3. Tätigkeitsbericht
Berichtszeitraum 2019 und 2020

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

3. Tätigkeitsbericht

des Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland

für die Jahre 2019 und 2020

vorgelegt im Juni 2021

Redaktionsschluss 31. Mai 2021

Inhaltsverzeichnis

Vorwort

Datenschutz in Zeiten der Corona-Pandemie - Motor oder Bremse?

Auch beim Beauftragten für den Datenschutz der EKD (BfD EKD) stand das Jahr 2020 sowohl inhaltlich als auch organisatorisch voll und ganz im Zeichen der Corona-Pandemie. Doch auch rechtliche Fragen zum EKD-Datenschutzgesetz, datenschutztechnische Fragen zu neuen Technologien oder die Auswirkungen von Grundsatzentscheidungen der Gerichte im Bereich Datenschutz haben den BfD EKD im Berichtszeitraum beschäftigt. Im Folgenden finden Sie einige Anmerkungen und Informationen zu diesen Fragen:

- Wieviel Datenschutz brauchen wir in Zeiten der Corona-Pandemie?
- Wie hat der BfD EKD im Berichtszeitraum seine Arbeit strukturiert?
- Mit welchen (Zukunfts-)Themen beschäftigt sich der BfD EKD?

Die öffentlichen Debatten und Diskussionen der letzten Monate während der Corona-Pandemie sind uns als Datenschützer nur allzu vertraut. Grundrechte wurden eingeschränkt. Bei der dabei erforderlichen Abwägung landen wir schnell im Spannungsfeld von Freiheit und Sicherheit. Für Datenschützer bedeutet das: Die Freiheit auch in Pandemiezeiten selber über den Umgang mit meinen Daten zu entscheiden und die Sicherheit vor Ansteckung und Infizierung mit dem Coronavirus SARS-CoV-2. Die Datenschutzgrundlage im Grundgesetz – das Grundrecht auf informationelle Selbstbestimmung – blieb von Einschränkungen bisher weitgehend unangetastet. Die Einhaltung des Datenschutzes war für alle Beteiligten – zum Beispiel bei der Entwicklung der sog. Corona-Warn-App – leitend. Diese Entscheidung wirkte bei der Bewältigung der Corona-Pandemie für breite Teile der Bevölkerung vertrauensbildend. Hingegen rufen Einige beim Datenschutzblick auf andere Länder immer lauter, dass der Datenschutz zur Bewältigung der Corona-Pandemie nun endlich auch bei uns „zurück geschraubt“ werden müsse. Diesem Begehren ist deutlich zu widersprechen, vor allem weil entsprechende Erfahrungen in anderen demokratischen Ländern nicht auf eine deutlich bessere Pandemiebekämpfung hindeuten. Alles in allem hat sich die in den Mitgliedsstaaten der Europäischen Union seit Mai 2018 geltende Datenschutz-Grundverordnung und somit ein einheitliches europäisches Datenschutzrecht auch in Zeiten der Corona-Pandemie sehr bewährt.

Als evangelische Kirche sind wir in Kirche und Diakonie mit dem im Mai 2018 in Kraft getretenen EKD-Datenschutzgesetz unter Berücksichtigung unserer Besonderheiten beim Thema Datenschutz eigenständig, aber verlässlich und vergleichbar aufgestellt. So konnten wir im Berichtszeitraum unsere Arbeit als Datenschutzaufsichtsbehörde in den Bereichen Aufsicht, Beratung und Weiterbildung weiter etablieren und adressatenorientiert verbessern und somit der Durchsetzung des „Datenschutzgrundrechts“ auch in Kirche und Diakonie noch mehr Geltung verschaffen. Dabei ist die Beratung von kirchlichen und diakonischen Stellen auch in Zeiten der Pandemie – etwa beim Thema Homeoffice oder bei der Verarbeitung von Gesundheitsdaten – ein entscheidender Bestandteil unserer Arbeit, um situations- und adressatenbezogen ganz konkrete Antworten und Hilfestellungen zu geben. Am Ende des Berichtszeitraums traten unsere Planungen für ein proaktives aufsichtliches Handeln mit den ersten Schwerpunktprüfungen im Bereich Kindertageseinrichtungen in die Umsetzungsphase und auch das Thema Weiterbildungen wird mit neuem Schwung online fortgesetzt. Pandemiebedingt erfüllt der BfD EKD seine Aufgaben stärker als bisher digital und sieht sich dabei ständig auch seinem „eigenen“ Thema kritisch ausgesetzt. Diese Herausforderungen bieten auch für uns neue Chancen und Möglichkeiten.

Durch das sog. Schrems II-Urteil des Europäischen Gerichtshofs (EuGH) aus Juli 2020 wurde mit der Abkehr vom EU-US Privacy Shield das Thema der rechtmäßigen Datenübermittlung in den Drittstaat USA auf die europäische Tagesordnung gehoben. Die Vorgaben im Urteil des EuGH sind eindeutig, aber rechtskonforme und

technisch-umsetzbare Lösungen für den Datentransfer in die USA sind bisher noch nicht abschließend erarbeitet und umgesetzt. Gerade beim Einsatz von Videokonferenzsystemen und anderen Softwaretools – etwa im Bereich Social Media und neuer digitaler Kommunikationsformen – merken wir die sich daraus ergebenden praktischen Probleme, vor allem beim Datentransfer in die USA, sehr deutlich. Bei alledem sollten wir die vielen – unabhängig von der Corona-Pandemie bestehenden – rechtlichen und technischen Datenschutzherausforderungen unserer Zeit nicht aus dem Blick verlieren! Auch die Entwicklung von künstlicher Intelligenz schreitet im beruflichen und privaten Alltag unaufhaltsam voran und wirft weiterhin viele rechtliche und ethische Fragen im Datenschutz auf. Und auf das unter dem Begriff Big Data zusammengefasste Sammeln, Speichern und Verknüpfen von Daten gibt es im europäischen Datenschutzrecht weiterhin nur wenige zukunftsweisende Antworten.

Dieser Tätigkeitsbericht versteht sich in der Tradition und Weiterentwicklung der bisher vom BfD EKD vorgelegten Tätigkeitsberichte für die Berichtszeiträume 2015/2016 und 2017/2018. Dabei wurde erstmals das Kapitel I „Über die Entwicklungen im Datenschutz“ ergänzt um wichtige Datenschutzgrundsatzentscheidungen der Gerichte auf nationaler und europäischer Ebene und somit im Ganzen rechtlicher. Das Kapitel II „Über den Beauftragten für den Datenschutz der EKD“ wurde weiter gekürzt und konzentriert. Das Kapitel III „Über die Themen bei Aufsicht und Beratung“ wurde mit vielen unterschiedlichen konkreten Beispielen und Themen aus dem rechtlichen und technischen Datenschutz angereichert und somit deutlich praxisbezogener, umfangreicher und technischer als in den bisherigen Tätigkeitsberichten.

Auch in Zeiten der Corona-Pandemie brauchen wir in Staat und Kirche einen grundrechtebasierten Datenschutz! Das „Datenschutzgrundrecht“ hat sich stets als ein verlässlicher Partner an der Seite der Menschen erwiesen. Die gesetzliche Aufforderung im EKD-Datenschutzgesetz, jede einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird, ist somit aktueller denn je!

Allen Mitarbeiterinnen und Mitarbeitern, 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 2021

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

Über die Entwicklungen im Datenschutz

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

In der evangelischen Kirche

Das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) trat in seiner novellierten Fassung am 24. Mai 2018 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.

Art. 91

Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

(1) Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.

(2) Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.

Nachdem auf dieser gesetzlichen Grundlage die EKD mit dem novellierten EKD-Datenschutzgesetz ihre Datenschutzregelungen mit der DSGVO rechtzeitig in Einklang gebracht hatte, steht nun eine Evaluation des EKD-Datenschutzgesetzes bevor. Gemäß § 54 Abs. 4 DSG-EKD soll das EKD-Datenschutzgesetz innerhalb von fünf Jahren, also bis Ende Mai 2023, überprüft werden. Die Evaluation des EKD-Datenschutzgesetzes wird federführend durch das Kirchenamt der EKD betreut. Damit bis Mai 2023 Ergebnisse einer Überprüfung vorliegen, soll sich nach Planungen des zuständigen Referates in der Rechtsabteilung des Kirchenamtes der EKD im 1. Quartal 2022 eine Arbeitsgruppe konstituieren, die dann spätestens Anfang des 2. Quartals 2022 die Arbeit aufnimmt. In den letzten Jahren seit Inkrafttreten des neuen EKD-Datenschutzgesetzes hat das zuständige Referat bereits Hinweise – sowohl redaktioneller als auch inhaltlicher Art – aufgenommen. Weitere Anregungen und Änderungsbedarfe werden zu Beginn des Überprüfungsprozesses bei den Gliedkirchen, den diakonischen Werken und den Beauftragten für den Datenschutz in der EKD erfragt. Die Ergebnisse der Überprüfung sollen im Herbst 2023 der Synode der EKD vorgelegt werden. Zur Vorbereitung der Evaluation erarbeitet der BfD EKD bereits zum jetzigen Zeitpunkt eine umfängliche Liste mit Änderungs- und Formulierungsvorschlägen.

Zwischenzeitlich haben darüber hinaus nahezu alle Gliedkirchen von ihrem Recht aus § 54 Abs. 2 DSG-EKD Gebrauch gemacht und für ihren Bereich Durchführungsbestimmungen zum EKD-Datenschutzgesetz bzw. ergänzende Bestimmungen zum Datenschutz erlassen. Mit dieser Rechtsgrundlage im EKD-Datenschutzgesetz wird den Gliedkirchen ermöglicht, spezielle und an ihre Bedürfnisse angepasste Datenschutzregelungen zu treffen, soweit sie dem Recht der EKD nicht widersprechen.

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 neben dem Beauftragten für den Datenschutz der EKD und der von ihm geleiteten Aufsichtsbehörde drei weitere Aufsichtsbehörden. 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. Weitere Informationen über den BfD EKD können der Website https://datenschutz.ekd.de/ entnommen werden.

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 personenbe-

zogenen Daten, um so das aus dem Grundgesetz abgeleitete Grundrecht auf informationelle Selbstbestimmung für jeden einzelnen Menschen 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 katholische Kirche unter die Vorgaben in Art. 91 Abs. 1 DSGVO und kann somit (weiterhin) eigenes Datenschutzrecht anwenden. Am 24. Mai 2018 wurde das Gesetz über den Kirchlichen Datenschutz (KDG) durch die Diözesanbischöfe in ihren Diözesen in Kraft gesetzt. Gemäß § 58 Abs. 2 KDG soll das KDG innerhalb von drei Jahren ab Inkrafttreten am 24. Mai 2018 überprüft werden. Vorschläge für Gesetzesänderungen werden zurzeit in einer Arbeitsgruppe erarbeitet, die sich bereits konstituiert hat.

Neben dem KDG finden in der römisch-katholischen Kirche weitere datenschutzrechtliche Bestimmungen Anwendung. So ist gleichzeitig mit dem KDG die Kirchliche Datenschutzgerichtsordnung (KDSGO) in Kraft getreten, die unter anderem die Errichtung, Zusammensetzung und die Zuständigkeiten der kirchlichen Gerichte in Datenschutzangelegenheiten regelt. Weitere wichtige Rechtsquellen sind die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) sowie das Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG), die ergänzende Bestimmungen zum KDG und zu den Tätigkeiten der kirchlichen Datenschutzaufsichten enthalten.

Im Blick auf Art. 91 Abs. 2 DSGVO sind in der 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 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 das Datenschutzrecht im Berichtszeitraum ebenfalls durch eine Überprüfung und Anpassung der staatlichen datenschutzrechtlichen Bestimmungen sowie durch neue Rechtsprechung weiterentwickelt.

Datenschutzrecht des Bundes und der Länder

Am 20. November 2019 hat der Deutsche Bundestag mit Zustimmung des Bundesrates das Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) beschlossen. Im Rahmen des 2. DSAnpUG-EU wurden auch mehrere Änderungen im Bundesdatenschutzgesetz (BDSG) vorgenommen. Die wichtigsten Änderungen werden im Folgenden kurz erläutert.

- Eine auch in der Öffentlichkeit wahrgenommene Änderung betrifft die Regelung in § 38 Abs. 1 BDSG, die sich mit der Benennung von Datenschutzbeauftragten von nichtöffentlichen Stellen befasst. Nach der Gesetzesänderung sind der Verantwortliche und der Auftragsverarbeiter zur Benennung einer Datenschutzbeauftragten oder eines Datenschutzbeauftragten verpflichtet, soweit sie mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Damit wurde die Schwelle von 10 auf 20 Mitarbeitende hochgesetzt. Die Gesetzesänderung soll zur Entlastung von kleinen und mittleren Unternehmen (KMU) beitragen.
- Eine weitere wichtige Änderung betrifft § 26 BDSG. § 26 BDSG regelt die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses. In Absatz 2 geht es um die Voraussetzungen für eine wirksame Einwilligung von Mitarbeitenden. Während § 26 Abs. 2 Satz 3 BDSG bisher ein Schriftformerfordernis für die

Einwilligung von Mitarbeitenden im Rahmen des Beschäftigungsverhältnisses vorsah, reicht nun auch die elektronische Form für die Erteilung einer Einwilligung aus.

- In § 22 BDSG sind Tatbestände geregelt, nach denen abweichend von Art. 9 Abs. 1 DSGVO die Zulässigkeit der Verarbeitung besonderer Kategorien von personenbezogenen Daten erlaubt wird. Im Rahmen des 2. DSAnpUG-EU wurde nun eine Rechtsgrundlage, die bisher nach § 22 Abs. 1 Nr. 2 lit. a) BDSG nur für öffentliche Stellen galt, auch für nichtöffentliche Stellen aufgenommen. Nach § 22 Abs. 1 Nr. 1 lit. d) BDSG dürfen nun besondere Kategorien von personenbezogenen Daten von öffentlichen und nichtöffentlichen Stellen verarbeitet werden, wenn dies aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist.

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. In dieser Funktion überwacht er im föderalen System Deutschlands gemäß § 9 BDSG die Einhaltung des Datenschutzrechts in öffentlichen Stellen des Bundes sowie in Unternehmen, die Telekommunikations- und Postdienstleistungen erbringen. Die Behörde wird seit Anfang 2019 von Prof. Ulrich Kelber geleitet und hat rund 220 Mitarbeitende.

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 Landesdatenschutzbeauftragten von Baden-Württemberg, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz, des Saarlandes, Sachsen-Anhalt, Schleswig-Holstein und Thüringen sind auch für die Informationsfreiheit beziehungsweise für das Akteneinsichtsrecht zuständig. Je nach Größe des Bundeslandes und nach Aufgabengebiet der Behörde haben die Landesdatenschutzbeauftragten zwischen 20 und 90 Mitarbeitende.

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 oberster Gerichte

Im Berichtszeitraum sind jeweils zwei grundlegende Urteile des Bundesverwaltungsgerichts (BVerwG) sowie des Bundesverfassungsgerichts (BVerfG) zum Datenschutz ergangen.

Videoüberwachung in Arztpraxis

Im Urteil vom 27. März 2019 hat sich das BVerwG mit den datenschutzrechtlichen Anforderungen an eine Videoüberwachung zu privaten Zwecken auseinandergesetzt (BVerwG, Urteil vom 27.03.2019, Az.: 6 C 2.18).

Hintergrund des Urteils ist die Klage einer Zahnärztin, die in ihrer Praxis oberhalb des Empfangstresens eine Videokamera angebracht hatte. Die Videokamera erfasste den Bereich hinter dem Empfangstresen sowie diejenigen Bereiche, in denen sich die Besucher aufhielten. An der Außenseite der Eingangstür sowie am Empfangstresen selbst war jeweils ein Schild mit der Aufschrift „Videogesichert“ angebracht.

Die zuständige Datenschutzaufsichtsbehörde ordnete im Jahr 2012 an, die Videokamera so auszurichten, dass die Bereiche, in denen sich die Besucher aufhielten, während der Öffnungszeiten der Praxis nicht mehr erfasst werden. Die Klägerin wendete sich gegen diese Anordnung. Die Klage blieb in allen Instanzen erfolglos und wurde in letzter Instanz vom BVerwG zurückgewiesen.

Das BVerwG stellte in seinem Urteil fest, dass eine Videoüberwachung zu privaten Zwecken nur dann zulässig ist, wenn der datenschutzrechtlich Verantwortliche plau-

sible Gründe für die Erforderlichkeit der Maßnahme darlegt. Der Grund müsse hinreichend durch Tatsachen oder die allgemeine Lebenserfahrung belegt sein und es dürfe keine andere gleich wirksame, aber mildere Maßnahme in Betracht kommen. Diese Voraussetzungen waren in dem zugrundeliegenden Fall nicht gegeben. Das BVerwG hat in Übereinstimmung mit den vorherigen Instanzen geurteilt, dass die Videoüberwachung unzulässig gewesen sei. Es seien keine plausiblen Gründe für die Erforderlichkeit der Videoüberwachung vorgebracht worden. Die Anordnung der Datenschutzaufsichtsbehörde sei ermessensfehlerfrei und verhältnismäßig erfolgt. Die dauerhaft andere Ausrichtung der Kamera sei das mildeste Mittel gewesen.

Das Urteil des BVerwG beruht noch auf der Rechtslage vor dem Inkrafttreten der DSGVO. Das BVerwG hat in dem Urteil jedoch auch auf die neue Rechtslage Bezug genommen und diesbezüglich geäußert, dass nach der neuen Rechtslage die gleichen Anforderungen an eine Videoüberwachung zu privaten Zwecken zu stellen sind. Danach seien Videoüberwachungen zu privaten Zwecken an Art. 6 Abs. 1 Unterabs. 1 lit. f) DSGVO zu messen. Eine Verarbeitung personenbezogener Daten auf der Grundlage von Art. 6 Abs. 1 Unterabs. 1 lit. e) DSGVO komme bei Privatpersonen grundsätzlich nicht in Betracht. Dies setze voraus, dass die Privatpersonen im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt dazu befugt seien auf personenbezogene Daten zuzugreifen. Dies sei nur der Fall, wenn Privatpersonen anstelle einer Behörde tätig werden.

Deaktivierungsanordnung gegen Facebook-Fanpage-Betreiber

In einem weiteren Urteil zum Datenschutz vom 11. September 2019 hat das BVerwG entschieden, dass die Betreiber einer Facebook-Fanpage für die damit in Zusammenhang stehenden Datenverarbeitungen mitverantwortlich sind und somit potenzieller Adressat einer Anordnung einer Datenschutzaufsichtsbehörde sein können (BVerwG, Urteil vom 11.09.2019, Az.: 6 C 15.18).

Eine gemeinnützige Bildungseinrichtung hat eine Facebook-Fanpage betrieben, auf der sie die Bildungseinrichtung sowie das Bildungsangebot präsentierte. Die zuständige Datenschutzaufsichtsbehörde ordnete aufgrund schwerwiegender datenschutzrechtlicher Mängel die Deaktivierung der Fanpage an. Gegen diese Anordnung wendete sich die Klägerin. In den Vorinstanzen war die Klage der Klägerin erfolgreich. Erst im Revisionsverfahren hob das BVerwG das Urteil des Oberverwaltungsgerichts auf und verwies die Sache zur erneuten Entscheidung dorthin zurück.

Zuvor hatte das BVerwG den Europäischen Gerichtshof (EuGH) in einem Vorabentscheidungsverfahren um die Auslegung verschiedener datenschutzrechtlicher Bestimmungen gebeten. Der EuGH hat entschieden, dass Betreiber einer Facebook-Fanpage für die Datenverarbeitung auf dieser Fanpage datenschutzrechtlich mitverantwortlich sind. Die Mitverantwortung folge aus der Tatsache, dass Facebook durch den Betreiber der Fanpage die Möglichkeit erhalte, auf die personenbezogenen Daten der Nutzer zuzugreifen und Cookies zu platzieren. Dies gelte unabhängig davon, ob die betroffenen Personen ein Facebook-Konto haben oder nicht.

Auf dieser Grundlage stellte das BVerwG fest, dass der Betreiber einer Facebook-Fanpage Verantwortlicher im Sinne des Datenschutzrechts ist. Er könne insofern auch Adressat einer datenschutzrechtlichen Anordnung sein. Insbesondere sei die Datenschutzaufsichtsbehörde auch nicht gehalten gewesen, sich direkt an Facebook zu wenden. Kämen mehrere Stellen als Verantwortliche im Sinne des Datenschutzrechts in Betracht, so sei eine Ermessensausübung bezüglich der Auswahl des Adressaten erforderlich. Im Sinne des Gebotes einer effektiven und wirkungsvollen Gefahrenabwehr sei es zulässig, denjenigen Verantwortlichen heranzuziehen, der den rechtswidrigen Zustand schnell und effektiv beseitigen kann. Da vorausgegangene Gespräche zwischen der Datenschutzaufsichtsbehörde und Facebook selbst erfolglos geblieben seien, sei die Inanspruchnahme der Bildungseinrichtung zulässig gewesen.

Das Urteil des BVerwG beruht noch auf der Rechtslage vor dem Inkrafttreten der DSGVO. Der Grundsatz der gemeinsamen Verantwortlichkeit ist nunmehr sowohl in der DSGVO als auch im EKD-Datenschutzgesetz ausdrücklich geregelt.

„Recht auf Vergessen I“

In dem Beschluss vom 6. November 2019 beschäftigt sich das BVerfG mit dem „Recht auf Vergessen“ (BVerfG, Beschluss vom 06.11.2019, Az.: 1 BvR 16/13).

Dem Beschluss liegt die Beschwerde einer Person zugrunde, die sich gegen die kostenlose und barrierefreie Bereitstellung von über 30 Jahre alten Presseartikeln in Onlinearchiven eines Verlags richtet. Der Beschwerdeführer ist 1982 rechtskräftig wegen Mordes verurteilt worden. In den Artikeln, die aus den Jahren 1982 und 1983 stammen, wird der Beschwerdeführer namentlich genannt. Gibt man den Namen des Beschwerdeführers in Internetsuchmaschinen ein, gelangt man zu diesen Artikeln.

Der Beschwerdeführer erhob zunächst Unterlassungsklage gegen den Verlag. Die Klage blieb in allen Instanzen erfolglos und wurde zuletzt vom BGH abgewiesen. Anschließend erhob der Beschwerdeführer Verfassungsbeschwerde und berief sich dabei auf die Verletzung seines Allgemeinen Persönlichkeitsrechts. Das BVerfG gab dem Beschwerdeführer recht und hob das Urteil des BGH auf und wies die Sache zur erneuten Entscheidung dorthin zurück.

In dem Beschluss stellte das BVerfG zunächst fest, dass der Sachverhalt, obwohl er grundsätzlich in den Anwendungsbereich des Unionsrechts fällt, primär am Maßstab der Grundrechte des Grundgesetzes zu messen ist. Es sei eine Abwägung zwischen dem Allgemeinen Persönlichkeitsrecht des Beschwerdeführers und der Meinungs- und Pressefreiheit des Verlags vorzunehmen.

Im Rahmen der Abwägung berücksichtigte das Gericht auch die zeitlichen Umstände. Dabei stellte es fest, dass bei einer aktuellen Berichterstattung über Straftaten grundsätzlich das Informationsinteresse überwiegt. Dieses nehme aber mit der Zeit immer weiter ab. In die Abwägung müsse auch die Wirkung und der Gegenstand der Berichterstattung miteinbezogen werden. Insbesondere komme es darauf an, wieweit die Berichte das Privatleben und die Entfaltungsmöglichkeiten des Betroffenen beeinträchtigen.

Aufgrund der Digitalisierung blieben Informationen dauerhaft verfügbar. Betroffene Personen müssten daher durch die Rechtsordnung davor geschützt werden, sich frühere Positionen, Äußerungen und Handlungen dauerhaft von der Öffentlichkeit vorhalten lassen zu müssen.

Daneben müsse jedoch auch die Meinungs- und Pressefreiheit des Verlags ausreichend berücksichtigt werden. Eine anonymisierte Berichterstattung beschränke sowohl die Informationsmöglichkeiten der Öffentlichkeit sowie das Recht der Presse, selbst zu entscheiden, wann und worüber sie berichtet.

