einer Verletzung des Schutzes personenbezogener Daten durch Verlust von mobilen Endgeräten vorzubeugen, wurden mit der verantwortlichen Stelle **Schutzmaßnahmen** besprochen. So sind zukünftig alle Notebooks mit Bitlocker und PIN gegen das fremde Auslesen der darauf gespeicherten personenbezogenen Daten zu **verschlüsseln**. Das Schutzkonzept umfasst zukünftig auch die Verschlüsselung von externen Speichermedien, zu denen beispielsweise USB-Sticks und Festplatten gehören.

Fazit: Die Vielzahl an Datenpannenmeldungen über den Verlust von unverschlüsselten mobilen Endgeräten und Datenträgern zeigt, dass die Verschlüsselung von Datenträgern noch immer nicht überall umgesetzt wird. Wenn Datenträger nicht verschlüsselt werden, dann ist es Unbefugten ohne größeren Aufwand möglich, alle Daten auszulesen und weiter zu verwenden. Aktuelle Betriebssysteme bieten mittlerweile eine einfache Möglichkeit zur Verschlüsselung der eingesetzten Speichermedien.

Einwilligungspflicht beim Einsatz von Telekommunikations- und Telemediendiensten

Gleichzeitig mit dem Inkrafttreten des neuen **Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)** zum 1. Dezember 2021 traten auch ein neues Telekommunikationsgesetz (TKG) und die Änderungen des Telemediengesetzes (TMG) in Kraft. Im neuen TTDSG werden die wesentlichen Datenschutzvorschriften für Telekommunikations- und Telemediendienste gebündelt. Seit diesen Gesetzesänderungen sind sowohl im TKG als auch im TMG keine Datenschutzvorschriften mehr enthalten. Anlass dieser Gesetzgebung war die Richtlinie 2018/1972/EU über den europäischen Kodex für die elektronische Kommunikation, die eine Änderung des TKG erforderlich machte.

Das TTDSG enthält unter anderem Regelungen zum Schutz der Privatsphäre bei der Nutzung von Endeinrichtungen (z. B. Computer oder Laptops), unabhängig davon, ob ein Personenbezug vorliegt oder nicht. Das TTDSG wirkt sich damit unter anderem auf den **Einsatz von Cookies und ähnlichen Technologien** aus und ist auch für kirchliche und diakonische Stellen relevant. Mit Cookies können Informationen auf den Endgeräten der Nutzenden abgelegt, angereichert und verwaltet werden. Bei der Verwendung eindeutiger Kennungen lassen diese eine Identifikation oder Zuordnung zu einer natürlichen Person zu. In der Praxis dienen diese Prozesse häufig dazu, das individuelle Verhalten der Nutzenden nachzuverfolgen und Profile über eine Person zu erstellen.

Die Erhebung dieser Daten und die weitere Verarbeitung dieser Informationen wird regelmäßig als ein einheitlicher Sachverhalt wahrgenommen. Rechtlich sind hier jedoch zwei Schritte zu unterscheiden. Erstens die **Speicherung von und der Zugriff auf Informationen in der Endeinrichtung** sowie zweitens die **Verarbeitung von personenbezogenen Daten**, die oftmals mit dem Einsatz von Cookies und ähnlichen Technologien bezweckt wird. Die Rechtmäßigkeit der Datenverarbeitung durch kirchliche und diakonische Stellen im zweiten Schritt richtet sich nach den Anforderungen des EKD-Datenschutzgesetzes. Die vorgelagerten technischen Prozesse – insbesondere das Setzen und Auslesen von Cookies – berühren jedoch (auch) die Integrität der Endeinrichtungen und fallen damit in den **Anwendungsbereich von § 25 TTDSG**. In dieser Norm ist geregelt, dass Internetseiten für den Einsatz von Cookies und von Tracking eine Einwilligung der Nutzenden benötigen. Ausnahmen sind nur unter engen Voraussetzungen zugelassen.

§ 25 Abs. 1 Satz 2 TTDSG verweist bezüglich der Informationspflichten gegenüber den Endnutzenden als auch in Bezug auf die formalen und inhaltlichen Anforderungen an eine **Einwilligung** auf die DSGVO. Für kirchliche und diakonische Stellen bedeutet dies, dass eine wirksame Einwilligung die Anforderungen nach § 11 DSG-EKD erfüllen muss. Insbesondere muss die Einwilligung freiwillig und informiert erfolgen und es ist auf die Möglichkeit des jederzeitigen Widerrufs hinzuweisen.

Eine **Ausnahme von der Einwilligungspflicht** ist in **§ 25 Abs. 2 Nr. 2 TTDSG** geregelt. Danach ist keine Einwilligung notwendig, wenn der Einsatz der Cookies oder die Einbindung von Drittdiensten **unbedingt erforderlich** ist, damit Anbieter die von den Nutzenden ausdrücklich gewünschten Telemediendienste zur Verfügung stellen können. Da es sich um eine Ausnahmeregelung handelt, ist grundsätzlich von einem engen Verständnis auszugehen, sodass es nur wenige Cookies und Drittdienste geben wird, die ohne eine Einwilligung auf der Internetseite eingesetzt werden können. Ob der Einsatz eines Cookies oder die Einbindung von Drittdiensten unbedingt erforderlich ist, ist unter anderem davon abhängig, welche Funktion oder welchen Dienst die Nutzenden von dem Telemediendienst ausdrücklich wünschen. Dabei ist zu beachten, dass erforderliche Cookies erst bei Inanspruchnahme des jeweiligen Dienstes gesetzt werden dürfen, also erst, wenn sich die Nutzenden beispielsweise auf einer Internetseite anmelden oder ein Produkt in den Warenkorb legen.

Eine Ausnahme von der Einwilligungspflicht kann beispielsweise für die Bereitstellung spezieller Informationen und Dienste nach einer Anmeldung auf einer Internetseite vorliegen. In diesen Fällen kann das Setzen eines sogenannten **Session-Cookies** für die Dauer des Verweilens auf allen Seiten dieses geschützten Bereiches bis zur Abmeldung und Schließen des Browsers als erforderlich eingestuft werden. Ein solches Session-Cookie ermöglicht dem Webserver die Unterscheidung der verschiedenen Nutzenden, die gleichzeitig auf die Internetseite zugreifen. Der Browser sendet das Cookie bei jedem Zugriff vom Endgerät. Dadurch müssen die Anwendenden zum Beispiel nicht bei jedem Seitenaufruf ihre Anmeldedaten erneut eingeben. Die Gültigkeit des Cookies sollte nur für jeweils eine Browser-Sitzung eingestellt sein. Darüber hinaus kann ein **Warenkorb-Cookie** bis zum erfolgreichen Abschluss einer Bestellung oder auch bis zum Schließen des Browsers erforderlich sein, um das Einkaufsverhalten während des Surfens in einem Shop zu speichern. Ebenfalls kann die Verwendung von Cookies im Rahmen von Bezahlfunktionen (Spenden, Bezahlvorgänge in einem Online-Shop u.ä.) während des Bezahlvorgangs als erforderlich angesehen werden.