Um einen angemessenen Ausgleich der Interessen zu finden, stellte das BVerfG fest, dass ein Verlag anfänglich rechtmäßig veröffentlichte Berichte grundsätzlich auch in Onlinearchive einstellen dürfe. Erst wenn sich der Betroffene mit gewichtigen Gründen an ihn wende, seien entsprechende Schutzmaßnahmen geboten. Ziel sei es, einen Ausgleich zwischen dem Schutz des Betroffenen und dem ungehinderten Zugriff auf die Originaltexte zu finden.

„Recht auf Vergessen II“

Das BVerfG beschäftigte sich in einem weiteren Beschluss vom 6. November 2019 ebenfalls mit dem „Recht auf Vergessen“ (BVerfG, Beschluss vom 06.11.2019, Az.: 1 BvR 276/17).

Dem Beschluss liegt ein Beitrag des Norddeutschen Rundfunks (NDR) zu dem Thema „Kündigung: Die fiesen Tricks der Arbeitgeber“ zugrunde, der in einer Sendung aus dem Jahr 2010 ausgestrahlt wurde. Die Beschwerdeführerin hat als Geschäftsführerin eines Unternehmens zuvor ein Interview für den Beitrag gegeben. Dieses wurde am Ende der Sendung im Zusammenhang mit der Kündigung eines ehemaligen Mitarbeitenden des Unternehmens gezeigt.

Der Beitrag wurde nach der Ausstrahlung unter dem Titel „Die fiesen Tricks der Arbeitgeber“ auf der Internetseite des NDR veröffentlicht. Durch Eingabe des Namens der Beschwerdeführerin bei dem Suchmaschinenbetreiber Google wurde der Beitrag als eines der ersten Suchergebnisse angezeigt. Die Beschwerdeführerin reichte zunächst Klage gegen Google ein, die zuletzt vom Oberlandesgericht abgewiesen wurde. Anschließend erhob die Beschwerdeführerin Verfassungsbeschwerde wegen der Verletzung ihres Allgemeinen Persönlichkeitsrechts und ihres Grundrechts auf informationelle Selbstbestimmung.

Das BVerfG hat entschieden, dass die Verfassungsbeschwerde zwar zulässig, aber unbegründet ist. Da der Sachverhalt in den Anwendungsbereich des Unionsrechts falle, seien die Grundrechte der Beschwerdefüh-

rerin auf Achtung des Privat- und Familienlebens aus Art. 7 der Grundrechtecharta (GRCh) sowie das Grundrecht auf Schutz personenbezogener Daten aus Art. 8 GRCh gegen das Recht des Suchmaschinenbetreibers auf unternehmerische Freiheit aus Art. 16 GRCh gegeneinander abzuwägen. Ebenfalls seien die unmittelbar betroffenen Grundrechte Dritter miteinzubeziehen. Dazu gehören das Informationsinteresse der Öffentlichkeit sowie die Meinungsfreiheit des NDR. Die Abwägung ergebe, dass gegenwärtig das Interesse an der Veröffentlichung des Beitrags das Interesse der Beschwerdeführerin an der Auslistung überwiege.

Der Beitrag beziehe sich auf ein berufliches Verhalten der Beschwerdeführerin, das in die Gesellschaft hineinwirke. Es sei nicht allein ihr Privatleben betroffen. Auch habe sie dem Interview zugestimmt. Daher bestehe ein fortdauerndes, wenn auch mit der Zeit abnehmendes öffentliches Informationsinteresse, das die Veröffentlichung des Beitrags rechtfertige. Die Beschwerdeführerin müsse die belastende Wirkung hinnehmen. Ein Anspruch auf Auslistung sei daher zum gegenwärtigen Zeitpunkt nicht gegeben.

In der Europäischen Union

In der Europäischen Union wurde das Datenschutzrecht im Berichtszeitraum durch eine Evaluierung der DSGVO und durch die europäische Rechtsprechung weiterentwickelt.

Datenschutz-Grundverordnung

Im Rahmen der Evaluierung der DSGVO haben auf europäischer und nationaler Ebene verschiedene Stellen mitgewirkt.

Evaluierung EU-Kommission

Gemäß Art. 97 DSGVO muss die DSGVO nach zwei Jahren und danach alle vier Jahre einer Evaluierung durch die EU-Kommission unterzogen werden. Im Vordergrund steht dabei insbesondere die Anwendung und die Wirkungsweise der Kapitel 5 und 7 der Verordnung. Zur Überprüfung und Bewertung kann die Kommission auch Informationen und Einschätzungen der nationalen Aufsichtsbehörden und der Mitgliedstaaten anfordern. Am 24. Juni 2020 hat die EU-Kommission einen Bericht vorgelegt, in dem sie eine erste positive Bilanz zur Anwendung der DSGVO in der Praxis der Mitgliedstaaten zieht. Gleichzeitig stellte sie fest, dass es noch zu früh sei, definitive Schlussfolgerungen aus der Bestandsaufnahme ziehen zu können. Die EU-Kommission betonte in dem Bericht unter anderem die große Bedeutung der Sicherstellung einer adäquaten Ausstattung der Datenschutzaufsichtsbehörden in personeller, finanzieller wie auch technischer Hinsicht und kündigte an, die Unabhängigkeit der Datenschutzaufsichtsbehörden auch künftig kritisch überwachen zu wollen. Verbesserungsbedarf attestierte die EU-Kommission im Blick auf die datenschutzrechtlichen Anforderungen bei kleinen und mittleren Unternehmen (KMU).

Entschließung Bundesrat

Auch der Bundesrat hat eine Entschließung (BR-Drucksache 570/19) gefasst und die Bundesregierung gebeten, die in der Entschließung genannten Anliegen der Bundesländer bei den weiteren Beratungen zu berücksichtigen. Hierbei stehen sowohl Praxisprobleme in der Anwendung der DSGVO bei kleinen und mittleren Unternehmen (KMU), Vereinen und Ehrenamtlichen als auch die zunehmende Konzentration der Datenverarbeitung bei einzelnen Anbietern bzw. Plattformen im Fokus. Auch auf die Risiken der zunehmenden Verbreitung von „Scoring und Profiling“ sowie auf die Chancen und Risiken von künstlicher Intelligenz als auch Blockchain-Anwendungen wird hingewiesen. Neben dem Wunsch der Bundesländer an die Bundesregierung, sich auf der europäischen Ebene gegen eine Beschränkung von Öffnungsklauseln und somit von Abweichungsmöglichkeiten der einzelnen Mitgliedsstaaten einzusetzen, werden auch einzelne Punkte genannt, die in der konkreten Auslegung der DSGVO derzeit noch umstritten sind. Hier sei exemplarisch die Frage genannt, wann eine gemeinsame Festlegung der Zwecke und Mittel zur Datenverarbeitung bei gemeinsam Verantwortlichen gemäß Art. 26 DSGVO anzunehmen ist.

Erfahrungsbericht der DSK

Der Erfahrungsbericht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zur Evaluierung der Anwendung der DSGVO bewertet neun Schwerpunkte und enthält Änderungsvorschläge. So wird beispielsweise festgestellt, dass Umfang und Inhalt der Informationspflichten möglicherweise praktikabler und bürgerfreundlicher definiert werden könnten. In der Praxis stelle sich zumindest in

manchen Konstellationen die Frage nach der Alltagstauglichkeit. Unsicherheiten bei der Meldung von Datenpannen hätten im Übrigen zu einem sehr hohen Anstieg der Meldungen geführt. Auch hier gebe es noch Klarstellungsbedarf.

Europäischer Datenschutzbeauftragter

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 und beschäftigt derzeit rund 100 Mitarbeitende.

Europäischer Datenschutzausschuss

Durch die DSGVO wurde mit dem Europäischen Datenschutzausschuss (EDSA) mit Sitz in Brüssel ein neues Gremium geschaffen. In Kapitel 7 der DSGVO finden sich in den Artikeln 60 bis 76 Regelungen zur Zusammenarbeit und Kohärenz der Aufsichtsbehörden der Mitgliedstaaten und des Europäischen Datenschutzbeauftragten (EDSB). 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 beispielsweise 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 können anschließend durch den EDSA veröffentlicht werden.

Datenschutzrechtsprechung des Europäischen Gerichtshofs

Im Bereich der europäischen Rechtsprechung sind während des Berichtszeitraums vier grundlegende Urteile des Europäischen Gerichtshofs (EuGH) zum Datenschutz ergangen.

Umfang des „Rechts auf Vergessen“

In seinen beiden Urteilen vom 24. September 2019 hat der EuGH eine Konkretisierung zum Umfang des sog. „Rechts auf Vergessen“ vorgenommen (EuGH, Urteile vom 24.09.2019, Az.: C-136/17 und C-507/17).

Das gemäß Art. 17 DSGVO gewährte Recht verpflichtet verantwortliche Stellen, die personenbezogene Daten öffentlich gemacht haben, im Fall einer Löschung angemessene Maßnahmen zu treffen. So ist z. B. nach einer Veröffentlichung auf der Internetseite ein Suchmaschinenbetreiber davon zu unterrichten, dass eine betroffene Person die Löschung aller Links, Kopien oder Replikationen seiner personenbezogenen Daten verlangt hat.

Der EuGH stellte nun klar, dass der Betreiber einer Suchmaschine – im konkreten Fall Google – nicht verpflichtet ist, im Fall eines Löschungsbegehrens personenbezogene Suchergebnisse weltweit in allen Versionen seiner Suchmaschine auszulisten. Die Auslistung müsse vielmehr nur in allen Versionen der Suchmaschine in den Mitgliedstaaten der EU vorgenommen werden.

Im Übrigen müsse durch entsprechende Maßnahmen verhindert werden, dass Nutzerinnen und Nutzer von einem Mitgliedstaat aus auf die entsprechenden Links in Nicht-EU-Versionen der Suchmaschine zugreifen können. Der EuGH begründete dies damit, dass in zahlreichen Drittstaaten, d. h. Staaten außerhalb der EU, ein Recht auf Vergessen nicht bestehe.

Das Recht auf Schutz personenbezogener Daten gelte auch nicht uneingeschränkt. Vielmehr müsse unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes und der jeweiligen gesellschaftlichen Funktion das Datenschutzrecht gegen andere Grundrechte abgewogen werden. Diese Abwägung zwischen dem Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten einerseits und der Informationsfreiheit der Internetnutzer andererseits könne weltweit sehr unterschiedlich ausfallen.

„Planet 49“

In seiner Entscheidung vom 1. Oktober 2019 hat der EuGH klarstellende Aussagen zu den Voraussetzungen einer wirksamen Einwilligung in die Verwendung von Cookies getroffen (EuGH, Urteil vom 01.10.2019,

Az.: C-673/17).

Im konkreten Fall ging es um ein Gewinnspiel auf einer Internetseite zu Werbezwecken. Der Betreiber der Internetseite hatte ein Ankreuzkästchen mit einem vorangekreuzten Häkchen verwendet.

Der EuGH stellte klar, dass für wirksame Einwilligungen auf Internetseiten ein aktives Verhalten des Nutzers erforderlich ist. Hierzu reiche es nicht aus, wenn der Nutzer bei einem vorausgewählten angekreuzten Kästchen das Kreuz entfernen muss.

Der BGH bestätigte in seinem Urteil vom 28. Mai 2020 diese Auffassung und erklärte das vorformulierte Einverständnis in das Setzen eines Cookies für unwirksam. Hierbei machte der BGH auch Ausführungen zu der Frage, ob § 15 Abs. 3 Satz 1 Telemediengesetz (TMG) mit der Richtlinie 2002/58/EG (sog. EU-Cookie-Richtlinie) vereinbar ist. Art. 5 Abs. 3 Satz 1 der Richtlinie sieht unter anderem vor, dass die Speicherung von und der Zugriff auf Informationen, die auf dem Endgerät eines Nutzers gespeichert sind, nur zulässig ist, wenn der Nutzer eingewilligt hat. Dagegen fordert § 15 Abs. 3 Satz 1 TMG lediglich einen Widerspruch und keine Einwilligung des Nutzers. Aus diesem Grund bestand Uneinigkeit darüber, ob die Vorgaben aus der EU-Cookie-Richtlinie ausreichend umgesetzt worden sind. Das hat der EuGH verneint. Der BGH stellte nun fest, dass § 15 Abs. 3 Satz 1 TMG mit Blick auf Art. 5 Abs. 3 Satz 1 der Richtlinie dahin richtlinienkonform auszulegen ist, dass der Dienstanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen darf.

Nutzung von Social Plugins

Der EuGH hat am 29. Juli 2019 über die datenschutzrechtliche Verantwortung bei der Nutzung von Social Plugins eines anderen Anbieters durch einen Internetseitenbetreiber entschieden (EuGH, Urteil vom 29.07.2019, Az.: C-40/17).

Konkret handelte es sich dabei um den „Gefällt mir"-Button von Facebook. In dem Urteil stellte der EuGH fest, dass zwischen dem Betreiber der Internetseite und dem Anbieter des Social Plugins eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO bestehe. Diese sei auf die Verarbeitung beschränkt, bei der der Betreiber der Internetseite über Zwecke und Mittel entscheidet. Dasselbe gelte bei der Beurteilung des Umfangs der Einwilligungen und der Informationspflichten. Im konkreten Fall war dies das Erheben und Übermitteln der Nutzerdaten an Facebook Irland. Der EuGH stellte klar, dass Betreiber von Websites nicht ohne weiteres Social Plugins Dritter einbinden dürfen, sondern damit selbst eine datenschutzrechtliche Verantwortung haben können.

„Schrems II"

Mit Entscheidung vom 16. Juli 2020 erklärte der EuGH das EU-US Privacy Shield für ungültig (EuGH, Urteil vom 16.07.2020, Az.: C-311/18).

Ein Bürger hatte sich an die irische Datenschutzaufsichtsbehörde gewandt und sich über die Weitergabe seiner personenbezogenen Daten durch Facebook in die USA beschwert.

Im Rahmen eines Vorabentscheidungsverfahrens stellte der EuGH fest, dass durch das EU-US Privacy Shield kein ausreichendes Datenschutzniveau sichergestellt werden könne. Dies begründete der EuGH unter anderem damit, dass beim EU-US Privacy Shield, ebenso wie in der Safe-Harbour Entscheidung, den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang eingeräumt wird. Dies ermögliche Eingriffe in die Grundrechte der Personen, deren Daten in die Vereinigten Staaten übermittelt werden. Die nach US-Recht bestehenden Eingriffsmöglichkeiten der amerikanischen Behörden auf die aus der EU übermittelten Daten seien nicht auf das zwingend erforderliche Maß beschränkt. Die betreffenden Vorschriften ließen nicht erkennen, dass für Nicht-US-Bürger Garantien existieren, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können. Insbesondere sei den betroffenen Personen kein Rechtsweg zu einem Organ eröffnet, das dem EU-Recht gleichwertige Garantien biete. Zwar sehe das EU-US Privacy Shield eine Ombudsperson vor, die von den Geheimdiensten unabhängig und dazu ermächtigt ist, gegenüber den amerikanischen Behörden verbindliche Entscheidungen zu erlassen. Tatsächlich sei die Ombudsperson aber weder unabhängig noch könne sie verbindliche Entscheidungen treffen (vgl. hierzu weiterführende Erläuterungen auf den Seiten 43 und 44).

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 Behörde „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. Vier Gliedkirchen und einige diakonische Landesverbände nehmen die Datenschutzaufsicht weiterhin eigenständig wahr.

Überblick zur Datenschutzaufsicht in der EKD

Vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofes zur Unabhängigkeit von Datenschutzaufsichtsbehörden wurden bereits 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 2014 hat der Rat der Evangelischen Kirche in Deutschland Herrn Michael Jacob zum Beauftragten für den Datenschutz der EKD berufen, der seitdem die gleichnamige, unabhängige und eigenständige Behörde (BfD EKD) leitet und für große Bereiche der evangelischen Kirche die Datenschutzaufsicht in Kirche und Diakonie ausübt. Dadurch wird die Datenschutzaufsicht innerhalb der evangelischen Kirche seit dem Jahr 2014 einheitlicher als in der Vergangenheit und in größeren Strukturen wahrgenommen. Vier Gliedkirchen und fünf diakonische Landesverbände nehmen die Datenschutzaufsicht weiterhin mit eigenen Behörden wahr. Der Beauftragte für den Datenschutz der Nordkirche, Peter von Loeper, ist seit dem 1. Oktober 2018 der stellvertretende Beauftragte für den Datenschutz der EKD.

Die Hauptaufgaben des BfD EKD sind Aufsicht, Beratung und Weiterbildung in den Bereichen des rechtlichen und technischen Datenschutzes sowie 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.

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 16 Gliedkirchen, die gliedkirchlichen Zusammenschlüsse und im Bereich von zehn diakonischen Landesverbänden wahr. Seit dem 1. Januar 2014 haben die nachfolgenden Gliedkirchen und gliedkirchlichen Zusammenschlüsse sowie diakonischen Landesverbände die Datenschutzaufsicht auf die EKD übertragen (Stand: 01.05.2021):

- Baden
- Bayern
- Berlin-Brandenburg-schlesische Oberlausitz
- Braunschweig
- Bremen
- Hannover
- Hessen und Nassau
- Kurhessen-Waldeck
- Lippe
- Mitteldeutschland
- Oldenburg
- Reformiert
- Rheinland
- Schaumburg-Lippe
- Westfalen
- 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 Berlin-Brandenburg-schlesische Oberlausitz e.V.
- Diakonisches Werk Bremen 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 in Württemberg e.V.
- Diakonisches Werk in Hessen und Nassau und Kurhessen-Waldeck e.V.
- Diakonisches Werk Rheinland-Westfalen-Lippe e.V.
- Diakonisches Werk der Evangelischen Kirche der Pfalz
- Diakonisches Werk der Evangelisch-Lutherischen Kirche in Bayern e.V.
- Diakonisches Werk der Evangelischen Landeskirche in Baden e.V.

Darüber hinaus zeichnet sich ab, dass weitere Gliedkirchen und diakonische Landesverbände Interesse haben, die Datenschutzaufsicht in absehbarer Zeit auf die EKD zu übertragen. Für die Ausgestaltung der Übertragung ist das Kirchenamt der EKD zuständig.

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 folgenden Karte zu entnehmen.

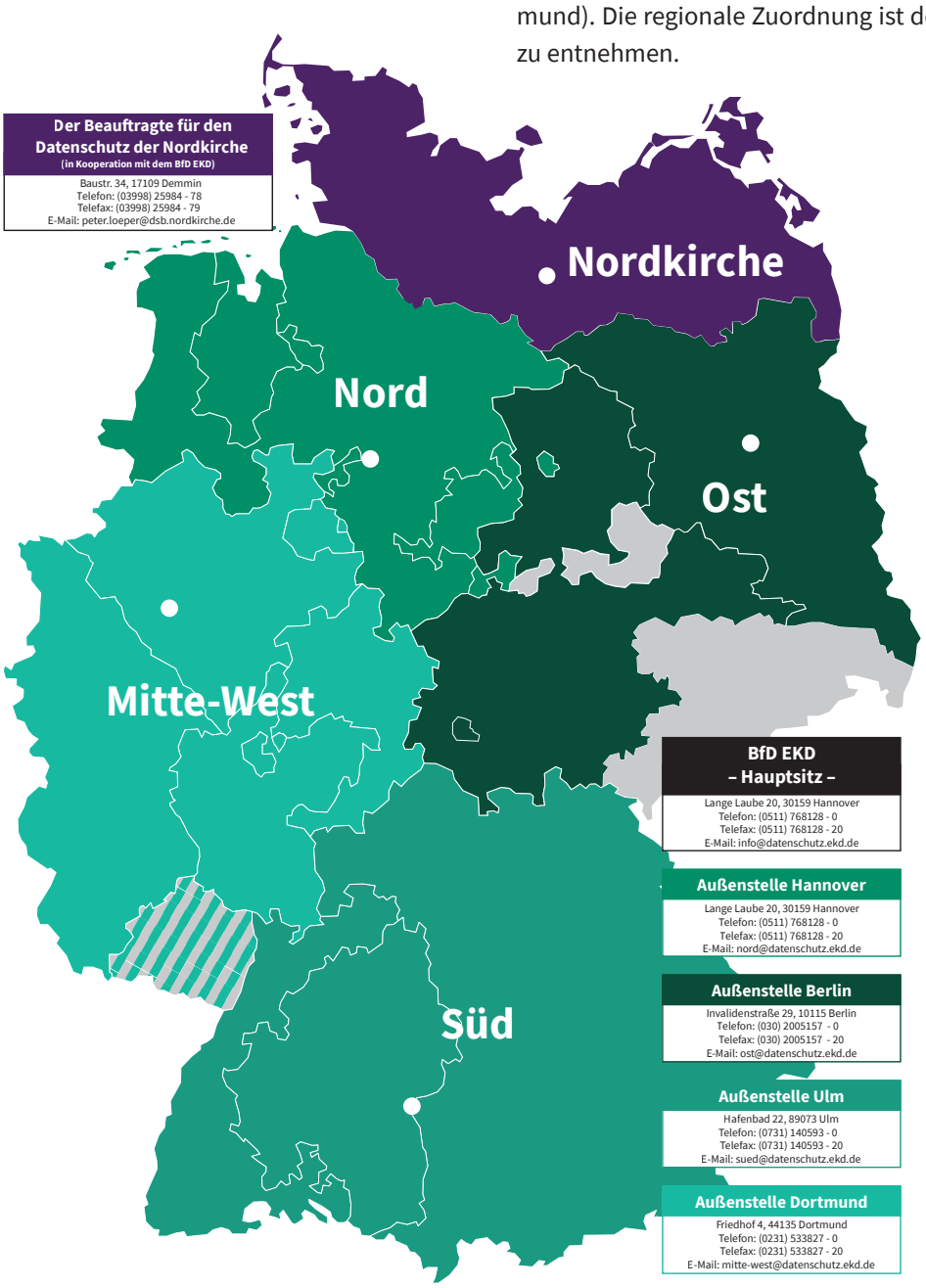

Abbildung 1: Karte mit Datenschutzregionen und Außenstellen
(Der Kooperationspartner Nordkirche ist violett hinterlegt. Die übrigen Gliedkirchen mit eigenständiger Datenschutzaufsicht sind grau hinterlegt.)

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)“. Seit der Bestellung des Beauftragten für den Datenschutz der Nordkirche zum stellvertretenden Beauftragten für den Datenschutz der EKD haben beide Aufsichtsbehörden ihre Kooperation weiter ausgebaut.

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.

Im Rahmen der fortschreitenden Übertragung der Datenschutzaufsicht der diakonischen Landesverbände konnte im Jahr 2020 auch in der Außenstelle Ulm die Stelle eines zweiten Regionalverantwortlichen besetzt werden. Ebenso ist im Jahr 2020 die Stelle der IT-Sachbearbeitung am Hauptsitz des BfD EKD erstmals besetzt worden. Auch mehrere vakante Stellen konnten im Berichtszeitraum wiederbesetzt werden. Die Auswahl von Mitarbeitenden erfolgte stets potenzial- und genderorientiert. Zum 31. Mai 2021 hat die Behörde insgesamt 22 aktivierte (Plan-)Stellen. Alle vier Außenstellen sind mit mindestens einer oder einem Regionalverantwortlichen (juristische Kompetenz), einer IT-Sachbearbeitung und einer Teamassistenz besetzt. Die Aufbauorganisation des BfD EKD zum 31. Mai 2021 ist dem Organigramm in Abbildung 2 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) inkl. Regelungen zur Behandlung vertraulicher Informationen (Klassifizierung)
- 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. Im Zuge von neu angeschaffter Hardware für die Behörde wurden weitere Bausteine aus dem IT-Sicherheitskonzept und die daraus resultierenden Maßnahmen umgesetzt. 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.

Im Berichtszeitraum wurde die Behörde auch in den Bereichen Personal und Finanzen organisatorisch weiter professionalisiert.

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

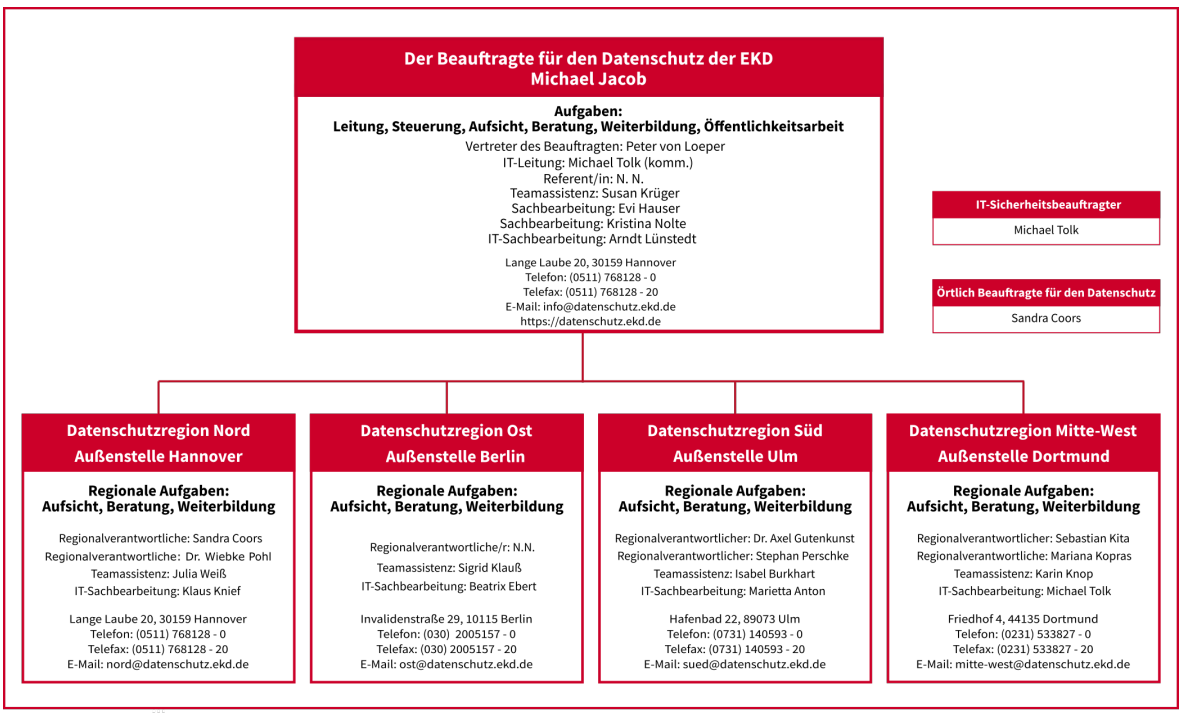

Abbildung 2: Organigramm des BfD EKD

Stand: 01.05.2021

diesem Zusammenhang wurde zusammen mit dem Referat für 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 auch für den BfD EKD ein wichtiges Thema. Mit flexiblen Arbeitszeiten und Arbeitsmodellen sind bereits einige der im Rahmen der „berufundfamilie“-Auditierung des Kirchenamtes erarbeiteten Maßnahmen in der Behörde des BfD EKD erfolgreich umgesetzt. Um die Vereinbarkeit von Beruf und Familie noch weiter zu verstärken und ebenfalls die besonderen Anforderungen der Behörde mit ihren vier deutschlandweiten Standorten stärker in das Audit mit einzubringen, hat der BfD EKD im Berichtszeitraum aktiv am Auditverfahren teilgenommen. Im Rahmen eines mit allen Mitarbeitenden durchgeführten Auditierungsworkshops wurden die bestehenden Arbeitsbedingungen evaluiert sowie Verbesserungsvorschläge erarbeitet und im Anschluss eine Zielvereinbarung mit den weiteren Umsetzungsschritten verabschiedet.

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 Finanzumlage derjenigen finanziert, die die Datenschutzaufsicht vereinbarungsgemäß oder auf gesetzlicher Grundlage auf die EKD übertragen haben. Der Finanzbeirat der EKD hat im März 2018 den Finanzbedarf der Behörde für Personal- und Sachkosten für die Jahre 2019 bis einschließlich 2021 fortgeschrieben mit der Maßgabe, dass alle Gliedkirchen und diakonischen Landesverbände die Datenschutzaufsicht auf die EKD übertragen. Dabei werden diese Kosten 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. Eine erneute Feststellung des Finanzbedarfs des BfD EKD erfolgt im September 2021 durch den Finanzbeirat der EKD.

Im Jahr 2020 hat der BfD EKD überdies aus eigener Initiative heraus und auf Grundlage des Prozesses zur Neuorientierung der Finanzstrategie der EKD eine Finanzplanung bis 2030 erstellt und diese in mehreren Gesprächen mit der Finanzabteilung des Kirchenamtes der EKD diskutiert. Der BfD EKD begrüßt im Kontext des Prozesses zur Neuorientierung der Finanzstrategie der EKD die Aufstellung der Kriterien für die Prioritätsentscheidungen durch den begleitenden Ausschuss, insbesondere das Kriterium „Die Bedeutung der gemeinschaftlichen Bearbeitung einer Aufgabe durch die EKD“. Danach sind der Ebene der EKD Themen, Arbeitsfelder oder Teilaufgaben zuzuordnen, die bei gemeinschaftlicher Bearbeitung die Stabilität und Wirksamkeit der Arbeit stärken und die Ressourcennutzung verbessern. Die Identifizierung und ggf. der Abbau von Doppel- oder Parallelstrukturen unter Evaluation der gewachsenen Geschichte sind voranzutreiben.

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. Mithin geht in den Haushaltsplan 2022 die seit Anfang 2020 erarbeitete Neustrukturierung des Handlungsfeldes 201002 „Der Beauftragte für den Datenschutz der EKD“ ein. 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 ortunabhängiges 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. Sollten Gesprächspartner keine Möglichkeit der Ende-zu-Ende-Verschlüsselung mittels PGP besitzen, können sie auf die alternative Submit-Box ausweichen, die eine Ende-zu-Ende verschlüsselte Kommunikation mit dem BfD EKD 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 jedes Jahr sechs bis acht 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 Telefonkon-

ferenzen 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.

Der BfD EKD hat im Berichtszeitraum zur weiteren Professionalisierung der Behörde und noch besseren standortübergreifenden Zusammenarbeit das Projekt „Digitalisierung“ initiiert und vorbereitet. Der BfD EKD plant in diesem Zusammenhang die Einführung eines Dokumentenmanagementsystems sowie eines Veranstaltungs- und Adressmanagements. Dafür wurden bereits die rechtlichen Rahmenbedingungen sondiert und Anforderungskriterien durch die Projektgruppe festgelegt. Das Projekt soll im nächsten Berichtszeitraum weiter vorangetrieben und durchgeführt werden.

Aufgaben und Tätigkeiten

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

Der BfD EKD ist inhaltlich in den Bereichen rechtlicher Datenschutz, technischer Datenschutz und Organisation des Datenschutzes tätig. Sämtliche Tätigkeiten des BfD EKD sind den drei Aufgaben Aufsicht, Beratung und Weiterbildung zugeordnet. Eine grobe Übersicht über die Aufgaben und Tätigkeiten des BfD EKD ist der Matrix in Tabelle 1 auf dieser Seite zu entnehmen. Über die Anzahl der in den Jahren 2019 und 2020 bearbeiteten Vorgänge in den einzelnen Aufgabenbereichen geben die Tabellen 2 und 3 auf der nachfolgenden Seite Auskunft.

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 (pro-) aktiven Datenschutz-aufsicht	✓	✓	✓						
Materialdienst (standardisierte Beratung)				✓	✓	✓			
einzelfallbezogen	✓	✓	✓	✓	✓	✓			
einheitliches und aufeinander abgestimmtes (modulares) Weiterbildungsangebot für örtlich Beauftragte für den Datenschutz							✓	✓	✓
individuelles Angebot für andere Zielgruppen							✓	✓	✓
schwerpunktsetzend	✓	✓	✓	✓	✓	✓	✓	✓	✓

Tabelle 2: Statistik über die Anzahl der Tätigkeiten im Jahr 2019

	Aufsicht	Beratung	Weiterbildung	Gesamt
Hauptsitz	15	39	5	**59**
AS Hannover	108	280	8	**396**
AS Berlin	44	90	6	**140**
AS Ulm	124	353	19	**496**
AS Dortmund	143	259	15	**417**
Summe	**434**	**1021**	**53**	**1508**

Tabelle 3: Statistik über die Anzahl der Tätigkeiten im Jahr 2020

	Aufsicht	Beratung	Weiterbildung	Gesamt
Hauptsitz	17	36	5	**58**
AS Hannover	116	219	1	**336**
AS Berlin	49	83	3	**135**
AS Ulm	159	303	1	**463**
AS Dortmund	133	272	6	**411**
Summe	**474**	**913**	**16**	**1409**

Tabelle 4: Statistik über die Anzahl der gemeldeten Datenpannen und eingegangenen Beschwerden in den Jahren 2019 und 2020

	2019	2020
Datenpannen	199	234
Beschwerden	235	240
Summe	**434**	**474**

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 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 wird der BfD EKD bei seinem Handeln zukünftig stärker berücksichtigen. Im Berichtszeitraum wurden eingehende Datenpannenmeldungen, Beschwerden und Eingaben ordnungsgemäß bearbeitet.

Zur Etablierung einer (pro-)aktiven Datenschutzaufsicht hat der BfD EKD zu Beginn des Berichtszeitraums ein Konzept unter Zugrundelegung eines risikobasierten Prüfansatzes erarbeitet, mit dem Körperschaften auf der mittleren Ebene einer Landeskirche geprüft werden sollten. Dabei zeigte sich im Rahmen von ersten Umsetzungsschritten, dass das Verfahren aufgrund fehlender bzw. schwer zu beschaffener Daten nicht praktikabel war. Zudem erwies sich die Risikoermittlung als unverhältnismäßig im Verhältnis von Aufwand und Nutzen. Aufgrund der gesetzlichen Anforderungen aus den §§ 43 und 44 DSG-EKD sowie den Vorgaben aus der Rechtsprechung des Europäischen Gerichtshofs besteht für den BfD EKD aber die Verpflichtung verantwortliche Stellen zu prüfen, ohne dass ein konkreter Anlass (z. B. Beschwerde oder Hinweis) vorliegt.

Daher hat der BfD EKD nunmehr ein Verfahren zur Durchführung von Schwerpunktprüfungen konzipiert und setzt dieses im folgenden Berichtszeitraum um. Die Schwerpunktprüfungen werden in einem ersten Prüfzyklus in 100 zufällig ermittelten evangelischen Kindertageseinrichtungen zum Thema ‚Sicherheit von mobilen Endgeräten' durchgeführt. Die Auswahl dieses Handlungsfeldes kirchlich-diakonischer Arbeit mit diesem Thema erfolgte aufgrund der besonderen Schutzwürdigkeit von Kindern und der Erkenntnis aus den gemeldeten Datenpannen, dass es einen signifikant hohen Anteil verlorener oder gestohlener mobiler Endgeräte im Bereich von Kindertageseinrichtungen gibt. Die Schwerpunktprüfungen werden mittels eines online-basierten Fragebogens durchgeführt. In zukünftigen Prüfzyklen beabsichtigt der BfD EKD andere Bereiche kirchlich-diakonischer Arbeit zu prüfen (z. B. Krankenhäuser, Kirchengemeinden, Beratungsstellen, etc.).

Darüber hinaus hat der BfD EKD im Berichtszeitraum ein Konzept zur Bemessung von Geldbußen nach § 45 DSG-EKD erarbeitet. Vor diesem gesetzlichen Hintergrund beschreibt das Konzept ein standardisiertes Verfahren zur Ermittlung der Bußgeldhöhe und ermöglicht somit dem BfD EKD eine überprüfbare, transparente und einzelfallbezogene Festsetzung von Geldbußen. Das Konzept findet Anwendung für die Bemessung von Geldbußen gegen kirchliche Stellen, die in den Anwendungsbereich des EKD-Datenschutzgesetzes fallen und als Unternehmen im Sinne des § 4 Nr. 19 DSG-EKD am Wettbewerb teilnehmen. Bußgelder wurden bisher nicht verhängt.

Beratung
Die Bearbeitung sämtlicher Beratungsanfragen ist ein Hauptbestandteil der Arbeit aller Mitarbeitenden des BfD EKD. Wie aus den Tabellen 2 und 3 hervorgeht, ist die Anzahl der Beratungsanfragen gleichbleibend hoch. Dabei ist erkennbar, dass die Anfragen den folgenden Themenbereichen zugeordnet werden können:

- Auswirkungen der Corona-Pandemie
- Datenerhebung und Auskunftsrecht
- Besondere Datenschutzthemen im gemeindlichen Alltag
- Datenübermittlung in Drittländer und Auftragsverarbeitung
- Digitale Kommunikation und Videoüberwachung
- Datensicherheit, Verschlüsselung und „Cookies"
- Softwareentwicklung und Softwareprüfung
- 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 „Über die Themen bei Aufsicht und Beratung" ab Seite 33 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. Informationen zum Thema Weiterbildung 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 wird eine Basisqualifikation zum Datenschutz vermittelt. In drei Modulen wird eine Einführung in den rechtlichen und technischen Datenschutz und die Organisation des Datenschutzes gegeben. Die Teilnahmegebühr umfasst die vom BfD EKD erbrachten Leistungen inklusive Schulungsmaterial, Übernachtungs- und Verpflegungskosten. Im Jahr 2019 betrug sie 330,00 €.

Die 3-tägigen 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. Die Teilnahmegebühr umfasst die vom BfD EKD erbrachten Leistungen inklusive Schulungsmaterial, Übernachtungs- und Verpflegungskosten. Im Jahr 2019 betrug sie 330,00 €.

Die Anzahl der im Jahr 2019 durchgeführten Grund- und Aufbauseminare können der Tabelle 5 entnommen werden. An jedem Grund- und Aufbauseminar nahmen 20 Personen teil. Im Jahr 2020 konnten die Grund- und Aufbauseminare, bis auf ein Grundseminar in Augsburg Anfang 2020, aufgrund der Corona-Pandemie nicht stattfinden. Der BfD EKD hat sein komplettes Seminarprogramm im Jahr 2020 auf ein Online-Format umgestellt, sodass im laufenden Jahr 2021 nunmehr fünf Grundseminare und fünf Aufbauseminare durchgeführt werden können.

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 Beauftragte für den Datenschutz in kirchlichen und diakonischen Einrichtungen aus Landeskirchen und Diakonischen Werken, die die Datenschutzaufsicht auf den Beauftragten für den Datenschutz der EKD übertragen haben. Die Datenschutz-Infotage für örtlich Beauftragte werden

vom Hauptsitz des BfD EKD sowie von den Mitarbeitenden der jeweiligen Außenstellen des BfD EKD geleitet und durchgeführt. In den Jahren 2019 und 2020 wurden jeweils vier Datenschutz-Infotage durchgeführt. Die Hauptthemen waren im Jahr 2019 Cloud- und Messenger-Dienste und im Jahr 2020 Homeoffice und Videokonferenz-Dienste. Die Datenschutz-Infotage wurden in 2020 aufgrund der Corona-Pandemie online durchgeführt. Im Jahr 2019 nahmen an den vier Regionalkonferenzen im Ganzen ca. 500 Personen teil, im Jahr 2020 online ca. 400 Personen.

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. Auf den Erfa-Kreisen können sich örtlich Beauftragte für den Datenschutz gemeinsam datenschutzrechtlichen oder technischen Problemen und Themen fachlich nähern und austauschen. Die Erfa-Kreise bieten auch eine Möglichkeit sich mit anderen örtlich Beauftragten für den Datenschutz zu vernetzen. 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 Werken, die die Datenschutzaufsicht auf den Beauftragten für den Datenschutz der 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 Beauftragten für den Datenschutz der EKD angeboten. Die Termine werden zeitnah auf der Website des BfD EKD veröffentlicht. Im Herbst 2020 fanden die Erfa-Kreise erstmalig online statt. Für die Teilnahme an den Erfa-Kreisen fällt keine Gebühr an. Die Anzahl der durchgeführten Erfa-Kreise kann Tabelle 6 entnommen werden.

Sensibilisierung

Daneben widmet sich der BfD EKD auch weiterhin der Sensibilisierung von anderen Beschäftigten und (Leitungs-)Gremien zu datenschutzrechtlichen und -technischen Themen mit individuellen Vorträgen. Im Berichtszeitraum 2019/2020 hat der BfD EKD 60 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

Tabelle 5: Statistik über die Anzahl der durchgeführten Grund- und Aufbauseminare im Jahr 2019

	AS Berlin	AS Dortmund	AS Hannover	AS Ulm	Nord-kirche	Haupt-sitz	Summe
Grundseminare 2019	2	2	2	2	2		**10**
Aufbauseminare 2019						5	**5**
					Gesamt		**15**

Tabelle 6: Statistik über die Anzahl der durchgeführten Erfa-Kreise in den Jahren 2019 und 2020

	AS Berlin	AS Dortmund	AS Hannover	AS Ulm	Summe
Erfa-Kreise 2019	2	4	2	2	**10**
Erfa-Kreise 2020		3	1	1	**5**
				Gesamt	**15**

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 regelmäßigen 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. Auch für die Einrichtungen selber ist das Thema von hoher Relevanz. Und in der Kirchengemeinde ist das Thema in der Konfirmanden- und Jugendarbeit präsent. Zum Schwerpunktthema wurden bislang mehrere Materialien veröffentlicht. Im Berichtszeitraum hat der BfD EKD mehrere Vorträge zu diesem Thema gehalten. Zur Vernetzung mit den evangelischen Schulen nimmt der BfD EKD regelmäßig an der Wirtschaftskonferenz Evangelischer Schulen teil. Im Rahmen der Vernetzung mit staatlichen Aufsichtsbehörden waren im Berichtszeitraum die Bemühungen zur Aufnahme des BfD EKD in den Arbeitskreis Schulen und Bildungseinrichtungen der DSK erfolgreich. Darüber hinaus gibt es eine Kooperation mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. zum Projekt „Datenschutz geht zur Schule“.

Gesundheitsdatenschutz

Das Thema Gesundheitsdatenschutz spielt im kirchlichen Datenschutz vor allem in der Diakonie seit jeher eine bedeutende Rolle, da es sich bei Gesundheitsdaten regelmäßig um besondere Kategorien personenbezogener Daten gemäß § 4 Nr. 2 DSG-EKD handelt. Gesundheitsdaten liegen bereits vor, sobald Informationen einen Rückschluss auf den physischen oder psychischen Gesundheitszustand zulassen. Zum Schwerpunktthema wurden bislang mehrere Materialien veröffentlicht. Im Berichtszeitraum hat der BfD EKD mehrere Vorträge zu diesem Thema gehalten, um die datenschutzrechtlichen Pflichten hinsichtlich der besonderen Arbeitsbereiche der Diakonie im Gesundheits- und Sozialbereich darzustellen und zu besprechen. Im Rahmen der Vernetzung mit staatlichen Aufsichtsbehörden wurden im Berichtszeitraum die Bemühungen zur Aufnahme des BfD EKD in den Arbeitskreis Gesundheit und Soziales der DSK fortgesetzt. Des Weiteren plant der BfD EKD im nächsten Berichtszeitraum eine Fachgruppe Diakonie zu errichten.

Ehrenamtliche

Das Engagement von Ehrenamtlichen ist in vielen Bereichen von Kirche und Diakonie unverzichtbar. Wo Ehrenamtliche sich engagieren, kommen sie auch mit personenbezogenen Daten in Kontakt. Dabei gewinnen Ehrenamtliche auch Einblicke in persönliche und sachliche Verhältnisse von Gemeindegliedern, Beschäftigten sowie von Ratsuchenden, Betreuten oder anderen Personen. Um den Schutz der Persönlichkeitsrechte dieser Personen sicherzustellen, wurden Ehrenamtliche im Berichtszeitraum intensiv beraten und begleitet, wie sie im Rahmen ihrer Tätigkeit Persönlichkeitsrechte Dritter wahren können. Dabei wurde darauf hingewirkt, dass IT-Systeme „ehrenamtfreundlich“ gestaltet werden. Insbesondere soll die Einbindung der Ehrenamtlichen in die kirchliche oder diakonische Arbeit so ermöglicht werden, dass keine Sicherheitsrisiken entstehen und der Schutz von personenbezogenen Daten gewahrt bleibt.

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 drei Kurzinformationen veröffentlicht (Mitarbeitervertretung und Datenschutz, Was müssen Mitarbeitende über den Datenschutz wissen?, Datenschutz in Personalakten) und mehrere Vorträge gehalten. Die Tätigkeiten zum Schwerpunktthema umfassten im Berichtszeitraum

auch die erfolgreichen Bemühungen zur Aufnahme des BfD EKD in den 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 kirchlichen 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 Microsoft Cloud-Diensten vom 4. April 2019

- Häufig gestellte Fragen (FAQ)
  - Häufig gestellte Fragen zum Urteil des EuGH vom 16. Juli 2020 „Schrems II“
  - Häufig gestellte Fragen zum Medienprivileg
  - Häufig gestellte Fragen zum kirchlichen Datenschutz in (Förder-)Vereinen
  - Häufig gestellte Fragen zur Bestellung von örtlich Beauftragten für den Datenschutz
  - Häufig gestellte Fragen aus den Kirchengemeinden
  - Häufig gestellte Fragen zum (neuen) EKD-Datenschutzgesetz

- Handreichung
  - Datenschutz bei der Anfertigung und Veröffentlichung von Fotos
  - Arbeitshilfe zur Durchführung einer Datenschutz-Folgenabschätzung
  - Arbeitshilfe zur Umsetzung von Informationspflichten

- Kurzinformation
  - Datenschutz in Personalakten
  - Was müssen Mitarbeitende über den Datenschutz wissen?
  - Mitarbeitervertretung und Datenschutz

- Muster
  - Verzeichnis von Verarbeitungstätigkeiten

- Stellungnahme
  - Gemeinsame Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zum „Schrems II“ Urteil des EuGH vom 16. Juli 2020
  - Gemeinsame Stellungnahme des Beauftragten für den Datenschutz der EKD und des Beauftragten für den Datenschutz der Nordkirche zum Homeoffice im Zusammenhang mit der Corona-Pandemie vom 27. März 2020
  - Gemeinsame Stellungnahme des Beauftragten für den Datenschutz der EKD und des Beauftragten für den Datenschutz der Nordkirche zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Corona-Pandemie vom 20. März 2020

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

- BfD EKD verzeichnet mehr Datenschutzverstöße, veröffentlicht am 24. Mai 2020
- BfD EKD legt Tätigkeitsbericht vor, veröffentlicht am 28. Juni 2019
- Datenschutz ist Grundrechteschutz, veröffentlicht am 24. Mai 2019
- Der kirchliche Datenschutz ist auf einem guten Weg, veröffentlicht am 25. Januar 2019

Um auch über andere Kommunikationskanäle die Sensibilisierung weiter voran zu treiben, verfasst der BfD EKD

regelmäßig Artikel für kirchliche und diakonische Zeitschriften und gibt Interviews.

Anlässlich des Europäischen Datenschutztages 2020 führte der BfD EKD in den Räumlichkeiten an seinem Hauptsitz am 29. Januar 2020 die Veranstaltung „Kirchlicher Datenschutz in neuen Räumen“ durch. Zahlreiche Gäste aus Kirche, Staat und Politik folgten der Einladung, um sich zu vernetzen und Erfahrungen und Ideen zum Motto „Datenschutz beginnt bei mir“ auszutauschen. Neben Dialog und Vernetzung stand zu Beginn der Veranstaltung ein datenschutzbezogener geistlicher Impuls sowie ein fachlicher Impuls zum Spannungsverhältnis des Datenschutzes im Vordergrund.

Planungen des BfD EKD zusammen mit den katholischen Datenschutzaufsichtsbehörden auf dem 3. Ökumenischen Kirchentag in Frankfurt/Main im Jahr 2021 mit einem gemeinsamen Informationsstand und einer Podiumsdiskussion zum Thema Datenschutz vertreten zu sein, wurden coronabedingt abgesagt.

Daneben hat der BfD EKD an seinen Standorten die lokale Sichtbarkeit verbessert.