Grundsätzlich **nicht erforderlich** und damit **einwilligungspflichtig** sind Personalisierungsfunktionen – beispielsweise für individuell angepasste Werbung – und Analysefunktionen. Solche Dienste werden generell nicht als Wunsch der Nutzenden, sondern als Interesse der Anbieter eingestuft. Das Gleiche gilt für die Einbindung von Drittdiensten wie zum Beispiel von YouTube-Videos und Google Maps. Das Setzen von Cookies (sogenannte Third Party Cookies) bedarf in diesen Fällen einer Einwilligung.

Zu berücksichtigen ist, dass es zur **Websiteanalyse** auch **Softwareprodukte** gibt, die ohne Cookies auskommen, wie z. B. Matomo. Ob bei der Nutzung solcher „cookielosen“ Analysetools trotzdem eine Einwilligung nach § 25 Abs. 1 TTDSG erforderlich ist, ist davon abhängig, welche Technologie dabei zum Einsatz kommt. Eine weit verbreitete Methode ist das sogenannte **„Fingerprinting“**, wobei verschiedene Daten des Endgerätes eines Webnutzenden, etwa Betriebssystem-Version, installierte Plugins, Auflösung oder installierte Schriften genutzt werden. Ein Algorithmus kann aus diesen Daten individuelle Nutzerprofile ableiten, sodass Nutzende eindeutig identifizierbar werden. Diese Methode bedarf einer Einwilligung nach § 25 TTDSG, wenn zusätzliche Informationen, die nicht standardmäßig bei jedem Aufruf einer Internetseite übermittelt werden, aus dem Endgerät ausgelesen werden. Eine andere Möglichkeit ist die **Logfile-Analyse.** Standardmäßig schreibt jeder Webserver aus Sicherheitsgründen ein Logfile, in dem diverse Informationen zu jedem Aufruf jeder Internetseite abgelegt werden. Wenn eine Anonymisierung (Kürzung) der IP-Adressen vorgenommen wird, können diese Informationen für statistische Auswertungen über die Websitenutzung datenschutzkonform genutzt werden. Eine Einwilligung der Websitenutzenden ist in diesen Fällen nicht erforderlich. Allerdings sollte die

Websiteanalyse in der Datenschutzerklärung aufgeführt werden.

Fazit: Alle kirchlichen Stellen müssen prüfen, ob auf ihren Internetseiten Cookies oder Drittdienste ohne eine wirksame Einwilligung eingesetzt werden. Sollte dies der Fall sein, ist weiter zu klären, ob es sich um Cookies oder Drittdienste handelt, für die die Ausnahmeregelung gemäß § 25 Abs. 2 Nr. 2 TTDSG greift. Bei Unsicherheiten in Bezug auf diese rechtliche Bewertung, sollte das Cookie oder der Drittdienst bis zur Klärung deaktiviert werden.

Softwareprüfung und -bewertung

Der datenschutzkonforme Einsatz von Software war im aktuellen Berichtszeitraum Gegenstand verschiedener Beratungsanfragen von kirchlichen und diakonischen Einrichtungen.

Betriebssystem Windows 10

Im Zuge der Schwerpunktprüfung in Kindertageseinrichtungen wurden vom BfD EKD die **Betriebssysteme** der in den Kindertageseinrichtungen eingesetzten Endgeräte abgefragt. Diese Frage zielte insbesondere auf die eingesetzten Windows-Versionen und Editionen ab, in denen deutliche Unterschiede hinsichtlich der Konfiguration der **Übermittlung von Telemetriedaten** bestehen. Doch nicht nur die Betriebssysteme selbst sammeln Daten, die an den Hersteller der jeweiligen Software übermittelt werden, sondern auch die Anwendungen. Hersteller sammeln zur Optimierung ihrer Produkte teilweise umfangreiche Daten über die Nutzung der Software. Darunter befinden sich auch personenbezogene Daten. Sie enthalten unter anderem Versionsangaben der eingesetzten Software, Nutzungsverhalten, Absturzberichte, aber eben auch Teile von Dokumenten.

Windows 10 verwendet das sogenannte „Event Tracing for Windows“ (ETW) für die Protokollierung von Telemetriedaten. Hierbei lässt sich ein **Telemetrie-Level konfigurieren**: Security, Basic, Enhanced, Full. Nur im Level Security lässt sich die Übermittlung von Telemetriedaten auf ein datenschutzkonformes Maß reduzieren. Zu diesem Schluss kamen mehrere Analysen und Studien, die von Arbeitsgruppen der Datenschutzkonferenz und der Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10 (SiSyPHuS-Studie Win10) des BSI durchgeführt wurden.

Das Level Security lässt sich nur in den **Editionen** Windows Professional, Enterprise und Education einstellen, nicht jedoch in der Edition Windows Home, die generell nur im Privatbereich eingesetzt werden darf. Auch ist für jede eingesetzte Anwendung zu hinterfragen, welche Telemetriedaten abfließen und inwieweit dies datenschutzkonform ist oder ob dies durch technische und organisatorische Maßnahmen eingeschränkt werden muss.

Software Microsoft 365

Das Thema „datenschutzkonformer Einsatz von Microsoft 365“ hat den BfD EKD auch im Berichtszeitraum durch Anfragen verschiedener kirchlicher und diakonischer Stellen beschäftigt.

Microsoft 365 (ehemals Office 365) ist eine Softwarelösung der Microsoft Corporation, die verschiedene **Anwendungen** – insbesondere E-Mailing, Textverarbeitung, Tabellenkalkulation, Präsentationen und Datenbanken – umfasst.

Hinsichtlich des **technischen Betriebs** bestehen verschiedene Ausprägungen. So existieren Versionen, die den Betrieb auf der eigenen IT-Infrastruktur der verantwortlichen Stelle oder eines Dienstleisters erlauben sowie Versionen auf der Grundlage von Webanwendungen bzw. Cloud-Funktionalitäten.

Eine generelle und allgemeine Bewertung ist daher nicht möglich. Die verantwortliche Stelle muss für **jeden einzelnen Dienst** der Softwarelösung Microsoft 365 individuell prüfen, ob ein datenschutzkonformer Einsatz im Hinblick auf die Verarbeitungstätigkeit möglich ist.

Im Folgenden soll die Nutzung von Microsoft 365 und die diesbezüglich bestehenden datenschutzrechtlichen Bedenken zunächst aus **rechtlicher** und anschließend aus **technischer Perspektive** eingeschätzt werden.