Kooperation mit der Aufsichtsbehörde der Nordkirche

Mit der Berufung von 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. Im Jahr 2019 wurden die Seminare für örtlich Beauftragte für den Datenschutz erstmals in Kooperation mit dem Beauftragten für den Datenschutz der Nordkirche durchgeführt. Auch die jeweiligen Internetseiten sind bestmöglich aufeinander bezogen. Bei grundlegenden Datenschutzfragen stimmen beide Aufsichtsbehörden ihre Positionen und ihr Vorgehen miteinander ab. Im Rahmen der Zusammenarbeit sind im Berichtszeitraum folgende Stellungnahmen gemeinsam erarbeitet und veröffentlich worden:

- Gemeinsame Stellungnahme des Beauftragten für den Datenschutz der EKD und des Beauftragten für den Datenschutz der Nordkirche zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Corona-Pandemie vom 20. März 2020
- Gemeinsame Stellungnahme des Beauftragten für den Datenschutz der EKD und des Beauftragten für den Datenschutz der Nordkirche zum Homeoffice im Zusammenhang mit der Corona-Pandemie vom 27. März 2020

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 dem 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 sowie zu den Abteilungsleitungen Recht und Finanzen und zu dem für Datenschutzrecht zuständigen Referenten 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 -referenten sowie IT‘lerinnen und IT‘ler) 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 -referenten organisiert. Diese Treffen dienen dem fachlichen Austausch. In den Jahren 2019 und 2020 nutzte der BfD EKD diese Treffen, um mit den Datenschutzreferentinnen und -referenten über die erforderlichen Anpassungen der landeskirchlichen Rechtsvorschriften in Bezug auf das neue EKD-Datenschutzgesetz zu diskutieren sowie über das aufsichtliche Handeln des BfD EKD zu informieren. Neben diesen Kontakten werden landeskirchliche Vertreter auch in Arbeitsgruppen des BfD EKD eingebunden. Darüber hinaus fand auch in diesem Berichtszeitraum ein fachlicher Austausch mit dem Sprecherrat der Arbeitsgemeinschaft der Leitungen der kirchlichen Rechnungsprüfungseinrichtungen in der Evangelischen Kirche in Deutschland (kirpag) statt.

Der BfD EKD steht auch in Erfüllung des gesetzlichen Auf-

trags 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 2019 hat die Konferenz in Oesede bei Osnabrück und im Jahr 2020 online stattgefunden. Im Rahmen der Zusammenarbeit sind im Berichtszeitraum folgende Entschließung und 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 Microsoft Cloud-Diensten vom 4. April 2019
- Gemeinsame Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zum „Schrems II“ Urteil des EuGH vom 16. Juli 2020

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). Ausgebaut hat der BfD EKD seine Zusammenarbeit mit dem Kirchenrechtlichen Institut der Evangelischen Kirche in Deutschland, indem er im Berichtszeitraum mehrere Gutachten im Kontext des kirchlichen Datenschutzes in Auftrag gegeben sowie durch gemeinsame Treffen, Telefonate und der Teilnahme an Veranstaltungen auch den persönlichen Kontakt gestärkt hat. 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 (KDM)“. Ein entsprechender Projektauftrag hierzu wurde 2019 beim Ökumenischen Datenschutztag formuliert.

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 in deren Behörden.

Daneben nimmt der BfD EKD am regelmäßigen Austausch der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) mit den spezifischen Aufsichtsbehörden teil. Dabei fruchteten zudem die Bemühungen, zukünftig von der DSK stärker beteiligt zu werden. Der BfD EKD ist nunmehr Mitglied in den folgenden fünf Arbeitskreisen der DSK:

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

Darüber hinaus ist der BfD EKD Gast in der DSK-Taskforce Schrems II. Eine konkrete Mitwirkung in der DSK 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 zur eigenständigen Datenschutzaufsicht 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.

Auswirkungen der Corona-Pandemie

Die Auswirkungen der Corona-Pandemie sind auch im Bereich des Datenschutzes zu spüren. Immer wieder wird auch diskutiert, ob der Datenschutz zugunsten der Pandemiebekämpfung eingeschränkt werden darf. Die für alle in diesem Ausmaß unbekannte pandemische Situation sowie die ständig wechselnden und in den einzelnen Bundesländern unterschiedlichen Regelungen erschwerten die Situation zusätzlich. Den BfD EKD haben daher verschiedene Beratungsanfragen zu den Auswirkungen der Corona-Pandemie in Bezug auf den Datenschutz erreicht.

Erfassung von Gottesdienstbesuchern

Die Corona-Pandemie hat Kirchengemeinden vor große Herausforderungen gestellt. Nachdem Gottesdienste zu Beginn der Pandemie über mehrere Wochen nicht stattfinden durften, wurden die Regelungen im weiteren Verlauf wieder gelockert. Gottesdienste durften unter Einhaltung von bestimmten Sicherheitsvorkehrungen wieder stattfinden.

Eine wichtige Sicherheitsvorkehrung war – und ist auch weiterhin – die Erfassung von Gottesdienstbesuchern. Vor dem Besuch der Gottesdienste sind die Kirchengemeinden verpflichtet, alle Teilnehmenden zum Zweck der **Nachvollziehbarkeit der Infektionsketten** zu erfassen. Diese Regelung geht auf den Bund-Länder-Beschluss vom 30. April 2020 zurück, in dem unter anderem beschlossen wurde, dass Kirchengemeinden Vorkehrungen treffen müssen, um Infektionsketten rasch und vollständig nachvollziehen zu können. Wie die entsprechenden Vorkehrungen aussehen sollen und wie diese umzusetzen sind, ergibt sich aus dem Bund-Länder-Beschluss jedoch nicht. Jedes Bundesland ist verpflichtet, die zu treffenden Sicherheitsvorkehrungen eigenständig zu gestalten. Dies hat zu einer nur schwer zu überblickenden Rechtslage und zur Verunsicherung bei vielen Kirchengemeinden und Gemeindegliedern geführt.

Die Erfassung von Gottesdienstbesuchern ist nur bei **Vorliegen** einer entsprechenden **Rechtsgrundlage** zulässig. In manchen Bundesländern ist in der jeweiligen Corona-Schutzverordnung bzw. Corona-Bekämpfungsverordnung des Landes ausdrücklich geregelt, dass Gottesdienstbesucher zu erfassen sind. In anderen Bundesländern wurde dagegen keine Regelung getroffen. In diesen Fällen kommt als Rechtsgrundlage § 6 DSG-EKD in Betracht. Gemäß § 6 Nr. 7 DSG-EKD ist die Verarbeitung von personenbezogenen Daten rechtmäßig, wenn die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Durch die Erfassung der Gottesdienstbesucher ist es möglich, Infektionsketten nachzuvollziehen und gefährdete Personen rechtzeitig zu informieren.

Bei der Erfassung der Gottesdienstbesucher ist weiter zu fragen, **welche personenbezogenen Daten erfasst werden dürfen und wie diese aufzubewahren** sind. In einigen Landesverordnungen ist ausdrücklich geregelt, welche personenbezogenen Daten zu erfassen sind. Im Übrigen dürfen nur solche personenbezogenen Daten erfasst werden, die tatsächlich auch zur Nachvollziehbarkeit der Infektionsketten erforderlich sind. Dazu gehören der Vor- und Zuname sowie die Adresse oder Telefonnummer der betroffenen Person. Bei der Erfassung der personenbezogenen Daten sollte darauf geachtet werden, dass die Teilnehmenden einen separaten Zettel ausfüllen, sodass niemand die personenbezogenen Daten der anderen Teilnehmenden einsehen kann. Die separaten Zettel sollten in einem verschlossenen Umschlag, z. B. in einem abschließbaren Schrank, aufbewahrt und nach Ende der Inkubationszeit, maximal jedoch nach 4 Wochen, vernichtet werden.

Kontaktloses Fiebermessen bei Mitarbeitenden

Gerade zu Beginn der Pandemie wurde in den Medien vermehrt darüber berichtet, dass – vor allem im Ausland – an Flughäfen und an anderen öffentlichen Orten Fiebermessungen zur Erkennung einer möglichen COVID-19-Infektion durchgeführt wurden. In diesem Zusammenhang wurde von einer diakonischen Einrichtung die Frage gestellt, ob vor Dienstbeginn ein kontaktloses Fiebermessen bei den Mitarbeitenden als Bestandteil des Hygienekonzeptes durchgeführt und die Messdaten sodann in einer Excel-Tabelle dokumentiert werden könnten. Diese Maßnahme sollte der Vorbeugung einer COVID-19-Infektion dienen.

Nach Art. 13 Abs. 2 Nr. 2 DSG-EKD in Verbindung mit § 49 Abs. 1 DSG-EKD ist die **Verarbeitung besonderer Kategorien personenbezogener Daten** für Zwecke des **Beschäftigungsverhältnisses** unter anderem zulässig, wenn die Datenerhebung zur Ausübung von Rechten

oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht erforderlich ist und das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung nicht überwiegt. Im konkreten Zusammenhang stellt insbesondere die Fürsorgepflicht des Arbeitgebers eine solche rechtliche Pflicht aus dem Arbeitsrecht dar.

Zum Zeitpunkt der Anfrage im April 2020 konnte noch nicht eindeutig abgeschätzt werden, ob Fiebermessen eine **geeignete Maßnahme** zur Feststellung einer COVID-19-Infektion darstellt. Vor dem Hintergrund, dass die anfragende diakonische Einrichtung auch Menschen betreut, die zur Risikogruppe gehören, wurde kontaktloses Fiebermessen bei Mitarbeitenden in diesem Fall für erforderlich und damit für datenschutzrechtlich zulässig gehalten. Letztlich hat sich herausgestellt, dass Fiebermessen als Maßnahme nur bedingt geeignet ist, um eine COVID-19-Infektion nachzuweisen. Nach Angaben des Robert Koch-Institutes entwickle nur die Hälfte aller Infizierten überhaupt Fiebersymptome. Zudem könne Fieber durch Medikamente gesenkt werden. Eine Datenverarbeitung ist jedoch nur in Fällen erforderlich, in denen die personenbezogenen Daten für die Aufgabenerfüllung der verantwortlichen Stelle unabdingbar sind. Dies ist wiederum der Fall, wenn die Aufgabe ohne die Kenntnis der Information nicht, nicht rechtzeitig, nur mit unverhältnismäßigem Aufwand oder nur mit sonstigen unverhältnismäßigen Nachteilen erfüllt werden kann. Vor dem Hintergrund der zwischenzeitlichen Erkenntnisse wird man die Erforderlichkeit beim Fiebermessen von Mitarbeitenden vor dem Betreten einer diakonischen Einrichtung nicht mehr bejahen können.

Insoweit hat der BfD EKD im weiteren Verlauf dahingehend beraten, keine Fiebermessungen bei Mitarbeitenden vor Dienstbeginn bzw. vor dem Betreten der Arbeitsstätte durchzuführen. Der Arbeitgeber kann seiner **Fürsorgepflicht** anders nachkommen, indem er beispielsweise anordnet, dass die Mitarbeitenden im Fall von grippalen Symptomen einen Arzt aufsuchen oder – sofern möglich – Homeoffice anordnet. Abschließend ist anzumerken, dass eine Erfassung der gemessenen Temperaturen in einer Excel-Tabelle datenschutzrechtlich zu keinem Zeitpunkt zu rechtfertigen war und ist.

Notbetreuung von Kindern während der Schließzeiten der Kindertageseinrichtung

Ein Elternteil wandte sich an den BfD EKD und fragte, welche personenbezogenen Daten von ihm durch eine evangelische Kindertageseinrichtung angefordert werden dürfen, um einen Antrag auf Notbetreuung des Kindes zu begründen.

Im konkreten Fall forderte die Kindertageseinrichtung die Personensorgeberechtigten dazu auf, einen **Nachweis des Arbeitgebers** beizubringen, dass sie in der fraglichen Zeit aus betriebsbedingten Gründen keinen Urlaub nehmen können. Darüber hinaus sollten sie ihren kompletten **Jahresurlaub** gegenüber der Kindertageseinrichtung **offenlegen**.

Grundsätzlich kann die Gewährung einer Notbetreuung an die Vorlage eines Nachweises geknüpft werden. Anspruch auf eine Notbetreuung haben lediglich Kinder, deren Eltern im Zeitraum der Schließzeit keine andere Betreuungsmöglichkeit haben und insbesondere aus betrieblichen Gründen keinen Urlaub nehmen können.

Bei der **Ausgestaltung von Formularen** dürfen jedoch lediglich die personenbezogenen Daten abgefragt werden, die für den konkreten Zweck **erforderlich** sind.

Die Mitteilung aller Daten des gesamten Jahresurlaubs ist nicht erforderlich. Es muss lediglich der Nachweis erbracht werden, dass die Personensorgeberechtigten in den Schließzeiten der Kindertageseinrichtung aus betrieblichen Gründen keinen Urlaub nehmen können und somit Anspruch auf einen Platz in der Notbetreuung besteht. Dies lässt sich auch ohne eine konkrete Aufzählung des Jahresurlaubs nachweisen.

Arbeiten im Homeoffice ohne dienstliche IT-Ausstattung

Die Corona-Pandemie hatte in vielen Fällen zur Folge, dass viele Mitarbeitende plötzlich ins Homeoffice geschickt wurden, ohne dass die Mitarbeitenden im Besitz dienstlicher Endgeräte waren und die erforderlichen technischen Voraussetzungen gegeben waren. Viele Mitarbeitende haben deswegen die Frage gestellt, ob sie dienstliche E-Mails an ihre private E-Mail-Adresse weiterleiten und ihre privaten mobilen Endgeräte zu dienstlichen Zwecken nutzen dürfen.

Aus datenschutzrechtlicher Sicht ist die **Weiterleitung von dienstlichen E-Mails auf private E-Mail-Adressen** – auch in Ausnahmesituationen – als unzulässig zu beurteilen.

Gemäß § 27 Abs. 1 DSG-EKD ist die verantwortliche Stelle bei der Verarbeitung von personenbezogenen Daten dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten und Datensicherheit herzustellen. Die verantwortliche Stelle muss sicherstellen, dass die empfangenen und versendeten E-Mails entsprechend den datenschutzrechtlichen Bestimmungen geschützt sind. Dieser Schutz ist nicht sichergestellt, sobald die E-Mails an die private E-Mail-Adresse des Mitarbeitenden weitergeleitet werden. Bei privaten E-Mail-Accounts besteht in der Regel kein gleichwertiges Schutzniveau.

Das fehlende Schutzniveau wird insbesondere auch in Fällen deutlich, in denen die private E-Mail-Adresse von mehreren Personen (z. B. Familienmitgliedern) gemeinsam genutzt wird oder Dritten zumindest die Zugangsdaten bekannt sind. Es kann nicht ausgeschlossen werden, dass Unbefugte Einsicht in die dienstlichen E-Mails nehmen können.

Ein Risiko für den Schutz der personenbezogenen Daten besteht auch in dem Moment, in dem die E-Mails von der dienstlichen E-Mail-Adresse an die private E-Mail-Adresse weitergeleitet werden. Die E-Mails können während der **Weiterleitung** von Unbefugten abgefangen werden, sofern der Anbieter der privaten E-Mail-Adresse keine Transportverschlüsselung unterstützt. Darüber hinaus werden die weitergeleiteten E-Mails zunächst auf dem Server des Anbieters des privaten E-Mail-Accounts gespeichert. Es besteht daher die Möglichkeit, dass der Administrator des Anbieters des privaten E-Mail-Accounts auf die dienstlichen E-Mails zugreift.

Weiter ist zu beachten, dass die verantwortliche Stelle ohne **Einwilligung des Mitarbeitenden** nicht mehr auf die dienstlichen E-Mails zugreifen kann, sobald diese an die private E-Mail-Adresse weitergeleitet wurden. Die verantwortliche Stelle kann nicht kontrollieren, ob die personenbezogenen Daten datenschutzkonform verarbeitet und schließlich auch unwiederbringlich gelöscht werden.

Die Weiterleitung von dienstlichen E-Mails an private E-Mail-Adressen kann neben den datenschutzrechtlichen Folgen auch zu arbeitsrechtlichen Konsequenzen führen.

Für die **Nutzung von privaten Endgeräten zu dienstlichen Zwecken** gilt in der Regel das Gleiche wie für die Weiterleitung von dienstlichen E-Mails auf private E-Mail-Adressen. Die Nutzung privater Endgeräte zu dienstlichen Zwecken ist grundsätzlich unzulässig. Lediglich in **Ausnahmefällen**, z. B. wie zuletzt im Zusammenhang mit der Corona-Pandemie, können private Endgeräte unter Einhaltung strenger Sicherheitsvorkehrungen **vorübergehend** zu dienstlichen Zwecken genutzt werden.

Dabei ist insbesondere darauf zu achten, dass private und dienstliche Daten auf privaten Endgeräten strikt **voneinander getrennt** sind und nicht miteinander vermischt werden. Die dienstlichen Daten dürfen nicht auf privaten Endgeräten gespeichert werden, sondern sind entweder in der IT-Infrastruktur des Arbeitgebers oder verschlüsselt auf externen Datenträgern (z. B. externe Festplatten, USB-Sticks) zu sichern.

Die privaten Endgeräte sind mit einer **PIN** oder einem **Passwort** zu schützen, sodass allein der Berechtigte Zugang zu den dienstlichen Daten hat.

Da bei privaten Endgeräten in der Regel jedoch nicht das gleiche Schutzniveau wie bei dienstlichen Endgeräten besteht, dürfen private Endgeräte ausschließlich in Ausnahmesituationen zu dienstlichen Zwecken verwendet werden. Hält die Ausnahmesituation über einen längeren Zeitraum an, so sind den Mitarbeitenden dienstliche Endgeräte (z. B. dienstliche Smartphones oder dienstliche Laptops) zur Verfügung zu stellen.

Durchführung von Videokonferenzen als Instrument zur Aufgabenwahrnehmung

Die Corona-Pandemie hat sich im Jahr 2020 erheblich auf die Aufgabenwahrnehmung durch die kirchlichen und diakonischen Stellen ausgewirkt. In vielen kirchlichen und diakonischen Stellen sollte – häufig recht kurzfristig – auf neue digitale Kommunikationswege umgestellt werden. In diesem Zusammenhang erhielt der BfD EKD eine Vielzahl von Anfragen aus Kirche und Diakonie zum **datenschutzkonformen Einsatz von Videokonferenzsystemen**.

Grundsätzlich ist bei jedem Einsatz von Videokonferenzen – wie so häufig im Datenschutzrecht – vorab die Frage zu klären, ob eine Videokonferenz für die jeweilige Situation tatsächlich **erforderlich** ist oder ob beispielsweise eine Telefonkonferenz als „milderes Mittel“ ausreichend ist.

Bereits im Rahmen der **Auswahl** eines Videokonferenzsystems sind frühzeitig datenschutzrechtliche Aspekte zu berücksichtigen. So muss die verantwortliche Stelle vor der Auswahl einer Videokonferenz-Software prüfen, welches **Videokonferenzmodell** (Betriebsmodell) überhaupt in Betracht kommt.

Grundsätzlich ist der Einsatz einer **selbst entwickelten** oder einer **Open Source Software** anzustreben, die entweder auf eigenen Servern oder bei anderen deutschen oder europäischen Anbietern gehostet werden kann. Sofern keine selbst entwickelte oder Open Source Software in Betracht kommt, ist zu prüfen, ob eine Videokonferenz-Software von **deutschen oder europäischen Anbietern** eingesetzt werden kann, die ebenfalls entweder auf eigenen Servern oder bei anderen deutschen oder europäischen Anbietern gehostet wird. Sofern auch diese Alternative nicht in Betracht kommt, verbleiben zwei weitere Möglichkeiten, die jedoch ein erhöhtes Risiko für die personenbezogenen Daten der Nutzer mit sich bringen. Zum einen könnte eine Videokonferenz-Software von deutschen oder europäischen Anbietern genutzt werden, die zum Betrieb der Software zur Online-Kommunikation **Serverdienstleistungen von Anbietern aus Drittländern** einsetzen. Zum anderen ist der Einsatz von Videokonferenzdiensten direkt von **Anbietern aus Drittländern** denkbar. In beiden Fällen ist zu berücksichtigen, dass personenbezogene Daten in Drittländer übermittelt werden und daher die besonderen Vorgaben des § 10 DSG-EKD einzuhalten sind. Vor dem Hintergrund der aktuellen Entscheidung des EuGH zum Datentransfer in die USA (sog. „Schrems II“-Urteil) wird auch auf die Ausführungen in diesem Kapitel auf Seite 43 und 44 hingewiesen.

Je nach ausgewähltem Betriebsmodell muss die verantwortliche Stelle bzw. der Dienstleister auch entsprechende technische und organisatorische Maßnahmen treffen. Zu den allgemeinen **technischen und organisatorischen Maßnahmen** an ein Videokonferenzsystem gehören unter anderem:

- Zugangsschutz über ein differenziertes Rechtekonzept mit Passwortschutz
- Zulassen der einzelnen Teilnehmenden durch einen Organisator („Warteraum“ aktivieren)
- Deaktivierung der Aufzeichnungsfunktion
- regelmäßige Überprüfung im Hinblick auf aufgetretene Sicherheitslücken
- Beachtung einschlägiger Warnungen, z. B. des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Verwendung der jeweils aktuellen Programmversion

Darüber hinaus ist zu beachten, dass vor dem Einsatz neuer Technologien gemäß § 34 DSG-EKD eine **Risikobewertung** durchzuführen ist. Auch bei einem Videokonferenzsystem handelt es sich um eine solche neue Technologie, die überwiegend erst durch die Corona-Pandemie und die damit im Zusammenhang stehenden Einschränkungen in die kirchlichen und diakonischen Stellen Einzug gefunden hat. Aufgrund der Komplexität der damit verbundenen Verarbeitung von personenbezogenen Daten kann nicht ausgeschlossen werden, dass die Verarbeitung ein voraussichtlich hohes Risiko für die Rechte natürlicher Personen zur Folge hat. Dies macht eine **Datenschutz-Folgenabschätzung** erforderlich. Die Datenschutz-Folgenabschätzung muss insbesondere die in § 34 Abs. 4 DSG-EKD genannten Punkte enthalten. Entscheidend ist vor allem, in welchem Bereich die Software eingesetzt werden soll und welche Risiken für die betroffenen Personen, z. B. für Beschäftigte oder Klienten, bestehen. Eine besonders sorgfältige Prüfung ist bei der Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge vorzunehmen. Dabei ist insbesondere zu prüfen, ob der mit der Videokonferenz verfolgte Zweck nicht auch durch datenschutzfreundlichere Mittel, wie z. B. durch Telefonkonferenzen, erreicht werden kann. Für die Durchführung einer Datenschutz-Folgenabschätzung hat der BfD EKD auf seiner Website eine Handreichung veröffentlicht (https://datenschutz.ekd.de/wp-content/uploads/2020/04/Handreichung_Datenschutzfolgenabschaetzung.pdf).

Bei dem Einsatz von Videokonferenzsystemen ist zu berücksichtigen, dass dabei verschiedene personenbezogene Daten der Nutzer durch den Softwareanbieter verarbeitet werden. Es liegt ein **Auftragsverarbeitungsverhältnis** gemäß § 30 DSG-EKD zwischen der

verantwortlichen Stelle (Auftraggeber) und dem Softwareanbieter (Auftragsverarbeiter) vor, das den Abschluss eines Auftragsverarbeitungsvertrags erforderlich macht. Sofern das EKD-Datenschutzgesetz auf den Auftragsverarbeiter keine Anwendung findet, ist zusätzlich eine Zusatzvereinbarung gemäß § 30 Abs. 5 Satz 3 DSG-EKD zu unterzeichnen. Der BfD EKD hat auf seiner Website einen Mustervertrag zur Auftragsverarbeitung sowie eine Musterunterwerfungserklärung veröffentlicht (https://datenschutz.ekd.de/infothek-items/av-vertrag/).

Vor dem Hintergrund der Bedarfssituation in Kirche und Diakonie und der großen Produktdynamik hat der BfD EKD im April 2020 einen Beitrag zu den Anforderungen an Videokonferenzsysteme auf seiner Website veröffentlicht: https://datenschutz.ekd.de/2020/04/03/videokonferenzsysteme-in-kirche-und-diakonie/. Darüber hinaus berät der BfD EKD auch in Blick auf den Einsatz von konkreten Videokonferenzsystemen die örtlich Beauftragten für den Datenschutz der kirchlichen und diakonischen Stellen.

Fazit: Sofern eine verantwortliche Stelle ein Videokonferenzsystem einsetzen möchte, muss sie darauf achten, dass ein möglichst datenschutzfreundliches Betriebsmodell genutzt wird und ausreichende technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten getroffen werden. Vor dem Einsatz ist eine Datenschutz-Folgenabschätzung durchzuführen sowie ein Auftragsverarbeitungsvertrag mit dem Softwareanbieter zu schließen.

Anwendung des kirchlichen Datenschutzrechts

Zu guter Letzt: Auch in Zeiten der Corona-Pandemie hat sich immer wieder die Frage nach der Anwendung des kirchlichen Datenschutzrechts ergeben. Wer in den Anwendungsbereich des kirchlichen Datenschutzrechts fällt, ergibt sich aus § 2 Abs. 1 Satz 1 DSG-EKD. Einrichtungen der sog. verfassten Kirche und der Diakonie fallen unstreitig unter diese Regelung. Unabhängig davon ist immer noch einigen – in der Regel privatrechtlich-organisierten – Einrichtungen unklar, ob sie zur Einhaltung des EKD-Datenschutzgesetzes verpflichtet sind oder unter das staatliche Datenschutzrecht fallen.