Einschätzungen aus rechtlicher Perspektive

Aus rechtlicher Perspektive sind insbesondere die

Vorgaben des EKD-Datenschutzgesetzes, sonstige anzuwendende Gesetze zum Datenschutz sowie die einschlägige europäische und nationale Rechtsprechung zu berücksichtigen. Wichtig ist, dass die datenschutzrechtliche Zulässigkeit der Verarbeitung von personenbezogenen Daten in Bezug auf die **Nutzung der einzelnen Dienste** von Microsoft 365 geprüft und skizziert wird. Es ist nicht möglich, die datenschutzrechtliche Zulässigkeit von Microsoft 365 als einen Dienst insgesamt zu beurteilen.

Bei jeder Verarbeitung von personenbezogenen Daten sind die in **§ 5 Abs. 1 DSG-EKD** genannten Grundsätze der Datenverarbeitung zu beachten. Zu den Grundsätzen gehören insbesondere die Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz sowie die Integrität und Vertraulichkeit. Die verantwortliche Stelle muss gemäß **§ 5 Abs. 2 DSG-EKD** die Einhaltung dieser Grundsätze nachweisen können (Rechenschaftspflicht) und hierfür die erforderlichen Dokumentationen und Nachweise (z. B. Datenschutz-Folgenabschätzung) erstellen.

Die **Rechenschaftspflicht** ist mit Blick auf den jeweiligen Dienst dann erfüllt, wenn die verantwortliche Stelle Folgendes nachweisen kann und dokumentiert hat:

- Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten gemäß § 6 bzw. § 49 DSG-EKD
- Zulässigkeit der Datenübermittlung an und in Drittländer oder an internationale Organisationen auf der Grundlage von § 10 DSG-EKD
- Durchführung einer Datenschutz-Folgenabschätzung auf der Grundlage von § 34 DSG-EKD

§ 5 Abs. 1 Nr. 1 DSG-EKD legt als zentralen Grundsatz fest, dass personenbezogene Daten nur **rechtmäßig verarbeitet** werden dürfen. Daraus folgt, dass für jede Verarbeitung von personenbezogenen Daten innerhalb der einzelnen Dienste von Microsoft 365 eine **Rechtsgrundlage** gegeben sein muss. Die einschlägigen Rechtsgrundlagen sind zum Zweck der Nachweisbarkeit zu dokumentieren.

Werden innerhalb eines Dienstes von Microsoft 365 personenbezogene Daten in ein **Drittland** – insbesondere in die USA – **übermittelt**, ist zu prüfen, ob neben der Datenverarbeitung auch für die Datenübermittlung eine Rechtsgrundlage gegeben ist. Für die Bestimmung der Rechtsgrundlage ist § 10 DSG-EKD heranzuziehen. An dieser Stelle ist zu beachten, dass eine zulässige Übermittlung von personenbezogenen Daten in die USA aktuell nur unter **engen Voraussetzungen** zulässig ist.

Neben der Rechtmäßigkeit der Datenverarbeitung erfordert der Einsatz einzelner Dienste von Microsoft 365 eine **Schwellwertanalyse**. Eine Schwellwertanalyse sollte zu dem Ergebnis kommen, dass bei der Nutzung der jeweiligen Dienste von Microsoft 365 eine neue Technologie im Bereich der Verarbeitung von personenbezogenen Daten mit voraussichtlich hohem Risiko für die Rechte natürlicher Personen eingesetzt wird und daher eine **Datenschutz-Folgenabschätzung** gemäß § 34 DSG-EKD erforderlich ist.

Im Rahmen der Datenschutz-Folgenabschätzung ist zunächst eine **systematische Beschreibung** der **tatsächlichen Verarbeitungsvorgänge** vorzunehmen. Dabei muss ausgeführt werden, wie die **Datenströme,** insbesondere auch der Telemetrie- und Diagnosedaten, aussehen. Diese Beschreibung ist in Bezug auf die einzelnen Dienste von Microsoft 365 oft nicht möglich, da Microsoft keine detaillierten Informationen zur Verfügung stellt. In diesem Fall müsste die Datenschutz-Folgenabschätzung an dieser Stelle beendet werden. Auf der Ebene der **Bewertungsphase** führt die unvollständige Beschreibung der Verarbeitungsvorgänge dazu, dass die Gegenüberstellung und anschließende Bewertung der Risiken für die betroffenen Personen ebenfalls nicht vollständig möglich ist. Eine unvollständige Risikobewertung führt dazu, dass nicht alle Risiken erkannt werden und in der **Maßnahmenphase** keine vollständige Festlegung von Abhilfemaßnahmen zur Minimierung der Risiken möglich ist. Bei einer objektiv durchgeführten Datenschutz-Folgenabschätzung müsste die verantwortliche Stelle bei verschiedenen Diensten von Microsoft 365 zu dem **Ergebnis** kommen, dass die erstellte Datenschutz-Folgenabschätzung auf der Grundlage der getroffenen Feststellungen noch nicht der Rechenschaftspflicht nach § 5 Abs. 2 DSG-EKD genügt und der konkret geprüfte Dienst von Microsoft 365 noch nicht zum Einsatz kommen darf.

Einschätzungen aus technischer Perspektive

Auch aus technischer Perspektive bestehen beim Einsatz

von Microsoft 365 Datenschutzbedenken. Mit dem Wegfall des EU-US Privacy Shield-Abkommens und unter Anwendung der Standarddatenschutzklauseln stellt sich die Frage, ob es mit zusätzlichen **technischen und organisatorischen Maßnahmen** möglich ist, den datenschutzkonformen Einsatz der Dienste von Microsoft 365 zu erreichen. Zum Schutz der personenbezogenen Daten kommen als technische Maßnahmen insbesondere Verschlüsselung, Anonymisierung und Pseudonymisierung in Betracht.

Zunächst ist es notwendig, die Daten zu **klassifizieren** in

- Data at Rest
- Data in Transit
- Data in Use

Data at Rest (Ruhende Daten) sind solche Daten, die nicht über ein Netzwerk übertragen werden und deswegen auf dem Zielspeicher verschlüsselt gespeichert werden können. Auf diese – im Fall von Microsoft 365 – auf Cloudservern und Backupmedien abgelegten Daten kann bei Bedarf von den Anwendenden zugegriffen werden.

Data in Transit oder auch **Data in Motion** (Bewegungsdaten) sind Daten, die anwendungsbedingt über eine Netzwerkverbindung ständig hin und her bewegt werden, zum Beispiel die bei einer Videokonferenz anfallenden Daten. Data in Transit haben das **höchste Angriffspotential** (Mitschnitt). Eine Verschlüsselung der Daten selbst ist ohne gravierende Einschnitte bei der Benutzerfreundlichkeit nicht möglich, sodass lediglich eine Transportverschlüsselung in Betracht kommt.

Data in Use (Daten in Bearbeitung) sind Daten, die gerade von Programmen verarbeitet werden und sich daher z. B. im Speicher eines Rechners befinden (RAM). Die Verschlüsselung dieser Daten ist (noch) nicht möglich.

Neben der Klassifizierung der Daten ist ein **datenschutzkonformes Keymanagement** (Verwaltung der für die Verschlüsselung benötigten Schlüssel) umzusetzen. Auch wenn Microsoft die auf seinen Servern **ruhenden Daten** (Data at Rest) **verschlüsselt**, hat Microsoft mit einem eigenen Schlüssel Zugriff auf die Daten und muss diese – beispielsweise auf Weisung von US-amerikanischen Sicherheitsbehörden – herausgeben. Die Verwaltung der zur Verschlüsselung notwendigen Schlüssel ist somit zwingend für eine Datenschutzkonformität.

Im Fall von Microsoft 365 wird zwischen zwei Verfahren unterschieden, die zur Verwaltung der zur Verschlüsselung notwendigen Schlüssel verwendet werden können. Bei der **Double Key Encryption** (DKE) teilt sich die verantwortliche Stelle mit Microsoft ein Schlüsselpaar. Ein Schlüssel wird dabei von Microsoft generiert und der zweite von der kirchlichen Stelle selbst, in deren Händen der Schlüssel auch verbleibt. Sind die Daten verschlüsselt, kann Microsoft nicht ohne die Mithilfe seines Kunden die Daten entschlüsseln und umgekehrt. Selbst der **Zugriff durch US-amerikanische Sicherheitsbehörden** auf die Daten der kirchlichen oder diakonischen Stelle kann so unterbunden werden. Der Nachteil der Double Key Encryption liegt darin, dass nicht alle Daten mit ihr verschlüsselt werden können, sondern nur ein bestimmter sensibler Teil der ruhenden Daten. Der Anwendungsbereich für die DKE wird von Microsoft bewusst klein gehalten.

Für alle anderen Daten kann nur die zweite Variante **Bring Your Own Key** (BYOK) zur Anwendung kommen. Microsoft bezeichnet diese Methode auch als Unternehmensverschlüsselung. Bei der Unternehmensverschlüsselung generiert und verwaltet die verantwortliche Stelle zwar den Schlüssel zur Datenverschlüsselung, gibt diesen dann aber an Microsoft ab. Die Verschlüsselung und Entschlüsselung der Daten führt Microsoft durch. Die Verschlüsselungssoftware und den Verschlüsselungsalgorithmus verantwortet somit Microsoft und hat damit auch weiterhin Zugriff auf die Daten. Um eine datenschutzkonforme Lösung zu finden, muss somit bei der Unternehmensverschlüsselung noch eine zusätzliche Absicherung für die (ruhenden) Daten getroffen werden. Diese kann im Einsatz von **Verschlüsselungsgateways** liegen. Diese verschlüsseln alle Daten, bevor sie in der Cloud von Microsoft 365 abgelegt werden. Da der Schlüssel Microsoft nicht bekannt ist, wird somit verhindert, dass Microsoft oder ein Dritter in der Cloud auf (ruhende) Daten zugreifen kann. Jedoch verhindert der Einsatz solcher Gateways auch einige klassische Funktionen wie die Suche oder die Verschlagwortung in der Cloud. Die Vorteile einer Cloudlösung werden dadurch geschmälert.

Eine **Verschlüsselung der Bewegungsdaten** (Data in Transit / Data in Motion) ist zurzeit mit Microsoft 365 nur **eingeschränkt** möglich. Für den Transport der Daten über das Netzwerk wird eine Verschlüsselung nach dem TLS-Protokoll angeboten. Eine Videokonferenz mit Microsoft-Teams kann für zwei Teilnehmende auch Ende-zu-Ende-verschlüsselt werden. Jedoch ist es Microsoft nach heutigem Stand der Technik nicht möglich, eine Ende-zu-Ende-Verschlüsselung von mehr als zwei Teilnehmenden in ihrem Videokonferenztool bereitzustellen.

Um Microsoft 365 unter der Enterprise-Lizensierung überhaupt nutzen zu können, wird ein **Microsoft Tenant** benötigt. Ein Tenant ist eine logische Einheit – z. B. eine kirchliche Einrichtung, die Microsoft 365 nutzt –, unter der alle dazugehörigen Benutzenden und Daten zusammengefasst und verwaltet werden. Zudem werden für den Zugriff einzelne Konten für die Mitarbeitenden benötigt. Da sowohl für den Tenant als auch für die Benutzerkonten persönliche Daten wie z. B. eine E-Mail-Adresse benötigt werden, rät der BfD EKD dazu, diese **pseudonymisiert gegenüber Microsoft** anzugeben. Somit ist für die verantwortliche Stelle immer noch ein Personenbezug möglich, für Microsoft hingegen nicht.

Eine **voll umfängliche Nutzung von Microsoft 365** ist in der Cloudvariante technisch **nicht datenschutzkonform** umsetzbar. Vor dem Einsatz muss immer eine Überprüfung stattfinden, wie die benötigten Anwendungen abgesichert werden können. Der Einsatz von Verschlüsselungsgateways ist für die Absicherung des Zugriffs von Dritten erforderlich, auch wenn dadurch einige Vorteile für die Nutzung einer Cloud-Lösung verhindert werden.

Kita-Software KiDz

Ende 2021 wurde der BfD EKD in Bezug auf die Einführung des webbasierten Administrationsverfahrens für Kindertagesstätten (KiDz) um Beratung und Unterstützung gebeten.

Bei der Software KiDz handelt es sich um eine webbasierte Plattform, die ausschließlich für das Land Rheinland-Pfalz entwickelt wurde. Die Software soll zukünftig von allen **Kindertageseinrichtungen** und deren Trägern dazu genutzt werden, verschiedene Daten – darunter auch **personenbezogene Daten** der in der Einrichtung betreuten **Kinder** sowie der **Beschäftigten** – an die örtlichen Jugendämter sowie an weitere öffentliche Stellen zu **übermitteln**. Die erhobenen Daten sollen insbesondere zur Dokumentation der Personalausstattung, zur Prüfung der Landeszuwendungen, zur Erteilung der Betriebserlaubnis sowie für statistische Zwecke verwendet werden.