Nach § 2 Abs. 1 Satz 3 DSG-EKD führen die **Gliedkirchen** jeweils für ihren Bereich eine **Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit**, für die das EKD-Datenschutzgesetz gilt. In diesem Zusammenhang ist es Sache der Gliedkirchen festzulegen, wer in den Anwendungsbereich des EKD-Datenschutzgesetzes fällt. Entscheidend ist hierbei, ob die jeweilige Einrichtung der Kirche zugeordnet wurde.

Demnach kann der BfD EKD Einrichtungen nur raten, sich bei Unklarheiten bezüglich der Anwendbarkeit des EKD-Datenschutzgesetzes an ihre zugehörige Gliedkirche mit der Bitte um Klärung zu wenden. Der BfD EKD erhält in regelmäßigen Abständen von den Gliedkirchen, soweit sie die Datenschutzaufsicht auf den BfD EKD übertragen haben, die genannten Übersichten, da sich hieraus auch seine Zuständigkeit ergibt. Dieser verwendet die bereitgestellten Übersichten ausschließlich für den internen Gebrauch.

Fazit: Der Anwendungsbereich des EKD-Datenschutzgesetzes wird nach § 2 Abs. 1 Satz 3 DSG-EKD durch die Gliedkirchen festgelegt. Der BfD EKD leitet hieraus seinen Zuständigkeitsbereich ab.

Datenerhebung und Auskunftsrecht

Bei der Datenerhebung und der Erfüllung von Betroffenenrechten stehen viele kirchliche und diakonische Einrichtungen vor Herausforderungen. Im Berichtszeitraum beschäftigte sich der BfD EKD daher sowohl im Rahmen von Datenschutzbeschwerden als auch im Rahmen diverser Beratungsanfragen mit diesem Themenkomplex.

Datenerhebung bei Eltern von Kita-Kindern zur Vergabe von Ganztagsplätzen

Im Berichtszeitraum hat der Vater eines Kita-Kindes beim BfD EKD Beschwerde gegen ein Verfahren zur Bedarfsermittlung von Ganztagsplätzen eingelegt. Eine Kindertageseinrichtung hatte alle Eltern, die im folgenden Jahr beabsichtigten einen Ganztagsplatz zu beantragen, aufgefordert, eine umfangreiche **Erklärung des Arbeitgebers** vorzulegen. Der Arbeitgeber sollte Angaben machen, ob die entsprechenden Eltern in Teil- oder Vollzeit arbeiten, und ob sie befristet oder unbefristet beschäftigt sind. Ebenso sollten für jeden einzelnen Wochentag (Montag bis Sonntag) die Beschäftigungszeiten ausgefüllt und gegebenenfalls Schicht- bzw. Ein-

satzpläne beigefügt werden. Außerdem wurden die Eltern aufgefordert die Wegstrecke vom Wohnsitz zum Arbeitsplatz anzugeben. Begründet wurde diese Abfrage damit, dass durch die bevorstehende Beitragsfreiheit für Kinder ab dem dritten Geburtstag eine höhere Nachfrage nach Ganztagsplätzen bestehen könnte als tatsächlich zur Verfügung stünden. Die Kinder der Eltern, die einen Bedarf nachweisen können, sollten bei der Platzvergabe bevorzugt werden.

Auf die Bitte zur Stellungnahme erläuterten die Kirchengemeinde und die Leitung der Kindertageseinrichtung, dass eine **Übermittlung der Daten an die Kommunalgemeinde** nur dann erfolgen solle, wenn die Nachfrage die Kapazitäten übersteigen würde. Als Rechtsgrundlage wurde auf § 37 Abs. 2 und Abs. 3 der Datenschutzdurchführungsverordnung der Evangelisch-lutherischen Landeskirche Hannovers Bezug genommen. Dieser besagt, dass kirchliche und kommunale Stellen personenbezogene Daten im Rahmen der Platzvergabe gemeinsam verarbeiten dürfen und dass Kindertageseinrichtungen Daten der Kinder und Eltern verarbeiten dürfen, soweit dies zur Erfüllung ihres Erziehungs-, Bildungs- und Betreuungsauftrags notwendig ist. Um den Bedarf und das Angebot abzugleichen, erfolgte die Abfrage in der gesamten Kommunalgemeinde.

Abgesehen von der Frage, ob die Eltern in Teilzeit oder Vollzeit arbeiten, war die Datenerhebung unzulässig, da sie für die Bedarfsplanung nicht erforderlich war. Die Abfrage von konkreten Arbeitszeiten und den Wegstrecken zwischen Wohnort und Arbeitsplatz widersprach überdies auch dem Grundsatz der Datenminimierung. Der BfD EKD hat demzufolge eine Beanstandung ausgesprochen. Darüber hinaus wurde die Kindertageseinrichtung aufgefordert, die Daten nicht an die Kommunalgemeinde weiterzugeben, sondern sie zu vernichten. Die Kindertageseinrichtung kam der Aufforderung zur Vernichtung der Listen nach.

Einholung eines erweiterten Führungszeugnisses bei freigestelltem Mitglied einer MAV

Ein zu 100 % freigestelltes Mitglied einer Mitarbeitervertretung (MAV) einer diakonischen Einrichtung, in der unter anderem Maßnahmen der Jugendhilfe durchgeführt werden, wandte sich an den BfD EKD und teilte mit, dass es aufgefordert worden sei, ein erweitertes Führungszeugnis vorzulegen. Dies sei mit der Regelung in **§ 72 a Abs. 1 SGB VIII** begründet worden, wonach der Arbeitgeber unter bestimmten Voraussetzungen in regelmäßigen Abständen ein erweitertes Führungszeugnis verlangen darf. Der Petent vertrat die Auffassung, dass er in seiner Funktion als Mitglied der Mitarbeitervertretung nicht in Kontakt mit Kindern und Jugendlichen komme und deshalb kein erweitertes Führungszeugnis von ihm verlangt werden könne. Da er sich weigerte, ein solches Führungszeugnis vorzulegen, wurden ihm arbeitsrechtliche Maßnahmen angedroht.

Von Mitarbeitenden in einer diakonischen Einrichtung kann gemäß § 30 a Abs. 1 Nr. 2 Bundeszentralregistergesetz (BZRG) ein erweitertes Führungszeugnis verlangt werden, wenn dieses für eine berufliche oder ehrenamtliche Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger oder für eine Tätigkeit, die in vergleichbarer Weise geeignet ist, Kontakt mit Minderjährigen aufzunehmen, benötigt wird.

Die **besondere Gefahrenlage** muss sich aus der Tätigkeit, hier aus den Aufgaben der Mitarbeitervertretung, ergeben. Zu den Aufgaben der Mitarbeitervertretung gemäß dem Mitarbeitervertretungsgesetz der EKD gehören neben der Durchführung von Sprechstunden auch Besuche vor Ort in der Einrichtung. Dabei hat ein Mitglied der Mitarbeitervertretung vornehmlich Kontakt mit Mitarbeitenden, der Personalabteilung, der Dienststellenleitung sowie weiteren Funktionsträgern.

Die bloße Möglichkeit, dass ein Mitglied der Mitarbeitervertretung im Rahmen seiner Tätigkeit Teile der Einrichtung aufsuchen kann, führt allein nicht zu einer besonderen Gefahrensituation für die der Einrichtung anvertrauten Kinder und Jugendlichen. Weder übt ein Mitglied der Mitarbeitervertretung, das zu 100 % von seiner sonstigen Tätigkeit freigestellt ist, eine in § 30 a Abs. 1 Nr. 2 BZRG genannte Tätigkeit aus, noch kommt es in vergleichbarer Weise mit Minderjährigen in Kontakt.

Ein Kontakt mit Minderjährigen „bei Gelegenheit“ eines vor Ort-Termins stellt gerade keinen bestimmungs- und arbeitsplatzgemäßen Kontakt im Rahmen der Tätigkeiten der Mitarbeitervertretung dar.

Auskunftsansprüche und Einsichtsrechte

Auch im aktuellen Berichtszeitraum hat sich der BfD EKD im Rahmen zahlreicher Beschwerden und Beratungsanfragen mit dem **datenschutzrechtlichen Auskunftsanspruch** beschäftigt. Der Auskunftsanspruch ist im EKD-Datenschutzgesetz – so wie in allen Datenschutzgesetzen – ein zentrales Betroffenenrecht. Der Anspruch ermöglicht der betroffenen Person Auskunft darüber zu verlangen, ob und welche personenbezogenen Daten eine verantwortliche Stelle über sie verarbeitet. Der betroffenen Person ist eine strukturierte Zusammenstellung ihrer personenbezogenen Daten zur Verfügung zu stellen, um sich insbesondere einen Überblick darüber verschaffen zu können, wer was zu welchem Zweck über sie verarbeitet.

Der datenschutzrechtliche Auskunftsanspruch verdrängt damit jedoch nicht **spezialgesetzliche Einsichtsrechte**. Vielmehr können der datenschutzrechtliche Auskunftsanspruch und die spezialgesetzlichen Einsichtsrechte nebeneinander oder unabhängig voneinander geltend gemacht werden. Spezialgesetzliche Einsichtsrechte verfolgen einen anderen Zweck als das datenschutzrechtliche Auskunftsrecht. Als Beispiel ist der Anspruch auf Einsicht in die Patientenakte zu nennen. Dieses Einsichtsrecht stellt eine vertragliche Pflicht aus dem zugrundeliegenden Behandlungsverhältnis dar und ermöglicht Patienten, die gesetzlich vorgeschriebene Behandlungsdokumentation der behandelnden Ärzte einzusehen. Teilweise wird angenommen, dass dieser Anspruch mittlerweile vom datenschutzrechtlichen Anspruch mit umfasst ist. Dass der Anspruch auf Einsicht in die Patientenakte unverändert im Patientenrechtegesetz normiert ist, zeigt jedoch, dass es sich um einen eigenständigen Anspruch handelt, dessen Voraussetzungen und Einschränkungen nicht auf den datenschutzrechtlichen Anspruch anwendbar sind. Bei der Einsicht in die Patientenakte handelt es sich gerade nicht um eine strukturierte Zusammenstellung. Vielmehr wird in die vollständige Patientenakte Einsicht genommen oder es werden elektronische Abschriften bzw. Kopien zur Verfügung gestellt. Die Einsicht in die Patientenakte kann aus therapeutischen Gründen abgelehnt werden, die von der jeweiligen behandelnden Person darzulegen sind. Damit erfährt der datenschutzrechtliche Auskunftsanspruch jedoch keine – gegen das kirchliche Datenschutzrecht verstoßende – Einschränkung, da es sich um zwei eigenständige Ansprüche handelt. Gleichwohl können Regelungen aus den Datenschutzgesetzen nicht auf den Anspruch auf Einsicht in die Patientenakte übertragen werden, da es sich bei Patientenakten und deren Kopien in der Regel um umfangreichere Dokumente handelt. Ähnlich verhält es sich mit dem datenschutzrechtlichen Auskunftsanspruch im Hinblick auf spezialgesetzliche Einsichtsrechte im Beschäftigungsverhältnis oder in einem gerichtlichen Verfahren.

Fazit: Einsichtsrechte müssen immer konkret geltend gemacht werden und sind nicht vom datenschutzrechtlichen Auskunftsanspruch umfasst.

Auskunftsanspruch von Beschäftigten

Im Berichtszeitraum haben den BfD EKD vermehrt Anfragen zum Auskunftsersuchen von Beschäftigten gemäß § 19 DSG-EKD erreicht. In diesem Zusammenhang mussten folgende Fragen geklärt werden:

- Wie kann die verantwortliche Stelle auf ein allgemeines Auskunftsersuchen eines Beschäftigten reagieren?
- In welchem Umfang muss eine verantwortliche Stelle bei einem solchen Ersuchen Auskunft erteilen?

Sinn und Zweck einer Auskunft gemäß § 19 DSG-EKD ist es, dass die antragstellende Person aus der Antwort der verantwortlichen Stelle erkennen kann, welche personenbezogenen Daten die verantwortliche Stelle zum Zeitpunkt der Antragstellung über die antragstellende Person speichert.

Der Auskunftsanspruch bezieht sich auf die konkret zur betroffenen Person gespeicherten personenbezogenen Daten, also konkreter Name, Geburtsdatum, Adresse etc. Die Auskunft muss über die in §§ 16 ff. DSG-EKD geregelten Informationspflichten hinausgehen. Die Kategorien der personenbezogenen Daten ergeben sich zumeist aus den im Verzeichnis von Verarbeitungstätigkeiten aufgenommenen Kategorien.

Bei der Geltendmachung eines **allgemeinen Auskunftsanspruchs von einem langjährigen Mitarbeitenden,** der nicht beschränkt auf einzelne Datenkategorien gestellt wird, ist vertretbar, dass die verantwortliche Stelle ein **gestuftes Verfahren** wählt. Bei einem langjährigen Beschäftigtenverhältnis ist davon auszugehen,

dass es sich um eine große Menge personenbezogener Daten handelt. Bei der Verarbeitung großer Mengen personenbezogener Daten kann die verantwortliche Stelle verlangen, dass die antragstellende Person ihren Auskunftsanspruch auf Grundlage einer strukturierten Zusammenfassung (erste Stufe) genauer konkretisiert (zweite Stufe).

In einer **ersten Stufe** kann dem Antragstellenden durch die Zurverfügungstellung einer strukturierten Zusammenfassung die Möglichkeit eröffnet werden, sich einen Überblick darüber zu verschaffen, welche personenbezogenen Daten der Arbeitgeber über ihn oder sie speichert. Welche Vorgehensweise hierbei geeignet ist, hängt vom jeweiligen Einzelfall ab. So kann auch die Bereitstellung des Profils oder der Verweis des Mitarbeitenden auf den Abruf seiner personenbezogenen Daten in einem Personalinformationssystem im Rahmen des § 19 Abs. 1 DSG-EKD als zumutbar erachtet werden. Bei der Nutzung eines Dokumentenmanagementsystems kann auch eine Liste der gespeicherten Dokumente bzw. Aktenzeichen in einem ersten Schritt ausreichend sein. Selbstverständlich sind lediglich die Datenkategorien zu nennen, in denen auch personenbezogene Daten der betroffenen Person gespeichert werden. Eine abstrakte Darstellung aller Datenkategorien reicht aber nicht aus.

In einer **zweiten Stufe** kann der Antragstellende dann eine weitergehende Auskunft verlangen. Es kann sich hierbei beispielsweise um Präzisierungen bei bestimmten Verarbeitungszwecken, Zeiträumen bzw. Datenkategorien handeln.

Die verantwortliche Stelle muss auch prüfen, ob sie im Fall von § 19 Abs. 2 DSG-EKD die Auskunft verweigern muss oder die Auskunft wegen eines **unverhältnismäßigen Aufwands** nach § 19 Abs. 4 DSG-EKD verweigern darf. Bei der Auskunftsverweigerung wegen eines unverhältnismäßigen Aufwands muss eine Interessenabwägung zwischen dem Informationsinteresse der betroffenen Person und dem Interesse der verantwortlichen Stelle vorgenommen werden. Beim Interesse der verantwortlichen Stelle ist der durch die konkrete Benachrichtigung entstehende Aufwand zu berücksichtigen. Wird die verantwortliche Stelle auf einen Antrag hin nicht tätig, muss sie die auskunftsersuchende Person gemäß § 16 Abs. 4 DSG-EKD über die Gründe unterrichten.

Besondere Datenschutzthemen im gemeindlichen Alltag

Kirchengemeinden sind als eigenständige verantwortliche Stellen verpflichtet, die Regelungen des Datenschutzrechts einzuhalten. Insbesondere in der praktischen Arbeit einer Kirchengemeinde ergeben sich immer wieder spezielle Datenschutzfragen.

Einladung zur Jubiläumskonfirmation

Immer wieder erreichen den BfD EKD Beschwerden und Anfragen zum Datenschutz bei Einladungen zu sog. Jubelkonfirmationen. So erhielt in einem Fall ein Petent eine Einladung zur Diamantenen Konfirmation, obwohl er seit Jahrzehnten **kein Kirchenmitglied** mehr ist. Eine Erlaubnis zur Nutzung seiner Daten hatte er nicht erteilt. Auf einen Brief, den er an den Pastor der Kirchengemeinde schrieb, bekam er keine Antwort. In dem Brief widersprach der Petent ausdrücklich der Nutzung seiner Daten. Zunächst wandte sich der Petent an die staatlichen Datenschutzaufsichtsbehörden, erst an die Landes- dann an die Bundesbehörde. Von beiden Aufsichtsbehörden wurde er an den BfD EKD verwiesen. Im Rahmen seiner Stellungnahme teilte der Pastor der Kirchengemeinde mit, dass ein Mitkonfirmand eine Adressliste über diesen Jahrgang führe und bereits zu vorherigen Ereignissen eingeladen habe. Daraus wurde fälschlicherweise eine Zustimmung abgeleitet. Für gewöhnlich würden nur Personen angeschrieben, die sich zuvor im Gemeindebüro gemeldet oder anderweitig eine Erlaubnis erteilt hätten. Auch seien die Daten des Petenten auf seinen Brief hin umgehend gelöscht worden. Lediglich die Mitteilung an ihn hierüber sei unterblieben.

Es wird grundsätzlich empfohlen, ein Konfirmationsjubiläum im Gemeindebrief anzukündigen und die Gemeindeglieder zu bitten, ehemalige Konfirmanden in ihrem Umfeld darauf hinzuweisen, dass diese sich im Gemeindebüro melden sollen. Grundsätzlich gilt, dass Gemeindeglieder aus anderen Kirchengemeinden oder Nicht-Kirchenmitglieder ohne eine entsprechende Einwilligung nicht angeschrieben werden dürfen.

Der Kirchengemeinde wurde dieses Verfahren, das eigentlich wohl auch eingehalten wird, nochmal aufgezeigt und dringend angeraten, hiervon keine Ausnahmen zu machen.

Videoaufnahmen von Gottesdiensten

Viele Kirchengemeinden fertigen Videos von ihren Gottesdiensten an und veröffentlichen diese, um einem größeren Personenkreis die Teilnahme an den Gottesdiensten zu ermöglichen. Dabei werden in der Regel allein der Pfarrer bzw. die Pfarrerin sowie weitere mitwirkende Personen gefilmt. Die Gottesdienstbesucher sind auf den Videos grundsätzlich nicht zu sehen.

Die **Anfertigung und Veröffentlichung** von Gottesdienstvideos, auf denen auch die Gottesdienstbesucher zu sehen sind, sind Gegenstand eines Beschwerdeverfahrens gewesen. Bei der betroffenen Person handelte es sich um ein Kind, das gemeinsam mit seiner Kindergartengruppe den Gemeindegottesdienst besucht hat. Das Kind wurde während des Gottesdienstes gefilmt und das Video auf der Plattform „YouTube“ veröffentlicht. Die Eltern des Kindes haben weder in die Anfertigung noch in die Veröffentlichung des Videos eingewilligt.

Bevor Gottesdienste gefilmt werden, muss die Kirchengemeinde prüfen, ob es sowohl für die Anfertigung als auch für die Veröffentlichung des Videos eine Rechtsgrundlage gibt.

Bei der Aufzeichnung oder Übertragung von Gottesdiensten ist **§ 53 DSG-EKD** zu beachten. Eine Aufzeichnung oder Übertragung von Gottesdiensten ist gemäß § 53 DSG-EKD zulässig, wenn die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden. Dies kann durch entsprechende Hinweisschilder im Eingangsbereich erfolgen.

Sofern die Gottesdienstbesucher ebenfalls auf dem Video zu sehen und zu erkennen sind, ist neben § 53 DSG-EKD noch eine weitere Rechtsgrundlage für die Anfertigung und Veröffentlichung des Videos erforderlich. Werden Videos von Gottesdiensten angefertigt, auf denen die **Gottesdienstbesucher zu erkennen** sind, kommt als Rechtsgrundlage entweder **§ 6 Nr. 4 in Verbindung mit § 6 Nr. 8 DSG-EKD** oder eine **Einwilligung** der betroffenen Personen in Betracht. Gemäß § 6 Nr. 4 in Verbindung mit § 6 Nr. 8 DSG-EKD muss die verantwortliche Stelle ein berechtigtes Interesse an der **Anfertigung** des Videos haben und es dürfen keine schutzwürdigen Interessen der betroffenen Person überwiegen. Ist die betroffene Person minderjährig, so sind ihre Interessen gemäß § 6 Nr. 8 DSG-EKD besonders schutzwürdig. Mit der Anfertigung von Gottesdienstvideos wird der Zweck verfolgt, einem erweiterten Personenkreis die Teilnahme am Gottesdienst zu ermöglichen. Dazu ist es jedoch nicht erforderlich, die Gottesdienstbesucher ebenfalls zu filmen. Somit wird die Interessenabwägung in der Regel zu dem Ergebnis führen, dass die schutzwürdigen Interessen der betroffenen Person das berechtigte Interesse der verantwortlichen Stelle überwiegen. Gottesdienstvideos, auf denen die Gottesdienstbesucher zu sehen sind, dürfen dann nur mit Einwilligung der betroffenen Person angefertigt werden.

Bei der **Veröffentlichung** der Videos ist neben dem EKD-Datenschutzgesetz auch das **Kunsturhebergesetz** (KunstUrhG) zu berücksichtigen. Gemäß § 22 KunstUrhG ist bei einer Veröffentlichung von Bildnissen, wozu auch Videos gehören, grundsätzlich eine Einwilligung der betroffenen Person einzuholen.

Fazit: Möchte eine Kirchengemeinde Videos von Gottesdiensten anfertigen und diese veröffentlichen, sollte darauf geachtet werden, dass die Gottesdienstbesucher auf den Videos nicht zu erkennen sind. In Fällen, in denen die Gottesdienstbesucher auf dem Video zu sehen sind, muss die verantwortliche Stelle prüfen, ob für die Anfertigung und die Veröffentlichung des Videos eine Rechtsgrundlage gegeben ist oder eine Einwilligung der betroffenen Person erforderlich ist. In dem beschriebenen Beschwerdeverfahren lag weder eine Rechtsgrundlage noch eine Einwilligung der Petenten vor. Der BfD EKD hat daher eine Beanstandung ausgesprochen und die Kirchengemeinde aufgefordert, das Kind der Petenten auf dem Video unkenntlich zu machen.

Veröffentlichung von Kirchenaustritten im Gemeindebrief

Im Berichtszeitraum erreichten den BfD EKD mehrere Datenschutzbeschwerden, die die Veröffentlichung von Kirchenaustritten sowohl in der Print- als auch in der Onlineausgabe des Gemeindebriefes betrafen. Die aus der Kirche ausgetretenen Personen wurden mit Name, Adresse und Geburtsdatum im Gemeindebrief, der auch auf der Website der Kirchengemeinde für jedermann zugänglich veröffentlicht wurde, genannt.

Der Gemeindebrief dient der **Information der Gemeindeglieder** über das gemeindliche Leben. Um den Infor-

mationszweck erfüllen zu können, ist es zulässig, personenbezogene Daten in einem begrenzten Rahmen zu veröffentlichen. Dabei sind die Bestimmungen des EKD-Datenschutzgesetzes sowie ggf. geltende landeskirchliche Vorschriften zu beachten. Grundsätzlich ist die **Veröffentlichung von Amtshandlungen** im Gemeindebrief zulässig. Dies ergibt sich auch aus den meisten landeskirchlichen Vorschriften. Amtshandlungen sind Taufen, Konfirmationen, Trauungen und Beerdigungen. Kirchenaustritte gehören nicht dazu.

In einem Beschwerdeverfahren war die Veröffentlichung, d.h. die Offenlegung von Kirchenaustritten im Gemeindebrief **ausdrücklich durch eine landeskirchliche Vorschrift verboten.** Gemäß dieser landeskirchlichen Vorschrift dürfen Kirchenaustritte weder im Rahmen von gottesdienstlichen Veranstaltungen noch in Publikationsorganen einer Kirchengemeinde veröffentlicht werden. Im Rahmen dieses Beschwerdeverfahrens hat der BfD EKD gegenüber der Kirchengemeinde eine Beanstandung ausgesprochen. Darüber hinaus wurde die Kirchengemeinde aufgefordert, die personenbezogenen Daten der betroffenen Personen aus der Onlineausgabe des Gemeindebriefes zu entfernen und zukünftig keine Kirchenaustritte im Gemeindebrief zu veröffentlichen.