Im Zusammenhang mit der Prüfung der dem BfD EKD vorgelegten Unterlagen wurden **datenschutzrechtliche Bedenken** bezüglich der Verwendung der Software KiDz festgestellt. Unter anderem konnten die **Datenströme** an verschiedenen Stellen nicht nachvollzogen werden. Auch war den Unterlagen nicht immer zu entnehmen, auf welche **Rechtsgrundlagen** die Erhebung und Offenlegung der einzelnen personenbezogenen Daten der betreuten Kinder sowie der Beschäftigten gegenüber den einzelnen öffentlichen Stellen gestützt wurden. Bedenken bestanden auch bezüglich des **Rollen- und Rechtekonzeptes** in Fällen von einrichtungsübergreifenden Trägerstrukturen. So war es nicht ausgeschlossen, dass Einrichtungen auf die Daten anderer Einrichtungen des gleichen Trägers zugreifen konnten.

Zwischenzeitlich konnten die datenschutzrechtlichen Bedenken, die sich insbesondere in der Einführungsphase der Software ergaben, größtenteils gelöst und **wichtige Fortschritte** in Bezug auf einen datenschutzkonformen Einsatz der Software erzielt werden. Einige der zunächst bestehenden datenschutzrechtlichen Bedenken basierten auch auf der Tatsache, dass es sich bei der Software KiDz um ein **komplexes und fachspezifisches Verfahren** handelt, das ohne spezielle Kenntnisse in dem Bereich nicht ohne weiteres nachvollzogen werden kann. Insofern konnten einige der Bedenken auch durch Erklärung der Verfahrensweise und durch die Erläuterung der Hintergründe für die Verarbeitung der einzelnen personenbezogenen Daten behoben werden.

Fazit: Der BfD EKD unterstützt grundsätzlich den Einsatz der Software KiDz, die ein einheitliches Verfahren zur Datenübermittlung ermöglicht und damit eine Arbeitserleichterung mit sich bringen kann. In Bezug auf die ver-

bleibenden datenschutzrechtlichen Bedenken hat der BfD EKD der anfragenden Stelle verschiedene Empfehlungen zum Schutz der personenbezogenen Daten gegeben und hat darauf hingewiesen, dass die Software auch zukünftig regelmäßig auf ihre Datenschutzkonformität zu prüfen ist.

Nutzung von Kita-Apps

Im Bereich der Kindertageseinrichtungen wird zunehmend digital mit IT-Unterstützung gearbeitet. Dabei ist der IT-Einsatz mittlerweile nicht mehr auf reine Verwaltungsarbeiten beschränkt. Zentrale Verfahren – z. B. zur Abrechnung von Kitagebühren und Personalstellen – sind langjährig im Einsatz und fest etabliert. Die Schnittstellen und Zuständigkeiten sind bei diesen Verfahren klar definiert.

Durch die technische Weiterentwicklung ergeben sich in mehrfacher Hinsicht nun auch für Kindertageseinrichtungen neue Möglichkeiten und Herausforderungen. Zum einen gibt es eine **zunehmende Verbreitung von Smartphones** und **Tablets**, die auch in der täglichen Arbeit mit den Kindern und Eltern eine Rolle spielen. Das hat beispielsweise einen erheblichen Einfluss auf die Kommunikation miteinander. Zum anderen gibt es immer mehr **sogenannte Kita-Apps,** die neben der Verwaltungsarbeit auch die pädagogische Arbeit der Erzieherinnen und Erzieher digital unterstützen sollen. Viele dieser Angebote beruhen auf den neuesten Webtechnologien, deren IT-Sicherheit und Datenschutzkonformität noch nicht hinreichend abgeklärt sind. Einschlägige Zertifizierungen haben sich noch nicht etabliert. Einige am Markt angebotene Anwendungen richten sich nicht nur an die Kindertageseinrichtungen, sondern auch an die Träger.

Den BfD EKD erreichte im Berichtszeitraum die Beschwerde eines Elternteils, weil ohne das Einverständnis der Eltern personenbezogene Daten in einer **Kita-App** gespeichert wurden. Um den Sachverhalt aufzuklären, wurde die Kindertageseinrichtung um Auskunft gebeten. Dabei stellte sich heraus, dass die von der Kindertageseinrichtung genutzte Kita-App eine Vielzahl von Funktionen anbietet. Dazu gehören unter anderem die Kommunikation mit den Eltern, die Erstellung von Dienstplänen, Portfolioarbeit, das Anlegen von Akten, Kitaplatzvergabe und die Zeiterfassung für Mitarbeitende. Nach erster Prüfung stand fest, dass hier von einer umfangreichen Verarbeitung von personenbezogenen Daten – darunter auch besonderen Kategorien personenbezogener Daten – auszugehen war.

Nach Prüfung der eingereichten Unterlagen wurden **folgende Punkte bemängelt:**

- Es wurde keine Zusatzerklärung nach § 30 Abs. 5 DSG-EKD unterzeichnet.
- Trotz der Verarbeitung besonderer Kategorien personenbezogener Daten fehlte das Verfahrensverzeichnis.
- Es fehlte eine differenzierte Verfahrensbeschreibung mit einer Risikoabschätzung nach § 34 DSG-EKD und einer gegebenenfalls erforderlichen Datenschutz-Folgenabschätzung (DSFA).
- Ein Löschkonzept war nicht vorhanden.
- Der Grundsatz der Datenminimierung wurde nicht beachtet.

Im Verlauf der weiteren Prüfung stellte sich heraus, dass die vielfältigen Funktionen der Kita-App erst nach und nach genutzt werden sollten. Dazu gehörte die Zeiterfassung von Mitarbeitenden sowie die Erstellung von Dienstplänen. Vereinbarungen mit der Mitarbeitervertretung lagen zum Prüfungszeitpunkt noch nicht vor.

In Zusammenarbeit mit der verantwortlichen Stelle und der örtlich Beauftragten für den Datenschutz wurden einzelne Schritte zur Abarbeitung der festgestellten Mängel erarbeitet. Die verantwortliche Stelle hat eine **Datenschutz-Folgenabschätzung** durchgeführt. Nach Prüfung der getroffenen Maßnahmen konnte ein datenschutzkonformer Betrieb der Kita-App hergestellt werden. Besonders zu erwähnende **Maßnahmen** sind die Einführung regelmäßiger **externer Sicherheitsüberprüfungen** (Penetrationstests) und eine **Zwei-Faktor-Authentifizierung** in Bereichen, in denen besonders sensible Daten verarbeitet werden.

Die am Markt befindlichen Programme werden zwar oftmals als „datenschutzkonform“ beworben. Im Regelfall lässt sich aber nur bei dem geplanten konkreten Einsatz feststellen, ob und in welchem Umfang ein datenschutzkonformer Betrieb möglich ist. Mit dem Träger konnte im Rahmen einer Beratung der Einsatz der Kita-App bespro-

chen und der Umfang und die konkrete Ausgestaltung an die datenschutzrechtlichen Vorschriften angepasst werden.

„Kirchen-App“ Churchpool

Der BfD EKD wurde im Berichtszeitraum gebeten zu prüfen, ob die App Churchpool datenschutzkonform eingesetzt werden kann.

Viele kirchliche Einrichtungen nutzen vermehrt Informations- und Kommunikationskanäle, die allgemein unter dem Begriff **soziale Medien** zusammengefasst werden. Um mit bestimmten Gruppen im kirchlichen Bereich besser kommunizieren zu können, bieten einige Landeskirchen eigene datenschutzkonforme Lösungen an. Es gibt aber auch am Markt einige Anbieter sozialer Medien (wie z. B. Churchpool), die sich ganz allgemein an kirchliche und diakonische Einrichtungen richten.

Im Rahmen der konkreten Beratungsanfrage wurden die **Nutzungsbedingungen** der App Churchpool datenschutzrechtlich geprüft. Dabei wurden Datenschutzmängel festgestellt. So durften laut der geltenden Nutzungsbedingungen eingestellte Inhalte vom Anbieter verändert oder gelöscht werden. Dies widerspricht der im Datenschutz und in der IT-Sicherheit geforderten Integrität von Daten. Auch bestand durch das Einbetten von Karten durch Drittanbieter das Risiko eines unerlaubten Datenabflusses für die Nutzenden. In den Nutzungsbedingungen wurde des Weiteren nicht erwähnt, in welchem Land die Datenverarbeitung stattfindet.

Darüber hinaus fallen beim Einsatz der App Churchpool personenbezogene Daten an, die vom App-Anbieter im Auftrag verarbeitet werden. Somit müssen die kirchlichen Stellen als Auftraggeber den Schutz der personenbezogenen Daten über einen **AV-Vertrag** sicherstellen. Im Rahmen des AV-Vertrags sind unter anderem die konkreten technischen und organisatorischen Schutzmaßnahmen zu beschreiben. Dem BfD EKD konnte jedoch kein AV-Vertrag zur Prüfung vorgelegt werden. Aus diesen technischen und rechtlichen Gründen wurde im konkreten Fall von der Nutzung von Churchpool abgeraten.

Fazit: Vor dem Einsatz von sozialen Medien ist stets zu prüfen, ob die Nutzung datenschutzkonform möglich ist. Das Prüfen der Nutzungsbedingungen ist zwar häufig aufwändig, aber dennoch unverzichtbar. Die Prüfung der eingebetteten Inhalte kann wichtige Hinweise auf einen möglichen unberechtigten Datenabfluss geben.

Rückblick: Kontaktnachverfolgung mit der Luca-App

Während der Corona-Pandemie mussten auch kirchliche und diakonische Einrichtungen die in den von den Bundesländern erlassenen Corona-Regelungen zeitweise vorgeschriebene **Erhebung von Kontaktdaten bei Veranstaltungen** beachten. In diesem Zusammenhang erreichten den BfD EKD diverse Beratungsanfragen zur Luca-App.

Abgesehen von sehr komplexen Fragen zu den Datenströmen und zum einschlägigen Datenschutzrecht beim Einsatz der App bei kirchlichen und diakonischen Veranstaltungen gilt es aufgrund der großen Aufmerksamkeit der Luca-App in der Öffentlichkeit kurz folgende allgemeine Einschätzung fest zu halten: Die Luca-App wurde entwickelt, um eine **digitale Kontaktdatenverfolgung** von Veranstaltungsteilnehmenden und eine entsprechende Datenübermittlung an die Gesundheitsämter zu ermöglichen. Bei IT-Sicherheitsprüfungen wurden jedoch mehrere **Schwachstellen** in der App identifiziert. Es wurden **Bewegungsprofile** der Anwendenden mit personenbezogenen Daten und Standorten erstellt, die auf dem zentralen Server auslesbar sein konnten. Auch stellte die **zentrale Speicherung** der Kontaktdaten auf den Luca-Servern und die Absicherung mit nur **einem Generalschlüssel** auf Seiten der Gesundheitsämter ein **Sicherheitsrisiko** dar. Die korrekte Nutzung dieser App beruhte auf freiwilligen und ehrlichen Angaben durch die Nutzenden. Eine ausreichende Überprüfung der Authentizität der eingegebenen Daten bot die App nicht. Im Laufe der Zeit stellte sich außerdem heraus, dass die Gesundheitsämter nur in wenigen Einzelfällen diese Möglichkeit der Kontaktnachverfolgung nutzten.

Ende März 2022 **endeten** die zwischen dem Betreiber der Luca-App und den jeweiligen Bundesländern geschlossenen **Verträge**. Im April 2022 gaben die Betreiber bekannt, dass die Luca-App nicht mehr zur Nachverfolgung von Kontakten eingesetzt wird.

Aufbewahrung und Löschung

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

Elektronische Sicherung von Daten

Im Zuge der Schwerpunktprüfung von Kindertageseinrichtungen erkundigte sich der BfD EKD nach dem Vorhandensein eines Datensicherungskonzepts. Dabei ergab sich, dass bereits mehr als die Hälfte der Kindertageseinrichtungen ein Datensicherungskonzept hat. Die meisten Einrichtungen ohne ein Datensicherungskonzept sichern ihre Daten dennoch in regelmäßigen oder unregelmäßigen Zeitabständen.

Das Thema **Datensicherung** und die Beschreibung der jeweiligen Handhabung in einem Datensicherungskonzept ist in den einzelnen Einrichtungen für die Umsetzung des Datenschutzes und für das Erreichen eines guten Datenschutzniveaus eine wichtige Voraussetzung. Mit der **Dokumentation in einem Datensicherungskonzept** wächst auch das Bewusstsein über die Notwendigkeit von Datensicherungen. Ursache nicht erstellter Konzepte ist in den meisten Fällen das fehlende Knowhow, wie eine solche Dokumentation gestaltet werden kann. Auch ist den kirchlichen Einrichtungen in vielen Fällen nicht bekannt, aus welchen Gründen eine regelmäßige und möglichst tägliche Datensicherung wichtig ist. Im Folgenden soll daher dargestellt werden, weshalb die Datensicherung ein wichtiger Aspekt zum Schutz von personenbezogenen Daten ist.

Alle kirchlichen und diakonischen Einrichtungen – nicht nur Kindertageseinrichtungen – speichern personenbezogene Daten und sind auf den elektronischen Zugriff auf diese Daten angewiesen. **Was aber, wenn Daten verloren gehen**, beispielsweise durch defekte Hardware oder durch versehentliches Löschen? Auch Malware (z. B. Verschlüsselungstrojaner), der Diebstahl von Endgeräten oder von Speichermedien sowie andere Ursachen können zum **Datenverlust** führen. Gehen Daten verloren und besteht keine Möglichkeit der Wiederherstellung, können gravierende Schäden entstehen. Ein Datenverlust kann über klassische IT-Systeme hinaus, wie Server oder Clients, auch Router, Switches, Telekommunikationsanlagen oder jedwedes mit dem Internet verbundenes Gerät betreffen. So müssen auch die Konfigurationen von IT-Systemen, die für den laufenden Betrieb erforderlich sind, auf geeignete Weise gesichert werden.