In Fällen, in denen **keine landeskirchliche Vorschrift die Veröffentlichung von Kirchenaustritten regelt,** ist auf die Bestimmungen des EKD-Datenschutzgesetzes zurückzugreifen. Als Rechtsgrundlage für die Offenlegung von personenbezogenen Daten ausgetretener Gemeindeglieder kommt allein § 9 Abs. 1 Nr. 3 DSG-EKD in Betracht. Voraussetzung ist ein berechtigtes Interesse der datenempfangenden Stellen oder Personen an der Kenntnis der offenzulegenden Daten. Es dürfen keine schutzwürdigen Interessen der betroffenen Person an dem Ausschluss der Offenlegung entgegenstehen. Im Rahmen der Interessenabwägung ist zu berücksichtigen, dass die Gemeindeglieder ein Interesse daran haben zu wissen, wer Mitglied der Gemeinde ist und wer ausgetreten ist. Das Interesse der ausgetretenen Gemeindeglieder an der Nichtveröffentlichung ihrer personenbezogenen Daten wiegt jedoch im Allgemeinen höher als das Interesse der übrigen Gemeindeglieder an der Veröffentlichung der Kirchenaustritte. Dies gilt sowohl für die Print- als auch für die Onlineausgabe des Gemeindebriefes. Bei der Veröffentlichung im Internet ist zusätzlich zu beachten, dass ein unbestimmter Personenkreis und nicht lediglich die Gemeindeglieder auf den Gemeindebrief zugreifen können. Die Gefahr des Missbrauchs ist daher deutlich höher als bei der Printausgabe des Gemeindebriefes.

Bei allen weiteren Datenschutzfragen rund um den Gemeindebrief wird auf die Handreichung auf der Website des BfD EKD hingewiesen (https://datenschutz.ekd.de/infothek-items/datenschutz-im-gemeindebrief/).

Fazit: Sofern landeskirchliche Vorschriften keine spezielle Rechtsgrundlage vorsehen, ist die Offenlegung von Kirchenaustritten mangels einer Rechtsgrundlage im EKD-Datenschutzgesetz weder in der Print- noch in der Onlineausgabe des Gemeindebriefes zulässig.

Datenübermittlung in Drittländer und Auftragsverarbeitung

Im Rahmen der Auftragsverarbeitung, die als datenschutzrechtliches Instrument nicht mehr aus der täglichen Arbeitswelt wegzudenken ist, werden in vielen Fällen personenbezogene Daten an und in Drittländer übermittelt. Obwohl sich der BfD EKD bereits in der Vergangenheit intensiv mit beiden Themenbereichen beschäftigt hat, ergeben sich aufgrund des EuGH-Urteils „Schrems II“ viele neue Fragen und Probleme.

Datenübermittlung in die USA

Bei einer Vielzahl von Datenverarbeitungsvorgängen werden personenbezogene Daten in sogenannte Drittländer und insbesondere in die USA übermittelt. Drittländer sind gemäß § 4 Nr. 18 DSG-EKD Staaten, in denen die DSGVO keine Anwendung findet. Zum Schutz der personenbezogenen Daten werden an Datenübermittlungen in Drittländer besonders hohe Anforderungen gestellt. Gemäß **§ 10 Abs. 1 DSG-EKD** sind Datenübermittlungen in Drittländer lediglich dann zulässig, wenn die EU-Kommission entweder ein angemessenes Datenschutzniveau in dem jeweiligen Drittland festgestellt hat oder Standarddatenschutzklauseln verwendet werden, die von der EU-Kommission erlassen oder genehmigt worden sind. Sofern keine dieser Alternativen vorliegt, ist eine Datenübermittlung nur auf der Grundlage von **§ 10 Abs. 2 Nr. 1 bis 6 DSG-EKD** möglich. Ist keine Rechtsgrundlage gegeben, ist die Datenübermittlung in das jeweilige Drittland unzulässig.

Besondere Aufmerksamkeit hat im vergangenen Jahr das **EuGH-Urteil „Schrems II“** vom 16. Juli 2020 erlangt. Dieses betrifft die Übermittlung von personenbezogenen Daten in Drittländer, primär in die USA.

Der EuGH hat in dem Urteil das sog. **EU-US Privacy Shield,** das bis zu diesem Zeitpunkt als Rechtsgrundlage für die Datenübermittlung in die USA gemäß § 10 Abs. 1 Nr. 1 DSG-EKD herangezogen werden konnte, für ungültig erklärt. Eine Übergangsfrist wurde seitens des EuGH nicht vorgesehen. Dies hatte zur Folge, dass für sämtliche Datenübermittlungen in die USA, die bislang auf das EU-US Privacy Shield gestützt wurden, die Rechtsgrundlage für die Datenübermittlung entfallen ist. Da es gegenwärtig keinen anderen Angemessenheitsbeschluss der EU-Kommission bezüglich der Datenübermittlung in die USA gibt, kann § 10 Abs. 1 Nr. 1 DSG-EKD gegenwärtig nicht als Rechtsgrundlage herangezogen werden.

In dem Urteil beschäftigt sich der EuGH weiterhin mit den **Standarddatenschutzklauseln**, die gemäß § 10 Abs. 1 Nr. 2 DSG-EKD ebenfalls als Rechtsgrundlage für Datenübermittlungen in die USA herangezogen werden können. Der EuGH stellt in dem Urteil fest, dass die bestehenden Standarddatenschutzklauseln nach § 10 Abs. 1 Nr. 2 DSG-EKD grundsätzlich gültig bleiben. Allerdings trage die verantwortliche Stelle die Verantwortung dafür, dass die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der EU genießen. Dies können die verantwortlichen Stellen jedoch nicht gewährleisten. Nach den Feststellungen des EuGH ist in den USA kein gleichwertiges Schutzniveau gegeben. Auch führen verschiedene US-Sicherheitsgesetze wie z. B. der Cloud Act dazu, dass die in den Standarddatenschutzklauseln festgelegten Garantien von den US-amerikanischen Unternehmen nicht eingehalten werden können. Dies wirkt sich dahingehend aus, dass auch die bestehenden Standarddatenschutzklauseln aktuell nicht als Rechtsgrundlage für die Übermittlungen von personenbezogenen Daten in die USA herangezogen werden können. Es ist erforderlich, dass in den Standarddatenschutzklauseln weitere Garantien vorgesehen werden, mit denen ein gleichwertiges Schutzniveau hergestellt wird.

Zwischenzeitlich hat der Europäische Datenschutzausschuss (EDSA) **Maßnahmen** vorgestellt, mit denen Datenübermittlungen in Drittstaaten abgesichert werden können. Dazu hat er entsprechende Empfehlungen herausgegeben. Dabei handelt sich um die Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en) und um die Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen (https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en). Darüber hinaus hat die Europäische Kommission bereits einen Entwurf für angepasste Standarddatenschutzklauseln auf Grundlage von Art. 46 DSGVO erarbeitet. Es ist zu erwarten, dass die Europäische Kommission nach Abschluss des derzeit laufenden Stellungnahmeverfahrens neue Standarddatenschutzklauseln veröffentlichen wird.

Da es gegenwärtig jedoch keinen Angemessenheitsbeschluss der Europäischen Kommission für die Datenübermittlung in die USA gibt und die Datenübermittlung in die USA auch nicht auf die bestehenden Standarddatenschutzklauseln gestützt werden kann, kommt als Rechtsgrundlage allein § 10 Abs. 2 DSG-EKD in Betracht. Bei der Prüfung des § 10 Abs. 2 DSG-EKD ist zu beachten, dass die in den Nrn. 1 bis 6 genannten Voraussetzungen restriktiv auszulegen sind. An deren Vorliegen werden hohe Anforderungen gestellt.

Fazit: Hat eine kirchliche Stelle die Übermittlung von personenbezogenen Daten in die USA bisher auf das nun unwirksame EU-US Privacy Shield oder auf Standarddatenschutzklauseln gestützt, so muss die Stelle nun prüfen, ob die Datenübermittlung auf der Grundlage von § 10 Abs. 2 Nr. 1 bis 6 DSG-EKD zulässig ist. Sofern die Voraussetzungen von § 10 Abs. 2 Nr. 1 bis 6 DSG-EKD nicht vorliegen, ist die Datenübermittlung in die USA auszusetzen.

Nutzung von Speicherplattformen

Von Leitungsorganen einer Kirchengemeinde wird häufig der Wunsch an den BfD EKD herangetragen, die Speicherung von Dokumenten – etwa von Protokollen – auf leicht zu erreichenden Plattformen wie z. B. Google Drive, OneDrive, iCloud und Dropbox zu speichern. Das Anliegen weist auf ein grundsätzliches Problem hin.

Entweder gibt es in vielen Landeskirchen (noch) kein Angebot für eine gemeinsame **sichere Dateiablage zwischen Mitarbeitenden und Ehrenamtlichen** oder dieses Angebot ist (noch) nicht ausreichend bekannt.

Liegt der Speicherort der verwendeten Speicherplattform außerhalb der EU-Mitgliedsstaaten, ist zu prüfen, ob gemäß § 10 DSG-EKD die Voraussetzungen für eine Übermittlung von personenbezogenen Daten in Drittländer vorliegt. Sofern **personenbezogene Daten in die USA** übermittelt werden sollen, ist zu beachten, dass gemäß dem EuGH-Urteil „Schrems II" die Datenübermittlung gegenwärtig weder auf einen Angemessenheitsbeschluss noch auf bestehende Standarddatenschutzklauseln gestützt werden kann. Eine Datenübermittlung in die USA ist nur zulässig, wenn eine Rechtsgrundlage aus § 10 Abs. 2 Nr. 1 bis 6 DSG-EKD im konkreten Fall gegeben ist.

Weiterhin ist zu beachten, dass bei der Nutzung von Speicherplattformen eine **Auftragsverarbeitung** vorliegt. Die verantwortliche Stelle muss daher mit dem Betreiber der jeweiligen Speicherplattform einen Auftragsverarbeitungsvertrag sowie eine Zusatzvereinbarung gemäß § 30 Abs. 5 Satz 3 DSG-EKD abschließen. Ein Muster für die Zusatzvereinbarung ist auf der Internetseite des BfD EKD veröffentlicht (https://datenschutz.ekd.de/infothek-items/av-vertrag/).

Beim konkreten Anliegen wird häufig vollkommen unterschätzt und vernachlässigt, welche **Folgen die Nutzung** von zumeist kostenlosen Plattformen, wie beispielsweise Google Drive, hat. Häufig werden die Daten für eigene Geschäftszwecke ausgewertet. Ein Kennwortschutz bietet keinen ausreichenden Schutz vor der Analyse der gespeicherten Daten. Zusätzliche Schutzmaßnahmen zur Verhinderung eines unbefugten Zugriffs über eine Zwei-Faktor-Authentifizierung bieten nur einen verbesserten Schutz gegenüber Dritten. Durch eine Inhaltsverschlüsselung kann zwar eine Auswertung der Inhalte vermieden werden, nicht jedoch die Auswertung der zusätzlich zu den Inhaltsdaten erhobenen Metadaten (Anmerkung: Metadaten sind „Daten über Daten"), die in der Regel auch personenbezogene Daten sind.

Darüber hinaus müssen bei einer Nutzung von Speicherplattformen auch die allgemeinen Nutzungsbedingungen des jeweiligen Anbieters geprüft werden. In vielen Fällen widersprechen die **allgemeinen Nutzungsbedingungen** den Anforderungen des EKD-Datenschutzgesetzes. So beispielsweise auch die allgemeinen Nutzungsbedingungen von Google, die auch Google Drive betreffen. Zu den wichtigsten Punkten gehört die Erlaubnis zur Analyse der Dateninhalte. Es werden also nicht nur die Metadaten, sondern auch die übertragenen Inhalte sämtlicher Nutzenden ausgewertet. Der Zweck dient dem Verkauf von Werbeanzeigen und dem Zuschneiden der eigenen angebotenen Dienste. Es kommt somit zu einer umfassenden Profilbildung sämtlicher Nutzenden. Die Daten der Nutzenden werden weltweit gespeichert. Eine Kontrolle der Nutzenden über den Speicherort gibt es nicht. Die Daten werden an Geschäftspartner von Google weitergegeben. Das Recht auf Löschung ist beschränkt. Die im eigenen Konto gespeicherten Daten werden nicht gelöscht, wenn diese Daten anderen Unternehmen zur Verfügung gestellt wurden oder mit anderen Nutzenden geteilt wurden. Einen Anspruch auf die ständige Verfügbarkeit von Daten mit Google Drive wird von Google nicht gegeben.

Fazit: Vor der Nutzung von Plattformen zur Speicherung von personenbezogenen Daten muss die verantwortliche Stelle prüfen, ob eine datenschutzkonforme Nutzung möglich und vertretbar ist.

Nutzung von Microsoft 365 und Microsoft Cloud-Diensten

Microsoft 365 (früher Microsoft Office 365) ist eine sehr weit verbreitete Anwendung für typische Büroaufgaben. Auch in kirchlichen und diakonischen Einrichtungen ist Microsoft 365 im Einsatz. Der datenschutzfreundliche Einsatz von Microsoft 365 stellt im Hinblick auf die Nutzung von Microsoft Cloud-Diensten eine Herausforderung dar.

Bei der Nutzung von Microsoft 365 und Microsoft Cloud-Diensten werden in der Regel personenbezogene Daten in die USA, wo Microsoft seinen Hauptstandort hat, übermittelt. Die **Datenübermittlung in die USA** ist aufgrund des EuGH-Urteils „Schrems II" gegenwärtig lediglich auf der Grundlage von § 10 Abs. 2 Nr. 1 bis 6 DSG-EKD zulässig. Das EU-US Privacy Shield hat der EuGH in seinem Urteil für ungültig erklärt. Zugleich hat der EuGH festgestellt, dass auch die bestehenden Standarddatenschutzklauseln keinen ausreichenden Schutz für die personenbezogenen Daten der EU-Bürger bieten und daher ohne

weitere technische und organisatorische Maßnahmen nicht als Rechtsgrundlage herangezogen werden können.

Dessen ungeachtet sind bei einer Nutzung von Microsoft 365 und Microsoft Cloud-Diensten weitere Aspekte zu beachten. So verabschiedete die Konferenz der Beauftragten für den Datenschutz in der Evangelischen Kirche in Deutschland im Jahr 2019 eine **Entschließung zur Nutzung von Microsoft Cloud-Diensten**. Darin werden drei Voraussetzungen genannt, unter denen eine Nutzung entsprechender Cloud-Angebote datenschutzkonform möglich ist.

1. Es wird von Microsoft eine wirksame Zusatzerklärung nach § 30 Abs. 5 DSG-EKD angeboten.
2. Eine Verschlüsselung der Daten ohne Zugriff von Microsoft muss möglich sein (HYOK = Hold your own key).
3. Die Übermittlung von Telemetriedaten kann verhindert werden.

Zur praktischen Umsetzung dieser Entschließung erreichten den BfD EKD vermehrt Nachfragen, auf die im Folgenden eingegangen wird.

Zu 1.
Wird Microsoft 365 mit einem Cloudspeicher genutzt und dadurch personenbezogene Daten auf Servern außerhalb der kirchlichen und diakonischen Stellen verarbeitet, liegt ein Fall der Auftragsverarbeitung vor. Deshalb muss ein entsprechender Vertrag mit Microsoft geschlossen werden. Die Online Services Terms mit ihren Anlagen (OST) von Microsoft können nach § 30 Abs. 5 Satz 2 DSG-EKD als Vertrag zur Auftragsverarbeitung genutzt werden, sofern sich die Vertragsinhalte an Art. 28 DSGVO orientieren. Zusätzlich muss dann aber eine **Zusatzvereinbarung** nach § 30 Abs. 5 Satz 3 DSG-EKD abgeschlossen werden. Im Jahr 2019 wurden umfangreiche Verhandlungen mit Microsoft zur Ausformulierung dieser Zusatzvereinbarung geführt. Inzwischen haben mehrere Landeskirchen entsprechende Verträge abgeschlossen. Der BfD EKD hat ein Muster dieser Zusatzvereinbarung sowie weitere Hinweise zur Cloudnutzung auf seiner Internetseite zur Verfügung gestellt (https://datenschutz.ekd.de/2020/03/06/empfehlungen-und-hinweise-zur-nutzung-von-microsoft-office-cloud-diensten/).

Zu 2.
Eine **Verschlüsselung der Daten** muss unabhängig vom Zugriff durch Microsoft möglich sein. Dabei muss eine Ende-zu-Ende-Verschlüsselung aller in die Cloud übermittelten personenbezogenen Daten erfolgen, sodass der Zugriff von Unbefugten verhindert wird. Microsoft selbst bietet seit kurzem zwar den zusätzlichen Einsatz von Kundenschlüsseln an (BYOK = Bring your own key). Dabei erhält Microsoft aber den Schlüssel der Kunden und hat damit die Möglichkeit – ohne Wissen und Erlaubnis der Dateneigner – auf die Daten zuzugreifen. Diese, von Microsoft angebotene Technik, reicht daher als Schutzmaßnahme nicht aus. Für eine echte Ende-zu-Ende-Verschlüsselung gibt es verschiedene Möglichkeiten. Zum einen können besonders schützenswerte Daten in Einzeldateien verschlüsselt und erst in verschlüsselter Form in der Cloud abgelegt werden. Zum anderen gibt es auch IT-Anbieter, die eigene Verschlüsselungsmechanismen für den Cloudspeicher von Microsoft 365 entwickelt haben.

Zu 3.
Die **Übermittlung von Telemetriedaten** an Microsoft sollte unterbunden werden. Problematisch ist vor allem, dass Microsoft im Hinblick auf die Telemetriedaten nicht offen und transparent arbeitet. Es werden Diagnose- und Metadaten über die Nutzung und Leistung von Anwendungen und Anwendungskomponenten an Microsoft übermittelt, um die Software sicherer zu machen oder Fehler zu finden. Viele dieser Telemetriedaten sind personenbezogen oder personenbeziehbar im Sinne des EKD-Datenschutzgesetzes. Dazu gehören z. B. der Autor eines Dokumentes, die Namensangaben in Dateinamen sowie ganze Textinhalte bei der Nutzung von Online-Zusatzfunktionen (z. B. Übersetzungsdiensten). Bis vor kurzem bot Microsoft keine umfassende Dokumentation, keine Einstellungsmöglichkeiten und kein Datenanzeigetool für einen genauen Überblick über die mittels Telemetrie gesammelten Daten an. Das hat sich teilweise durch die Implementierung und Veröffentlichung des sogenannten „Microsoft Diagnostic Data Viewers“ im Jahr 2018 geändert. In diesem Tool können die Office-Nutzer nachvollziehen, welche Daten bei der Office-Nutzung unter welchen Datenschutzeinstellungen erfasst werden. Zusätzlich müssen bei der Verwendung des Betriebssystems Windows 10 spezielle Einstellungen zur Datensicherheit vorgenommen werden. Das Telemetrie-Level „Security“ ist zu aktivieren. Eine komplette

Abschaltung von Telemetriedaten ist nur in der Enterprise-Variante von Windows 10 ab Version 1909 möglich. Es sollte eine Version ab Microsoft 365 Enterprise E2 Lizenz eingesetzt werden. Erst ab dieser Version wurden die entsprechenden Einstellungsmöglichkeiten zur datenschutzkonformen Nutzung in Microsoft 365 implementiert. Unter den Optionen findet man das Trust Center und darunter die „Datenschutzoptionen“. Hier sollte die Datenübermittlung an Microsoft und die Nutzung von Online-Diensten abgeschaltet werden. Bei jedem Programmupdate werden von Microsoft zahlreiche Änderungen durchgeführt. Deshalb sollte bei jedem Update geprüft werden, ob dieses auch ungewollte Änderungen bei den Datenschutzeinstellungen zur Folge hatte.

Im Sinne des Datenschutzrechts muss die Übermittlung personenbezogener Daten an Microsoft durch Verschlüsselung (zu 2.) und Abschalten der Telemetriedaten (zu 3.) verhindert werden. Zu berücksichtigen ist, dass in diesen beiden Fällen nicht alle Funktionen der Software nutzbar sein könnten.

Abschließend ist darauf hinzuweisen, dass Microsoft 365 unterschiedlich genutzt werden kann – als Webversion (Arbeiten online über einen Browser als **Cloudvariante**), als Mobile App (Arbeiten mit mobilen Geräten als Cloudvariante) oder Desktop (Installation auf PC/Notebook als On-Premise-Lösung oder Cloudvariante möglich). Nur ausgewählte Desktop-Varianten mit lokal auf den Geräten installierten Programmen (sog. **On-Premise-Lösung**) sind datenschutzkonform konfigurierbar. Die lokal eingesetzten Desktop-Varianten sind ohne Nutzung einer Cloud möglich. In allen anderen Fällen kann ein Abfluss von Daten an Microsoft nicht komplett verhindert werden.

Allgemein gilt für alle Cloud-Dienste, dass vor dem Einsatz stets eine **Datenschutz-Folgenabschätzung** durchzuführen ist. Dabei muss insbesondere das Risiko für die Verarbeitung personenbezogener Daten in Drittländern bewertet und ggf. zusätzliche Maßnahmen zur Risikominimierung geplant werden.

Digitale Kommunikation und Videoüberwachung

Der Themenkomplex digitale Kommunikation – insbesondere in Videokonferenzen und mit Messenger-Diensten – und Videoüberwachung beschäftigte den BfD EKD im Berichtszeitraum sowohl im Rahmen von Datenschutzbeschwerden als auch im Rahmen von zahlreichen Beratungsanfragen.

Durchführen eines Klientengesprächs in einer Videokonferenz

Seit Beginn der Corona-Pandemie werden auch **im diakonischen Alltag** vermehrt Videokonferenzsysteme eingesetzt. Grundsätzlich ist bei jedem Einsatz von Videokonferenzsystemen vorab zu prüfen, ob eine Videokonferenz für die jeweilige Situation **erforderlich** ist oder ob eine Telefonkonferenz als „milderes Mittel“ den gleichen Erfolg bringt.

Sollen Videokonferenzsysteme eingesetzt werden, ist zunächst zu unterscheiden, in welchem Bereich sie eingesetzt und welche personenbezogenen Daten verarbeitet werden sollen. Soweit es um **dienstlich-interne Kommunikation** – beispielsweise Teambesprechungen – geht, sind die Voraussetzungen zu prüfen, die auch für andere kirchliche Einrichtungen gelten. Dabei muss strikt auf die **Nennung von Patienten- und Klientendaten verzichtet** werden. Um eine Nutzung der Daten durch kommerzielle Anbieter auszuschließen, ist bestenfalls auf selbst entwickelte Applikationen, die auf eigenen Servern laufen oder auf Open-Source-Software zurückzugreifen. Soweit externe Hoster genutzt werden, sollen diese in einem Mitgliedsstaat der Europäischen Union – bestenfalls in Deutschland – ansässig sein und die entsprechenden Verträge zur Auftragsverarbeitung geschlossen werden. Bei Anbietern aus Drittländern sind die Voraussetzungen hinsichtlich der Datenübermittlung in Drittländer gemäß § 10 DSG-EKD zu berücksichtigen.

Darüber hinaus kam in den diakonischen Einrichtungen die Frage auf, ob Videokonferenzsysteme auch in der **Arbeit mit Klienten** eingesetzt werden können. Dies war insbesondere fraglich, als zu Zeiten des „Lockdowns“ ein Besuch der Beratungsstellen nicht zulässig war. In diesem Einsatzbereich ist der Datenschutz der Klienten und damit die **Verarbeitung von zumeist besonderen Kategorien personenbezogener Daten** zu berücksichtigen.

Dass Videokonferenzsysteme auch im Gesundheitsbereich eingesetzt werden können, zeigt sich insbesondere bei der Telemedizin bzw. bei telemedizinischen Methoden in der Gesundheitsversorgung. Dabei handelt es sich jedoch um eigens dafür geschlossene Netze, die die Akteure verbinden und vom kommerziellen Internet abschotten. Werden Gesundheitsdaten im Rahmen der diakonischen Arbeit außerhalb von den an die Telemedizin angeschlossenen Einrichtungen verarbeitet, sind bei der Auswahl und Installation eines Systems ähnlich **hohe Maßstäbe** anzulegen. Bei der Auswahl für diesen Einsatzbereich ist insbesondere darauf zu achten, dass eine Ende-zu-Ende-Verschlüsselung zwischen den Akteuren vorliegt, um die Vertraulichkeit zu gewährleisten. Im Rahmen von Beratungsgesprächen liegt in der Regel gerade nicht die typische Videokonferenzsystemsituation mit mehreren Teilnehmenden vor, sondern ein Gespräch zwischen Beratenden und Klienten. Soweit hier auf Systeme zurückgegriffen wird, die eine direkte Verbindung zwischen zwei Akteuren herstellen, besteht die Möglichkeit, die Kommunikation vollständig zu verschlüsseln, ohne dass offene Daten an irgendeiner Stelle abgefangen werden können. Auch dürfen keine Metadaten von Dritten wahrgenommen werden können. Dazu gehören Angaben zu der Verbindung hinsichtlich der Teilnehmenden und die Verbindungszeiten. Der BfD EKD prüft die technischen Voraussetzungen von Videokonferenzsystemen, um Einrichtungen und örtlich Beauftragte für den Datenschutz bei der datenschutzkonformen Installation solcher Systeme beraten zu können.

Verschicken eines Videos mit einer Bewohnerin über einen Messenger

Im Jahr 2020 wurde aus einer diakonischen Einrichtung eine Datenpanne gemeldet, bei der eine Mitarbeiterin eine Bewohnerin bei einer pflegerischen Maßnahme mit einem Video aufgenommen und diese Aufnahme über einen Messenger-Dienst verbreitet hat.

Auch im diakonischen Bereich werden Messenger-Dienste immer wieder als Kommunikationsmittel eingesetzt. Ohne großen Aufwand kann bei den meisten Messenger-Diensten eine Gruppe von Personen erreicht und Informationen sowie Daten an ausgewählte Personen versendet werden. Allerdings handelt es sich bei Gesundheitsdaten um besonders schützenswerte Daten, sog. besondere Kategorien personenbezogener Daten gemäß § 4 Nr. 2 lit. e) DSG-EKD. Pflegekräfte unterliegen zudem der Schweigepflicht. Ein Messenger-Dienst darf daher zur **Übermittlung von (besonderen Kategorien) personenbezogener Daten nicht eingesetzt** werden.

Aber auch unabhängig davon stellt sich bei Messenger-Diensten regelmäßig die Frage nach dem **Umgang mit den Metadaten** – sofern es sich um personenbezogene Daten handelt – und ob der eingesetzte Messenger-Dienst diese Daten seiner Nutzenden kommerziell verwertet. In diesem Fall wird regelmäßig schon ein Verstoß der kirchlichen Stellen gegen den datenschutzrechtlichen Grundsatz der zweckgebundenen Datenverarbeitung vorliegen. Darüber hinaus verarbeiten viele Messenger-Dienste die Nutzerdaten in Drittländern, d.h. außerhalb des Geltungsbereichs der DSGVO. Auch im kirchlichen und diakonischen Bereich unterliegt eine Datenübermittlung in Drittländern gemäß § 10 DSG-EKD besonderen rechtlichen Anforderungen. In diesem Zusammenhang stellen vor allem sogenannte Angemessenheitsbeschlüsse der Europäischen Kommission eine Rechtsgrundlage zur Datenübermittlung in Drittländer dar. Hierunter fällt auch das EU-US Privacy Shield, das der Europäische Gerichtshof mit Urteil vom 16. Juli 2020 für ungültig erklärt hat. Die hiermit verbundenen Unsicherheiten können nur durch die Wahl eines Messenger-Dienstes vermieden werden, der die personenbezogenen Daten ausschließlich in einem Mitgliedsstaat der Europäischen Union, den Staaten des Europäischen Wirtschaftsraums, Norwegen, Liechtenstein, Island oder der Schweiz verarbeitet.

Ein weiteres Problem kann auch im **standardmäßigen Auslesen** der auf dem Endgerät des Nutzenden gespeicherten **Kontaktdaten** und deren **Abgleich** mit allen vom Anbieter gespeicherten Bestandsdaten liegen. Stets muss auch geprüft werden, wie die Daten verschlüsselt werden. Im Ganzen muss immer die Frage geklärt werden, ob der Einsatz von Messenger-Diensten zur Erledigung der Aufgaben tatsächlich erforderlich ist. Auf die datenschutzrechtlichen Aspekte bei der Nutzung von Messenger-Diensten geht der BfD EKD in der „Stellungnahme zum Einsatz von Messenger-Diensten“ (abrufbar unter: https://datenschutz.ekd.de/infothek-items/stellungnahme-zum-einsatz-von-messenger-diensten/) und der ergänzenden Stellungnahme zum Thema Messenger-Dienste (abrufbar unter: https://datenschutz.ekd.de/wp-content/uploads/2018/10/Erg%C3%A4nzende-Stellungnahm-MessgrDienste.pdf) ein.

Videoüberwachung in der Theorie

Der Wunsch nach einer Videoüberwachung wird auch in kirchlichen Einrichtungen immer größer. Doch zu welchem Zweck und unter welchen Voraussetzungen ist eine Videoüberwachung überhaupt rechtlich zulässig?

Die Videoüberwachung stellt einen besonders intensiven Eingriff in das Persönlichkeitsrecht des Betroffenen dar. Sowohl das Gesamtverhalten als auch äußerliche Merkmale werden beobachtet und können analysiert werden. Um der Intensität des Eingriffs gerecht zu werden, sieht das EKD-Datenschutzgesetz in **§ 52 DSG-EKD** eine spezielle Rechtsgrundlage für die Videoüberwachung öffentlich zugänglicher Räume vor. Auf Videoüberwachungen von nichtöffentlich zugänglichen Räumen findet § 52 DSG-EKD keine Anwendung. Werden Gottesdienste aufgezeichnet oder übertragen, so sind die zusätzlichen Voraussetzungen des § 53 DSG-EKD zu berücksichtigen.

Gemäß **§ 52 Abs. 1 DSG-EKD** ist die Beobachtung öffentlich zugänglicher Bereiche innerhalb und außerhalb von Dienstgebäuden mit optisch-elektronischen Einrichtungen zulässig, soweit sie in Ausübung des Hausrechts der kirchlichen Stelle oder zum Schutz von Personen und Sachen erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Optisch-elektronische Einrichtungen sind alle Geräte, die sich zur Beobachtung eignen. Sie müssen die Erfassung von Geschehnissen und Personen ermöglichen. Dazu gehören neben den typischen Kameras unter anderem auch Drohnen, Smartphone-Kameras und Dashcams.

Die Beobachtung muss in öffentlich zugänglichen Räumen erfolgen. Räume sind öffentlich zugänglich, wenn sie dem öffentlichen Verkehr gewidmet sind oder nach dem erkennbaren Willen des Berechtigten von jedermann genutzt bzw. betreten werden können. Es ist nicht erforderlich, dass ein mit Wänden umschlossener und überdachter Bereich vorliegt. Unerheblich ist auch, ob vor dem Betreten des Raumes eine Anmeldung, z. B. an der Pforte oder Rezeption, erfolgen muss. Entscheidend ist, dass der Raum grundsätzlich von jedem betreten werden darf und nicht nur einem bestimmten Personenkreis zur Verfügung steht. Räume können auch öffentlich zugänglich sein, wenn sie nur in einem festgelegten Zeitraum von jedermann betreten werden dürfen (z. B. nur Werktags).

Möchte eine kirchliche Stelle einen öffentlich zugänglichen Raum videoüberwachen, so muss sie vorab prüfen, welcher Zweck mit der Videoüberwachung verfolgt wird und ob der Zweck von § 52 Abs. 1 DSG-EKD umfasst ist.

Die Videoüberwachung kann gemäß § 52 Abs. 1 Nr. 1 DSG-EKD zur Ausübung des Hausrechts zulässig sein. Die Ausübung des Hausrechts obliegt dem unmittelbaren Besitzer, der nicht zugleich auch Eigentümer sein muss. Der Besitzer ist befugt zu entscheiden, wer die Räume betreten und sich darin aufhalten darf.

Darüber hinaus ist die Videoüberwachung öffentlich zugänglicher Räume gemäß § 52 Abs. 1 Nr. 2 DSG-EKD zulässig, wenn diese zum Schutz von Personen und Sachen erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Es muss eine Gefahr für die Rechtsgüter des Verantwortlichen oder für die Rechtsgüter von Dritten drohen. Der Verantwortliche muss verpflichtet sein, für den Schutz der Personen bzw. Sachen einzustehen. Darüber hinaus wird in § 52 Abs. 1 Nr. 2 DSG-EKD darauf hingewiesen, dass das Interesse an der nicht überwachten Teilnahme am Gottesdienst besonders schutzwürdig ist.

Die Videoüberwachung des öffentlich zugänglichen Raumes muss zur Erreichung des verfolgten Zwecks erforderlich sein. Sie muss dazu geeignet sein, den verfolgten Zweck zu erreichen und es darf kein milderes gleichwirksames Mittel zur Verfügung stehen. Kommt ein milderes Mittel in Betracht, so muss dies für den Verantwortlichen auch objektiv zumutbar sein. An der Erforderlichkeit kann es fehlen, wenn der verfolgte Zweck zum Beispiel durch eine bessere Beleuchtung, verstärkte Kontrollen, neue Schließanlagen oder bauliche Umgestaltung erreicht werden kann.

Vor der Einführung einer Videoüberwachung muss die verantwortliche Stelle gemäß § 52 Abs. 1 Nr. 2 DSG-EKD prüfen, ob die schutzwürdigen Interessen der betroffenen Personen die Interessen der verantwortlichen Stelle überwiegen. Die Interessenabwägung erfordert eine umfassende Abwägung aller widerstreitenden

Interessen. Können Anhaltspunkte für ein Überwiegen der Interessen der betroffenen Personen nicht ausgeräumt werden, so ist die Videoüberwachung unzulässig. Bei der Interessenabwägung sind insbesondere die Eingriffsintensität sowie die konkrete Ausgestaltung der Videoüberwachung zu berücksichtigen. Eine ständige und lückenlose Videoüberwachung stellt einen besonders schwerwiegenden Eingriff dar. Es ist daher zu prüfen, ob die Videoüberwachung auf konkrete Zeiträume (z. B. nachts) beschränkt werden kann. Daneben sind auch technische und organisatorische Maßnahmen zu treffen. Es sollte ein eingeschränktes Zugriffsmanagement und Möglichkeiten zur Verschlüsselung, Zugangskontrollen sowie automatisierte Speicherfristen bestehen. Auch sollten die Funktionen der Kamera möglichst datenschutzfreundlich eingestellt werden. Das heißt, dass z. B. die Zoom- und Schwenkfähigkeit einer Kamera ausgeschaltet sein sollte.

Gemäß **§ 52 Abs. 2 DSG-EKD** sind der Umstand der Beobachtung, der Name und die Kontaktdaten der verantwortlichen Stelle durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Dies kann z. B. durch gut sichtbare Hinweisschilder erfolgen, die vor dem Betreten des videoüberwachten Bereichs angebracht sind.

Die Speicherung oder Verwendung der erhobenen Daten ist gemäß **§ 52 Abs. 3 DSG-EKD** zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Speicherung und Verwendung setzen voraus, dass die Daten auch in zulässiger Weise erhoben wurden. War die Datenerhebung nicht zulässig, so sind die erhobenen Daten unverzüglich zu löschen. Vor der Speicherung oder Verwendung der Daten muss die verantwortliche Stelle eine Interessenabwägung durchführen. Danach ist die Speicherung und Verwendung nur zulässig, wenn die schutzwürdigen Interessen der betroffenen Personen die Interessen der verantwortlichen Stelle nicht überwiegen. Die Interessenabwägung sollte dokumentiert werden.

Werden die durch die Videoüberwachung erhobenen Daten einer bestimmten Person zugeordnet und verarbeitet, so ist die Person über die jeweilige Verarbeitung zu benachrichtigen. Durch die Regelung in **§ 52 Abs. 4 DSG-EKD** wird eine transparente Ausgestaltung des Datenverarbeitungsvorgangs sichergestellt. Von der Benachrichtigung kann abgesehen werden, solange das öffentliche Interesse an der Strafverfolgung das Recht auf Benachrichtigung der betroffenen Person erheblich überwiegt oder wenn die Benachrichtigung im Einzelfall einen unverhältnismäßigen Aufwand erfordert.

Gemäß **§ 52 Abs. 5 DSG-EKD** sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Die Daten sind zur Erreichung des Zwecks nicht mehr erforderlich, wenn der mit der Videoüberwachung verfolgte Zweck erreicht wurde oder der Zweck zwischenzeitlich weggefallen ist. Schutzwürdige Interessen der Betroffenen stehen einer weiteren Speicherung entgegen, sobald die Interessenabwägung nachträglich zugunsten der Betroffenen ausfällt. Liegt einer der beiden Löschungsgründe vor, so sind die Daten unverzüglich, d. h. ohne schuldhaftes Zögern zu löschen. Hat der Betroffene selbst ein schutzwürdiges Interesse an der weiteren Speicherung seiner personenbezogenen Daten, so dürfen die Daten nicht von der verantwortlichen Stelle gelöscht werden.

Fazit: Möchte eine kirchliche Stelle einen öffentlich zugänglichen Raum videoüberwachen, so muss sie zunächst prüfen, ob die Videoüberwachung zu einem legitimen Zweck erfolgt und ob der Zweck nicht auch durch mildere gleichwirksame Mittel erreicht werden kann. Vor der Einführung der Videoüberwachung muss die kirchliche Stelle eine Datenschutz-Folgenabschätzung gemäß § 34 DSG-EKD durchführen. Die vorgenommene Prüfung sollte dokumentiert werden.

Videoüberwachung des Opferstocks in einer Kirche

Im Rahmen des **Projekts „Offene Kirche“** soll es Gemeindegliedern oder sonstigen Interessierten ermöglicht werden, Kirchen auch außerhalb des Gottesdienstes zu betreten. Das Projekt wird in mehreren Landeskirchen durchgeführt. Im Zusammenhang mit der Kirchenöffnung stellt sich der verantwortlichen Stelle unter anderem die Frage, wie die Kirche und insbesondere der Opferstock in Zeiten, in denen niemand aus der Kirchengemeinde in der Kirche anwesend ist, gesichert werden können. Im Rahmen einer Beratungsanfrage an den

BfD EKD hat eine Kirchengemeinde erwogen eine Videoüberwachung des Opferstockes einzurichten.

Die Videoüberwachung könnte auf § 52 DSG-EKD gestützt werden. Beim Innenraum einer Kirche handelt es sich um einen öffentlich zugänglichen Raum gemäß § 52 Abs. 1 DSG-EKD. Dies lässt sich der klarstellenden Regelung in § 52 Abs. 1 Satz 2 DSG-EKD entnehmen, die auf die Gottesdienstteilnahme Bezug nimmt und regelt, dass die nicht überwachte Teilnahme an einem Gottesdienst besonders schutzwürdig ist.

Der Zweck des Schutzes von Sachen ist ebenfalls gegeben. Entscheidend ist somit – wie so oft im Datenschutzrecht – die Prüfung der **Erforderlichkeit der Videoüberwachung** im konkreten Fall. Insbesondere darf der verfolgte Zweck nicht durch mildere gleichwirksame Mittel erreicht werden.

Als **milderes gleichwirksames Mittel** könnten Ehrenamtliche, Nachbarn oder sonstige Dritte akquiriert werden, die in Zeiten der „offenen Kirche“ vor Ort sind. Auch wäre ein Hinweis am Opferstock, dass dieser regelmäßig geleert wird und somit „Diebstahl zwecklos“ ist, vorstellbar.

Zusätzlich darf **kein schutzwürdiges Interesse der Betroffenen** überwiegen. Es geht um die Interessen aller Besucher der „offenen Kirche“. In einer Handreichung der Landeskirche, zu der die anfragende Kirchengemeinde gehört, wird darauf hingewiesen, dass auch außerhalb des Gottesdienstes bei der offenen Kirche die Spiritualität im Vordergrund steht. Dies spricht für eine besondere Schutzwürdigkeit der Menschen, die diese Spiritualität suchen. Durch eine Videoüberwachung wäre ein unbeobachteter Besuch einer Kirche nicht mehr möglich. Hierin besteht aber ein schutzwürdiges Interesse der betroffenen Personen. Auch die Tatsache, dass die Kirchengemeinde nachvollziehen könnte, wer wann in welchem Umfang spendet, wurde durch die anfragende Kirchengemeinde selbst problematisiert. Die Möglichkeit einer freiwilligen und auch unbeobachteten Spende stellt ebenfalls ein schutzwürdiges Interesse dar.

Fazit: Aus den genannten Gründen wurde der Kirchengemeinde davon abgeraten, eine Videoüberwachung des Opferstocks sowie des Eingangsbereichs der Kirche während der Zeiten der „offenen Kirche“ durchzuführen.

Datensicherheit, Verschlüsselung und „Cookies“

In Kirche und Diakonie ist es im Berichtszeitraum aus unterschiedlichen Gründen zu Datenverlusten gekommen. Die Themen Datensicherheit und Verschlüsselung sind daher weiterhin ein wichtiger Bestandteil der Arbeit des BfD EKD. Daneben hat sich der BfD EKD auch mit verschiedenen anderen technischen Beratungsanfragen beschäftigt.

Gehackte E-Mail-Konten durch Virenbefall

Gefälschte E-Mails im Namen von Freunden, Kollegen oder Geschäftspartnern gefährden ganze Netzwerke. Im Berichtszeitraum erhielt der BfD EKD mehrere Datenpannenmeldungen, **die gehackte E-Mail-Konten** betrafen. Oft wurde das Problem erst erkannt, nachdem über das Postfach E-Mails an alle im E-Mail-Konto befindlichen Kontakte verschickt wurden und sich daraufhin einige der betroffenen Empfänger bei dem Absender meldeten, weil sie misstrauisch wurden. Das Zugriffspasswort auf den E-Mail-Account war außerdem geändert worden, so dass der Inhaber des E-Mail-Accounts keinen Zugriff mehr auf diesen hatte. Es handelte sich dabei überwiegend um E-Mail-Accounts bei Standardprovidern, die sich kleine kirchliche Einrichtungen wie Kindertageseinrichtungen oder Beschäftigte in Kirchengemeinden selbst eingerichtet hatten. Als Maßnahmen wurden **Passwortänderungen** vorgenommen. Manchmal war jedoch nur noch eine komplette Deaktivierung und Löschung des E-Mail-Kontos möglich.

Die Symptome deuteten in den meisten Fällen nicht auf ein einfaches individuelles Ausspähen der Passwörter hin, sondern auf einen **weiterreichenden Virenbefall** wie z. B. durch die Schadsoftware Emotet. Diese gilt als eine der größten Bedrohungen durch Schadsoftware weltweit und verursachte auch in Deutschland hohe Schäden. Hierbei wird das Virus durch das Öffnen von infizierten Microsoft Office-Dateien, die als Mailanhang vorlagen, oder durch das Anklicken von Internetlinks, die auf infizierte Internetseiten führen, aktiviert und durch die Nutzung des Programmes Outlook an alle in Outlook vorhandenen Mailadressen verbreitet. Weiterhin besteht die Möglichkeit, dass durch das Virus die Angreifer administrativen Zugang zu den befallenen IT-Systemen erlangen und weitere Schadsoftware auf diesen Systemen installieren können. Dadurch werden

beispielsweise interne Daten verschlüsselt und damit unbrauchbar gemacht oder Daten durch unbefugte Dritte ausgespäht. Der BfD EKD hat in diesen Fällen darauf hingewiesen, dass eine reine Passwortänderung des E-Mail-Kontos nicht ausreicht, sondern **weitere Maßnahmen** ergriffen werden müssen. So ist die IT-Technik, mit der auf dem E-Mail-Konto gearbeitet wurde, gesondert auf Virenbefall zu prüfen und gegebenenfalls das System völlig neu aufzusetzen. Sämtliche Zugangsdaten, die auf betroffenen Systemen genutzt wurden, sind vorsichtshalber zu ändern.

Fazit: Beschäftigte in Kirche und Diakonie sollten regelmäßig sensibilisiert und geschult werden, um verdächtige E-Mails, die immer professioneller gestaltet sind, erkennen zu können und angemessen zu handeln. Alle Systeme sollten immer auf einem möglichst aktuellen Stand gehalten werden. Außerdem sollten vorbeugend die vorhandenen Systeme möglichst so konfiguriert werden, dass unbekannte Programme und Makros in Office-Dateien nicht automatisch ausführbar sind.

Umgang mit E-Mails bei ungeplanten Abwesenheiten von Beschäftigten

Im Berichtszeitraum wurde mehrfach die Frage gestellt, wie bei ungeplanten Abwesenheiten von Mitarbeitenden die Bearbeitung von deren E-Mails sichergestellt werden kann. Dabei ist vor allem das Thema Privatnutzung des beruflichen E-Mail-Accounts und Internetzugangs relevant.

In einem konkreten Beratungsfall erkundigte sich eine kirchliche Einrichtung danach, welche datenschutzkonforme Lösung es bei einer **ungeplanten längeren krankheitsbedingten Abwesenheit** eines Mitarbeitenden für dessen **E-Mail-Bearbeitung** gibt. In der Einrichtung war die **Privatnutzung** der beruflichen E-Mail-Infrastruktur durch eine **Dienstvereinbarung ausgeschlossen.** Bei Vorliegen einer solchen Dienstvereinbarung kann im Fall von ungeplanten längeren Abwesenheiten (z. B. plötzliche schwere Erkrankung) sowohl eine automatische Weiterleitung von E-Mails an eine andere E-Mail-Adresse als auch die Nutzung des Abwesenheitsassistenten in Betracht kommen. Vor dem Hintergrund der Erforderlichkeit ist aber zu beachten, dass die Einrichtung einer automatischen Weiterleitung von E-Mails an einen im Rahmen eines Vertretungskonzepts oder ad hoc benannten Vertreters einen stärkeren Eingriff darstellt als die Einrichtung eines Abwesenheitsassistenten mit Verweis auf den Vertreter. Bei der Einrichtung eines Abwesenheitsassistenten handelt es sich um das rechtlich mildere Mittel. Aus diesem Grund ist eine Weiterleitung auch unter Berücksichtigung der Interessen der Beschäftigten nur dann statthaft, wenn eine Abwesenheitsmitteilung aus besonderen Gründen nicht ausreicht. Auf bereits empfangene bzw. versandte E-Mails darf stets nur zugegriffen werden, wenn dies für dienstliche Zwecke erforderlich ist.

Dienstvereinbarungen, die vor dem Inkrafttreten des neuen EKD-Datenschutzgesetzes geschlossen wurden, sind dahingehend zu überprüfen, ob diese noch den Anforderungen des EKD-Datenschutzgesetzes entsprechen. Insbesondere aufgrund der erhöhten **Transparenzpflicht** gemäß § 5 Abs. 1 Nr. 1 DSG-EKD besteht die Notwendigkeit, bei Kontrollmaßnahmen gegenüber den Betroffenen deutlich zu machen, welche personenbezogenen Daten wie lange gespeichert und von wem eingesehen werden können. In der Praxis hat der BfD EKD vielfach festgestellt, dass Dienstvereinbarungen, die älter als 10 Jahre sind, den Anforderungen nicht mehr entsprechen.

Allgemein kann auf die Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ aus dem Jahr 2016 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hingewiesen werden, die auch Beispiele für Dienstvereinbarungen enthält. Diese ist auf den Internetseiten der staatlichen Aufsichtsbehörden sowie in der Internetpräsenz des BfD EKD zu finden.

Verschlüsselung von Datenträgern und E-Mails

Im aktuellen Berichtszeitraum erreichten den BfD EKD zahlreiche Meldungen von Datenpannen zum Thema Verschlüsselung.

Mehrfach wurde mit Datenpannenmeldungen der Diebstahl unverschlüsselter Laptops und Festplatten sowie der Verlust von unverschlüsselten USB-Sticks auf dem Postweg angezeigt. Auf den Datenträgern wurden jeweils große Mengen personenbezogener Daten gespeichert, darunter z. B. Personaldaten von Beschäftigten oder Gesundheitsdaten von Patienten eines Krankenhauses. Eine **Verschlüsselung von Datenträgern**, auf denen personenbezogene Daten gespeichert sind, sollte in Kir-

che und Diakonie mittlerweile Standard sein und entsprechende Verschlüsselungsprogramme wie z. B. Bitlocker, Veracrypt oder Sophos SafeGuard von verantwortlichen Stellen eingesetzt werden. Bei USB-Sticks ist auch die Verwendung spezieller Geräte mit einer Hardwareverschlüsselung möglich.