Durch **regelmäßige Datensicherungen** lassen sich Auswirkungen von Datenverlusten minimieren. Eine Datensicherung mit erprobter Rücksicherung gewährleistet, dass sowohl die datenschutzrechtliche Anforderung der Verfügbarkeit als auch das IT-technische Erfordernis, den Betrieb nach Datenverlusten kurzfristig wieder aufnehmen zu können, erfüllt werden. Für den **Inhalt eines Datensicherungskonzeptes** kann das **Grundschutzkompendium des BSI**, das sich in einem eigenen Baustein (CON.3) dem Datensicherungskonzept widmet, herangezogen werden (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2022.pdf?__blob=publicationFile&v=3). Dieser Baustein zeigt typische Bedrohungen und Schwachstellen, wie fehlende Wiederherstellungstests, ungeeignete Aufbewahrung der Speichermedien oder Ransomware-Befall auf und nennt die Anforderungen an ein Datensicherungskonzept.

Für die **Basisanforderungen nach dem Grundschutzkompendium des BSI** müssen – neben der Benennung der Zuständigkeit für die Datensicherung (Fachverantwortliche) und der Auswahl geeigneter Speichermedien – folgende Rahmenbedingungen berücksichtigt werden:

- Speichervolumen
- Änderungsvolumen
- Änderungszeitpunkt
- Verfügbarkeitsanforderungen
- Integritätsbedarfs
- rechtliche Anforderungen

Zu einem vollständigen Datensicherungskonzept gehört nicht nur die **Beschreibung der Datensicherung** (**Backup**), sondern auch die **Beschreibung der Wiederherstellung** (**Restore**).

Nach den Maßgaben des Grundschutzkompendiums des

BSI ist für jedes IT-System und jede Gruppe von IT-Systemen ein **Datensicherungsplan** festzulegen und einzuhalten. Dabei sind folgende Fragen zu beantworten:

- Welche IT-Systeme und welche darauf befindlichen Daten werden durch welche Datensicherung gesichert?
- In welcher Reihenfolge werden IT-Systeme und Anwendungen wiederhergestellt?
- Wie können die Datensicherungen erstellt und wiederhergestellt werden?
- Wie lange werden Datensicherungen aufbewahrt?
- Wie werden die Datensicherungen vor unbefugtem Zugriff und Überschreiben gesichert?
- Welche Hard- und Software werden für Backup und Restore eingesetzt?

Bei der Datensicherung ist zu berücksichtigen, dass Daten unterschiedliche **Löschfristen** haben. Hier empfiehlt es sich, diese Daten entsprechend gruppiert und gegebenenfalls getrennt voneinander auf unterschiedlichen Datenträgern zu sichern und an geeigneter Stelle die frühesten und die spätesten Löschfristen zu vermerken.

Zu berücksichtigen sind alle Aspekte des Datenschutzes. Je genauer diese bereits bei der Planung der Datensicherung berücksichtigt werden, umso leichter sind dessen Belange nachher umzusetzen. Macht eine betroffene Person zum Beispiel von ihrem **Recht auf Löschen** ihrer personenbezogenen Daten nach § 21 DSG-EKD Gebrauch, so muss beachtet werden, dass die Daten auch von den Datensicherungsmedien zu löschen sind.

Die gesicherten Daten müssen vor dem **unbefugten Zugriff** durch geeignete **technische** und **organisatorische Maßnahmen** geschützt werden. Zu den Maßnahmen gehören beispielsweise der Kennwortschutz, die Verschlüsselung, die Aufbewahrung in einem feuersicheren Safe oder in einem anderen Brandabschnitt sowie die Wiederherstellung mit dem vier-Augen-Prinzip.

Löschen von Gesundheitsdaten nach der Pandemie

Im Zusammenhang mit der Corona-Pandemie wurden in den kirchlichen und diakonischen Einrichtungen eine Vielzahl von **Gesundheitsdaten von Beschäftigten** verarbeitet. Diesbezüglich war es im Berichtszeitraum wichtig, regelmäßig darauf hinzuweisen, dass diese erhobenen Gesundheitsdaten einerseits nur streng zweckgebunden verarbeitet werden durften und andererseits umgehend datenschutzkonform zu **vernichten** waren, sobald die **Rechtsgrundlagen entfielen**.

Die Verpflichtung zur Erbringung eines **3G-Nachweises am Arbeitsplatz** (§ 28b Abs. 1 IfSG alt) galt vom 24. November 2021 bis zum 24. März 2022 für alle Arbeitsstätten bundesweit. Zur Erfüllung der Verpflichtung wurde die Vorlage der jeweiligen Nachweise auf namentlichen Listen dokumentiert. Mit Entfall der Regelung bestand keine weitere Erforderlichkeit diese umfangreichen Daten weiter vorzuhalten, sodass Daten, die im Zusammenhang mit § 28b Abs. 1 IfSG erhoben wurden, zu vernichten waren.

Auf Basis des § 36 IfSG konnten bestimmte Einrichtungen personenbezogene Daten eines **Beschäftigten über dessen Impf- und Serostatus** in Bezug auf die Covid-19 Infektion verarbeiten, um über die Begründung eines Beschäftigungsverhältnisses oder über die Art und Weise einer Beschäftigung zu entscheiden. Anders als bei der einrichtungsbezogenen Impfpflicht wurde hiermit der Zugang zu Gesundheitsberufen nicht gänzlich vom Impf- und Serostatus der Beschäftigten abhängig gemacht. Vielmehr sollte den Einrichtungen auf Basis dieser Information, die Möglichkeit eröffnet werden, über den Einsatzbereich der Beschäftigten zu entscheiden und entsprechende Hygienekonzepte zu entwickeln. Auch hier sollten Dokumentationen erstellt werden. Fotokopien von Dokumenten waren auch hier nicht erforderlich und durften nicht angefertigt werden. Die Regelung trat zum 30. Juni 2022 außer Kraft. Damit entfiel auch die Rechtsgrundlage für eine Verarbeitung der damit zusammenhängenden Daten.

Die letzte geltende Regelung war die **einrichtungsbezogene Impfpflicht**, deren Geltung am 31. Dezember 2022 endete. Ähnlich wie bei § 36 IfSG durfte hier dokumentiert werden, wer seinen Immunitätsnachweis bis zum 15. März 2022 vorgelegt hatte und wie lange dieser gültig war. Ab dem 1. Oktober 2022 „verfielen“ die Immunitätsnachweise, sofern keine weitere Impfung oder eine Genesung nachgewiesen wurde, sodass zu diesem Zeitpunkt erneut der Immunitätsnachweis gegenüber den Gesundheitseinrichtungen hätte erbracht werden müssen. Hier wurde von den Bundesländern jedoch teilweise

signalisiert, dass eine erneute Vorlage für bereits Beschäftigte nicht nötig sei, um den bürokratischen Aufwand für Gesundheitseinrichtungen zu minimieren. Insofern waren die Gesundheitseinrichtungen in den betroffenen Bundesländern von der Offenlegungsverpflichtung der Mitarbeitenden ohne Immunitätsnachweis nach § 20a IfSG befreit. Mit dem gänzlichen Auslaufen der Regelung am 31. Dezember 2022 entfiel dann die Rechtsgrundlage für die Verarbeitung der Nachweise auf Basis des § 20a IfSG. Der Zugang zu Gesundheitsberufen war ab diesem Zeitpunkt wieder möglich, ohne den Immunitätsnachweis erbringen zu müssen.

Fazit: Zum Schutz der Persönlichkeitsrechte mussten die Gesundheitsdaten der Beschäftigten bei Wegfall der Rechtsgrundlage gelöscht werden.

Folgen einer unerlaubten Veröffentlichung im Internet

Die Veröffentlichung von personenbezogenen Daten im Internet ist aufgrund der Tatsache, dass mit der Veröffentlichung ein unbestimmter Personenkreis ohne jegliche Kontrolle auf die Daten zugreifen kann, stets mit Risiken für den Schutz von personenbezogenen Daten verbunden. Erfolgt eine Veröffentlichung ohne Rechtsgrundlage und insbesondere ohne Einwilligung der betroffenen Person, ist die verantwortliche Stelle verpflichtet, die unerlaubt verarbeiteten personenbezogenen Daten zu löschen. Dies ist auch der Hintergrund des vorliegenden Falles, in dem eine kirchliche Einrichtung **unerlaubt** personenbezogene Daten in sozialen Netzwerken veröffentlichte. Nachdem die kirchliche Stelle die Daten in dem sozialen Netzwerk gelöscht hatte, stellte sie fest, dass die gelöschten Daten weiterhin im **Internet** auf der Domain globalnpo.org **verfügbar** waren. Über diese internationale Website wurde über lokale gemeinnützige Vereine und ehrenamtliche Initiativen informiert und dazu ungefragt und automatisch Inhalte von anderen Internetseiten übernommen.

Gemäß § 21 Abs. 2 DSG-EKD müssen verantwortliche Stellen, die personenbezogene Daten öffentlich gemacht haben und zur Löschung verpflichtet sind, andere verantwortliche Stelle, die auf Grund der Veröffentlichung diese Daten verarbeiten, über die Pflicht zur Löschung informieren. In dem vorliegenden Fall versuchte die kirchliche Stelle mehrfach mit den Betreibern der Website Kontakt aufzunehmen. Alle Kontaktversuche **scheiterten** jedoch. Ein Impressum war auf der Website, die nicht dem deutschen Recht unterlag, ebenfalls nicht vorhanden. Die verantwortlichen Personen für die Website konnten nicht ermittelt werden. Inzwischen ist die Website nicht mehr erreichbar.

Dieser Vorfall ist ein Beispiel für das stets bestehende **Risiko**, dass einmal veröffentlichte Informationen im Internet gar nicht oder nur mit erheblichem Aufwand wieder vollständig gelöscht werden können. Es ist schwierig bis unmöglich, solche Sachverhalte im internationalen Kontext zu klären. Die verantwortlichen Stellen werden immer wieder sensibilisiert, bei der Bereitstellung von Informationen im Internet **besonders sorgfältig** vorzugehen und darauf zu achten, dass keine personenbezogenen Daten ohne Einwilligung veröffentlicht werden.

Fazit: Bei der Einholung einer Einwilligung ist stets auf das bestehende Risiko der möglicherweise andauernden Verfügbarkeit der Informationen im Internet hinzuweisen.

Ausblick

Beim Blick nach vorne ...

... wirft die voranschreitende Digitalisierung auch einige Fragen zum Datenschutz auf. Wie so häufig beim Thema Datenschutz wird das Thema von seinen Kritikern „dagegen“ positioniert. Bremst der Datenschutz nicht wieder mal – nun auch bei der dringend notwendigen Digitalisierung – den technischen Fortschritt aus?

Diese Polarisierung ist bekannt: Im staatlichen Bereich erschwert und bremst der Datenschutz die innere Sicherheit. Im kirchlichen Bereich erschwert und bremst der Datenschutz die kirchliche Arbeit gerade auch im Bereich von Social Media. Und nun auch bei der Digitalisierung. Diese Argumentation verkennt eine grundlegende Einordnung des Datenschutzes!

Seit dem sog. Volkszählungsurteil des Bundesverfassungsgerichts im Jahr 1983 fußt der Datenschutz auf dem Grundrecht der informationellen Selbstbestimmung! Kaum eine seriöse Meinung würde bei uns andere Grundrechte – wie die Meinungsfreiheit oder die Pressefreiheit – eingrenzen wollen. Beim Recht auf informationelle Selbstbestimmung und beim Datenschutz ist das manchmal anders. Das liegt sicherlich daran, dass das Recht auf informationelle Selbstbestimmung – gerade bei Datenverarbeitungen im virtuellen Raum – weniger praktisch und greifbar ist. Zu viel passiert dann im digitalen Hintergrund. Im Wechselspiel von Grund- und Freiheitsrechten kann der – die innere Sicherheit betonende und den Datenschutz relativierende – Slogan aus dem weltlichen Bereich „Keine Freiheit ohne Sicherheit!“ aber genauso gut umgekehrt gelesen werden: Keine Sicherheit ohne Freiheit! Und so bleibt es dabei: Das Grundrecht auf informationelle Selbstbestimmung „spielt in der selben Grundrechte-Liga“ wie alle anderen Grundrechte auch und muss stets in einen Ausgleich mit anderen widersteitenden (Grund-) Rechten gebracht werden!

Auch im kirchlichen und diakonischen Bereich realisieren wir bereits heute, dass die mit der Digitalisierung weiter voranschreitenden Zukunftstechnologien zukünftig ganz überwiegend auf dem Einsatz von künstlicher Intelligenz beruhen werden. Dies hat – wie so häufig bei neuen Technologien – Chancen, aber auch Risiken und Herausforderungen. Bei all diesen Entwicklungen wird der kirchliche Datenschutz in Erfüllung unseres gemeinsamen kirchlichen und diakonischen Auftrags auch zukünftig an der Seite der Menschen bleiben! Datenschutz ist und bleibt nämlich in erster Linie Menschenschutz!

https://datenschutz.ekd.de