Weiterhin erreichten den BfD EKD Datenpannenmeldungen, dass sensible personenbezogene Daten – wie z. B. Patientendaten oder Entwicklungsberichte von Kindern – unverschlüsselt per E-Mail an falsche E-Mail-Adressen geschickt wurden. An die Verarbeitung **besonderer Kategorien personenbezogener Daten** im Gesundheits- und Sozialbereich werden gemäß § 13 Abs. 2 und 3 DSG-EKD besonders strenge Anforderungen gestellt. Zur Gewährleistung der Vertraulichkeit wird empfohlen, beim Versenden von besonderen Kategorien personenbezogener Daten mit einer **E-Mail** eine **Ende-zu-Ende-Verschlüsselung** zu nutzen.

E-Mail-Systeme arbeiten standardmäßig lediglich mit einer **Transportverschlüsselung**. Dabei ist zwar der Übertragungsweg geschützt, doch die Mails liegen beim Absenden, beim Empfangen und während der Mailübertragung auf den jeweiligen Servern offen vor. Eine Möglichkeit zur Vermeidung von Datenpannen durch E-Mail-Fehlversand ist die Nutzung einer asymmetrischen Verschlüsselungsmethode mittels **PGP oder S/Mime**. Mit einem „öffentlichen" Schlüssel des Empfängers kann der Absender die betreffende Mail verschlüsseln und nur der berechtigte Empfänger kann mit seinem „privaten" (geheimen) Schlüssel die Daten wieder entschlüsseln. Da dieses System jedoch technisch aufwendig einzurichten und nicht überall anwendbar ist, gibt es die Alternative sensible Daten in einer Datei mittels eines geeigneten **Verschlüsselungsprogramms**, wie z. B. 7zip oder Winzip, zu schützen. Die verschlüsselte Datei kann dann als Anhang der E-Mail verschickt werden. Der Schlüssel – das Passwort – muss dem Empfänger auf eine andere Weise mitgeteilt werden (z. B. per Telefon oder SMS). Eine weitere Möglichkeit zum elektronischen Austausch von Dateien mit besonderen Kategorien personenbezogener Daten kann die Nutzung eines speziellen **Datei-Austausch-Servers** sein. Hierbei können Nachrichten und Dateien in einer Internet-Cloud automatisch verschlüsselt abgelegt werden. Der Empfänger wird nur per E-Mail darüber informiert und kann sich die Dateien dann herunterladen. Das Passwort ist allerdings auch hier auf einem anderen Wege zu übermitteln.

Einbinden von „Cookies" auf Internetseiten

Im Zusammenhang mit Beratungsanfragen wurden zahlreiche Websites von kirchlichen und diakonischen Stellen hinsichtlich der Umsetzung des Datenschutzes überprüft. Dabei wurden große Unsicherheiten deutlich, die insbesondere den Einsatz von „Cookies" betrafen. Cookies ermöglichen dem Websitebetreiber, die Besucher der Website wiederzuerkennen und Voreinstellungen für ein bequemes Surfen für die Nutzenden bereitzustellen. Es können aber auch Profile über das Surfverhalten der Nutzenden erstellt werden. Darüber hinaus ist es sogar möglich, die Besuchenden der Website und ihre Aktivitäten über verschiedene Websites hinaus nachzuverfolgen.

Nach der aktuellen **Rechtsprechung des BGH** vom 28. Mai 2020 (I ZR 7/16) ist eine aktive Einwilligung für sogenannte Tracking-Cookies notwendig. Das Wegklicken eines bereits vorausgefüllten Feldes stellt keine wirksame Einwilligung dar.

Die Betreiber von Websites müssen also prüfen, ob auf ihrer Internetpräsenz Cookies verwendet werden. Wenn ja, ist zunächst zu klären, ob diese **technisch notwendig** und somit ohne Einwilligung des Nutzenden zulässig sind. Sofern die „Cookies" eine **Analyse des Nutzerverhaltens** erlauben oder zu **Werbezwecken** verwendet werden, ist stets eine explizite Einwilligung der Nutzenden erforderlich. Werden solche technisch nicht notwendigen Tracking- und Analysetools gesetzt, so müssen diese standardmäßig deaktiviert sein. Die Nutzenden müssen vor dem Setzen eines solchen Cookies entsprechend informiert werden und ihre Einwilligung geben können. Dies kann durch eine extra vorgeschaltete Website oder ein Opt-In-Banner, bei dem man explizit die optionalen Cookies erlauben kann, ermöglicht werden. Das Weitersurfen auf den entsprechenden Seiten muss auch ohne Zustimmung möglich sein. Für technisch notwendige Cookies wird dagegen keine aktive Einwilligung benötigt. Sie müssen daher nur in der Datenschutzerklärung erwähnt werden. Werden keine Cookies auf der Website verwendet, ist auch keine Information zu diesem Thema nötig.

Alle kirchlichen und diakonischen Einrichtungen müssen

deswegen prüfen, ob und in welchem Umfang sie tatsächlich **Tracking- und Analyse-Tools** benötigen, da der datenschutzkonforme Betrieb in der Regel zusätzliche Maßnahmen und eine wirksame Einwilligung der Nutzenden nach § 6 Nr. 2 DSG-EKD erfordert. Um Informationen über das Nutzerverhalten zu erhalten, sind entsprechend § 5 Abs. 1 Nr. 3 DSG-EKD und § 28 DSG-EKD möglichst datensparsame Techniken einzusetzen. So könnte eine Analyse mit anonymisierten IP-Adressen das Setzen von Tracking-Cookies ersetzen. Sollen Tracking-Cookies durch externe Dienstleister (sogenannte „Drittanbieter“) gespeichert und ausgewertet werden, muss geprüft werden, ob die §§ 10, 29 und 30 DSG-EKD zu berücksichtigen sind.

Auch das Einbinden von **Social Media Plug-Ins** oder **externen Videos** muss so gestaltet werden, dass die Nutzenden vorher ihre Einwilligung zum Aufruf dieser geben können. Dies kann z. B. durch die sogenannte **„Zwei-Klick-Lösung“** oder die **„Shariff-Lösung“** erfolgen. Normale Linksetzungen auf die externen Internetdienstanbieter sind nicht einwilligungspflichtig.

Bei den exemplarischen Prüfungen des BfD EKD fielen unter anderem Websites mit einem prophylaktischen „Cookie-Banner“ auf, die gar keine Tracking-Cookies setzten. Eine kirchliche Stelle hatte auf ihrer Website eine Datenschutzerklärung eingestellt, die mittels eines sog. Generators erzeugt worden war und der sich nur allgemeine Erläuterungen zum Thema Cookies entnehmen ließen. Eine Anpassung der Datenschutzerklärung an die konkreten Bedingungen fehlte. Auf anderen Websites wurden Plug-Ins von Drittanbietern verwendet, die beim Aufruf der Websites direkt eigene Cookies setzten.

Fazit: Jede verantwortliche Stelle muss immer konkret prüfen, wie ihre Website technisch ausgestaltet ist, welche Tools tatsächlich eingesetzt werden und wie eine datenschutzkonforme Umsetzung der rechtlichen Vorgaben realisiert werden kann.

Softwareentwicklung und Softwareprüfung

Einige der im Berichtszeitraum beim BfD EKD eingegangenen technischen Beratungsanfragen bezogen sich auf Themen aus den Bereichen Softwareentwicklung und Softwareprüfung.

Sicherheitslücken und Schwachstellen in speziell entwickelten Webanwendungen

Im Rahmen der Datenpannenmeldung einer kirchlichen Stelle beschäftigte sich der BfD EKD mit den Datenschutzanforderungen bei der Softwareentwicklung. Ein unabhängiger IT-Sicherheitsexperte hatte der verantwortlichen Stelle das Vorhandensein mehrerer Sicherheitslücken und Schwachstellen in der Gruppenverwaltung einer individuell entwickelten Webanwendung gemeldet.

Dies hatte zur Folge, dass ein in der Anwendung authentifizierter Nutzer auf beliebige Konten und die damit verknüpften Daten zugreifen konnte. Zu diesen Daten gehörten unter anderem der Nutzername sowie der intern verwendete Benutzername, der der Einfachheit halber oftmals auch aus dem Vor- und Zunamen des Benutzers bestand. Darüber hinaus war in einigen Fällen sowohl das jeweilige Profilfoto als auch ein persönlicher Code einsehbar. Mit diesem Code wäre es für einen Angreifer möglich gewesen, sich in der dazugehörigen App zu authentifizieren, sich im Namen der betroffenen Person in fremde Gruppen einzuladen und auf die dort hinterlegten Bilder, Videos und Texte zuzugreifen. Um diesen **„Angriff“** auszuführen, war es lediglich notwendig den „ID“-Parameter in der URL des Requests zu ändern. Auf ähnliche Weise, nämlich durch die **Manipulation** von Parametern, hätte ein Angreifer auf fremde Gruppenfeeds zugreifen und mit den Rechten eines Gruppenadministrators Änderungen an den Beiträgen vornehmen können. Darüber hinaus wurde eine Sicherheitslücke gemeldet, die über Cross-Site-Scripting ausgenutzt werden konnte. Durch diese Schwachstelle hätte ein Angreifer einen eigenen Schadcode in eine Seite der Webanwendung einfügen können. Dieser Code wird beim Aufrufen der betroffenen Seite durch einen Nutzenden im Browser des Nutzenden ausgeführt. Dies kann zur Folge haben, dass die komplette Sitzung des Nutzenden durch den Angreifer übernommen wird. Durch das Ausnutzen weiterer Schwachstellen und Angriffstechniken kann dies im schlimmsten Fall zu einem vollständigen **Kompromittieren** des Endgerätes des Nutzenden führen. Da zu den Nutzenden dieser Anwendung insbesondere Minderjährige gehören, war dies besonders kritisch zu bewerten.

Die in der Anwendung entdeckten Sicherheitslücken und Schwachstellen zeigen deutlich auf, wie schwierig es ist, komplexe Systeme fehlerfrei und sicher zu entwickeln. Dafür ist ein IT-Sicherheitsbewusstsein bei den Entwicklern und den Verantwortlichen notwendig. Eine Sensibilisierung zu dem Thema reicht nicht aus. Durch die verantwortlichen Stellen muss sichergestellt werden, dass die mit der Entwicklung betrauten Personen auch tatsächlich Expertise bei der sicheren Softwareentwicklung besitzen, Angriffsvektoren kennen und wissen, wie man komplexe Systeme gegen Angriffe sichert.

Eine Hilfestellung kann das **„Open Web Application Security Project" (OWASP)** sein (https://owasp.org/). Dabei handelt es sich um eine gemeinnützige Stiftung, deren Ziel es ist, die Sicherheit von Software zu verbessern. Durch diverse Open Source Projekte und unterschiedliche Schulungsmaterialien und -veranstaltungen ist OWASP eines der am weitesten anerkannten Projekte im Hinblick auf IT-Sicherheit. OWASP arbeitet aktiv an diversen offenen Werkzeugen und Ressourcen. Es veröffentlicht regelmäßig Trainings- und Lehrmaterial und organisiert Veranstaltungen, um zu verschiedenen IT-Sicherheitsthemen zu informieren. Ein Großteil der Arbeiten des OWASP wird lediglich in englischer Sprache veröffentlicht. In einigen wenigen Fällen gibt es allerdings deutsche Übersetzungen. Das OWASP führt derzeit knapp 100 Projekte auf seiner Internetseite auf. Diese Projekte reichen von Guidelines über Testleitfäden bis hin zu Open Source Software, die bei Sicherheitsanalysen unterstützen kann. Einzelheiten zu den Projekten können der Website entnommen werden.

Grundsätzlich empfiehlt der BfD EKD vor Inbetriebnahme einer Anwendung, die am Internet angeschlossen ist, das **Durchführen von Penetrationstests**. Weiterführende Tests sind angebracht und sinnvoll, wenn ein erhöhtes Risiko besteht oder besonders sensible Daten verarbeitet werden. Auch sollten sich die Entwickler solcher Anwendungen regelmäßig im Bereich der (Software-) Sicherheit weiterbilden lassen. Dabei können die Materialien des OWASP eine sinnvolle Lernressource sein. Im Fall der gemeldeten Datenpanne hätten die Schwachstellen frühzeitig – also am besten noch vor Veröffentlichung – erkannt werden können, wenn ein Penetrationstest der Anwendung durchgeführt worden wäre.

Durch schnelles Reagieren der verantwortlichen Stelle konnten die Sicherheitslücken und Schwachstellen in der Webanwendung der kirchlichen Stelle gemeinsam mit dem Dienstleister, der für die Entwicklung zuständig war, geschlossen und zusätzliche Sicherheitsmaßnahmen implementiert werden. Durch die im Nachgang durchgeführte forensische Untersuchung konnte ein aktives Ausnutzen der Schwachstellen ausgeschlossen werden. Darüber hinaus wurde durch einen externen Dienstleister ein Penetrationstest der Anwendung durchgeführt, um etwaige weitere Schwachstellen zu identifizieren und zu beseitigen. Auch wurden die Nutzer der Anwendung über die Schwachstellen in Kenntnis gesetzt und darüber informiert, welche ihrer Daten von der Schwachstelle betroffen waren.

Technische Risikobetrachtung eines Content-Management-Systems

Im Rahmen einer Beschwerde über einen unsachgemäßen Umgang mit personenbezogenen Daten hat sich der BfD EKD mit einem freien Content-Management-System beschäftigt. Content-Management-Systeme werden von Internetseiten und Blogs genutzt und können mit Hilfe von Plugins um diverse Funktionen erweitert werden. Im Rahmen der Beschwerde wurde eine Risikobetrachtung durchgeführt. Die identifizierten Risiken konnten mit Hilfe von technischen und organisatorischen Maßnahmen minimiert werden.

Die meisten Angreifer suchen nach veralteten, angreifbaren Versionen von Content-Management-Systemen und den jeweiligen Bestandteilen. Daher sind **regelmäßige Updates der Software, der Plugins und Themes** für den Betrieb unverzichtbar und bieten einen guten Basisschutz. Für den Administratoren-Account muss außerdem ein starkes Passwort gewählt werden. Weiterhin können Plugin-Seiten mit einer Zwei-Faktor-Authentifizierung abgesichert werden. Die Inhalte sollten beim Transport von und zu dem Nutzer verschlüsselt werden. Eine Transportverschlüsselung kann sehr einfach und kostenlos, z. B. mit „Let's Encrypt" oder „ZeroSSL", realisiert werden.

Es gibt **Plugins**, die den Schutz von Content-Management-Systemen erhöhen, indem sie als zusätzliche Firewall dienen. Diese stellen unter anderem automatische Regelupdates für die Firewall sowie IP-Blacklists, die in Echtzeit abgefragt werden können, zur Verfügung. Darü-

ber hinaus bieten sie eine Erkennung von Schadsoftware über Signaturen an, welche Angreifer automatisch blockieren können, sofern das Angriffsmuster, die IP-Adresse oder die Schadsoftware schon bekannt sind. Plugins dienen unter anderem der Vermeidung von Spam auf den Content-Management-Systemen.

Je nach der benötigten Verfügbarkeit der mit dem Content-Management-System zur Verfügung gestellten Internetseite sind **Backups** und eine **Testumgebung** zu empfehlen. Schnelle und regelmäßige Updates haben den Nachteil, dass enthaltene Fehler oder die Kombination von Plugins und Themes den Betrieb der Instanz stören können. Daher ist es sinnvoll eine Testumgebung zu betreiben, in der man die Updates zuerst einspielt und erst nach einem erfolgreichen Test in die Produktivsysteme übernimmt. Regelmäßige Sicherungen der Dateien und der Datenbank sind ebenfalls zu empfehlen, falls es einmal zu einer Störung kommen sollte.

Fazit: Auch bei Einhaltung aller möglichen Sicherheitsmaßnahmen müssen zur Verfügung gestellte Updates für das Content-Management-System selbst oder für installierte Plugins zeitnah verarbeitet werden.

Audits, Zertifizierungen und Softwarefreigaben

Im Berichtszeitraum erreichten den BfD EKD einige Anfragen von verantwortlichen Stellen und Softwareanbietern (z. B. Anbieter von Verwaltungssoftware für Kindertageseinrichtungen) mit dem Anliegen der Durchführung eines Audits bzw. der Zertifizierung nach § 35 DSG-EKD. Hintergrund war bei diesen Anfragen auch die Herstellung von Rechtssicherheit für den datenschutzkonformen Einsatz von Software nach dem EKD-Datenschutzgesetz.

Bezüglich der Durchführung von Audits und Zertifizierungen nach § 35 DSG-EKD weist der BfD EKD bei Anfragen regelmäßig darauf hin, dass er **kein entsprechendes Verfahren** anbietet und im Übrigen der Rat der EKD **keine Rechtsverordnung** hierzu beschlossen hat. In Deutschland gibt es zahlreiche sehr unterschiedliche Zertifizierungsangebote für Software, wobei auch Zertifizierungen zum Datenschutz immer häufiger angeboten werden. Allerdings kann eine Zertifizierung immer nur ein Hinweis auf ein datenschutzfreundliches Produkt sein und bedeutet keinen „Freifahrtschein".

Vor dem Einsatz neuer Technik und Software muss immer eine **Überprüfung durch die verantwortliche Stelle** (z. B Träger einer Kindertageseinrichtung) erfolgen. Oftmals erfolgt die Prüfung des datenschutzkonformen Einsatzes von Software aber auch auf übergeordneter, beispielsweise auf landeskirchlicher Ebene. In jedem Fall müssen die Vorgaben des EKD-Datenschutzgesetzes eingehalten werden. Der BfD EKD stellt Materialen auf seiner Website in der Rubrik „Infothek" (https://datenschutz.ekd.de/infothek/) in unterschiedlichen Formaten bereit (z. B. Arbeitshilfe zur Durchführung einer Datenschutz-Folgenabschätzung, Muster-Vertrag zur Auftragsverarbeitung, etc.).

Fazit: Der BfD EKD führt keine Audits, Zertifizierungen und Softwarefreigaben durch.

Aufbewahrung und Löschung

Zu den beiden unmittelbar zusammenhängenden Themen Aufbewahrung und Löschung von personenbezogenen Daten bearbeitete der BfD EKD im Berichtszeitraum diverse Beratungsanfragen und Datenschutzbeschwerden.

Umgang mit Gesundheitsdaten in Krankenhäusern

Immer wieder melden evangelische Krankenhäuser dem BfD EKD Datenpannen, bei denen **Gesundheitsdaten** in die Hände von **Unbefugten** gelangt sind. Bei Gesundheitsdaten handelt es sich stets um besondere Kategorien personenbezogener Daten, die einem besonderen Schutz unterliegen. Bei diesen Datenpannen wurden sensible Informationen über Patienten oder Klienten gegenüber Personen oder Einrichtungen offengelegt, die davon keine Kenntnis nehmen durften. Diese Datenpannen sind auf der einen Seite ein Datenschutzverstoß im Sinne des EKD-Datenschutzgesetzes, da die Offenlegung von Gesundheitsdaten ohne eine Rechtsgrundlage erfolgt ist. Auf der anderen Seite wird dadurch das Arzt-Patienten-Geheimnis (ärztliche Schweigepflicht) verletzt und dieses Geheimnis unbefugt gegenüber Dritten offenbart.

Häufige **Ursachen** für diese Datenpannen im täglichen Umgang mit personenbezogenen Daten sind manuelle und organisatorische Fehler beim Versand von Gesundheitsdaten per Fax. Häufig passiert es im Arbeitsalltag, dass die Empfängernummern nicht ausreichend geprüft

werden und daher Gesundheitsdaten an falsche Empfänger versendet werden. Auch die verstärkte Verbreitung von Schadsoftware und Verschlüsselungstrojanern trifft diakonische Einrichtungen. Um dieser Verbreitung entgegenzutreten ist die Aktualisierung der IT-Infrastruktur sowie der organisatorischen Maßnahmen erforderlich. Der Einsatz von mobilen Speichermedien darf nach dem Stand der Technik nur noch verschlüsselt erfolgen, um eine unbefugte Offenbarung bei Verlust auszuschließen. Werden Gesundheitsdaten in analoger Form außerhalb der Einrichtungen genutzt, sind auch hier Sicherungsvorkehrungen wie verschlossene Behältnisse zu treffen, um Datenpannen durch Verlust oder Diebstahl vorzubeugen.

Im Rahmen der **Aufbewahrung von Gesundheitsdaten** sind im analogen und digitalen Bereich vergleichbare Sicherungsmaßnahmen anzuwenden, um eine Offenlegung gegenüber Unbefugten ausschließen zu können. Im analogen Bereich kann die Aufbewahrung mit Hilfe von separaten – dem Schutzniveau angemessenen – Räumlichkeiten mit entsprechender Infrastruktur und im digitalen Bereich mit Hilfe von entsprechend verschlüsselten Archivierungsbereichen sichergestellt werden. Die Aufbewahrung in einem verschlossenen Raum, der auch anderweitig genutzt wird, erfüllt das geforderte Schutzniveau grundsätzlich nicht.

Die datenschutzrechtlichen Anforderungen, die dem Risiko der Verarbeitung von Gesundheitsdaten geschuldet sind, gelten für sämtliche Verarbeitungsschritte bis zur **Vernichtung bzw. Löschung** der Daten und sind über den gesamten Verarbeitungszeitraum durchgängig zu gewährleisten.

Teilnehmendenliste beim Reha-Sport

Ein Klient einer diakonischen Einrichtung, die unter anderem Maßnahmen des Reha-Sports anbietet, wandte sich mit einer Beschwerde an den BfD EKD. Der Petent rügte, dass bei der Anmeldung zum jeweiligen Reha-Sport-Termin eine Liste an der **Anmeldung der diakonischen Einrichtung** ausliege und jeder **Teilnehmende** sich in diese **Liste eintragen** müsse. Es handelte sich bei der Liste um ein Muster einer Krankenkasse. Neben Namen und Vornamen seien auch die Versicherungsnummer und weitere personenbezogene Daten abgefragt worden. Hinter der Liste befänden sich jeweils die Verordnungen der einzelnen Klienten.

Gerade bei der Verarbeitung von Gesundheitsdaten, die z. B. in einer Verordnung zum Reha-Sport enthalten sein können, sind hohe Anforderungen an technische und organisatorische Maßnahmen zu stellen. Im konkreten Fall konnte die Einrichtung nicht begründen, aus welchem Grund das Ausliegen der Verordnungen am Empfang für die Teilnahme am Reha-Sport erforderlich ist. Außerdem konnte nicht vollkommen ausgeschlossen werden, dass unberechtigte Dritte Kenntnis von Gesundheitsdaten erlangen können. Die Verordnungen wurden durch den Reha-Sport-Anbieter umgehend aus den für die Teilnehmenden ausliegenden Ordnern herausgenommen.

Die Einrichtung führte anlässlich der Beschwerde eine eigenständige Überprüfung der Erforderlichkeit der Teilnehmendenlisten durch. Dabei stand der Zweck der Listen, die Teilnehmenden für die Abrechnung bei der Krankenkasse zu dokumentieren, im Vordergrund. Die Einrichtung hat entschieden zukünftig lediglich die Namen der Teilnehmenden in die Liste aufzunehmen.

Umgang mit personenbezogenen Daten im Ehrenamt

Ehrenamtliche Tätigkeit ist ein elementarer Bestandteil der kirchlichen und diakonischen Arbeit vor Ort und nimmt dort einen besonderen Stellenwert ein. Gleichzeitig stellt die ehrenamtliche Tätigkeit sowohl die verantwortliche kirchliche Stelle als auch die Ehrenamtlichen selbst vor große Herausforderungen, die zum Teil auch daraus resultieren, dass sämtliche Anforderungen des Datenschutzes auch für Ehrenamtliche gelten. In Folge dessen haben den BfD EKD im Berichtszeitraum verschiedene Anfragen aus dem Bereich des ehrenamtlichen Handelns erreicht.

Im Bereich der ehrenamtlichen Tätigkeit wird häufig außer Acht gelassen, dass die **kirchliche Stelle** aus datenschutzrechtlicher Sicht auch für ihre Ehrenamtlichen voll **verantwortlich** ist. Verstößt ein Ehrenamtlicher in Ausübung seiner Tätigkeit gegen datenschutzrechtliche Bestimmungen, wird der kirchlichen Stelle dessen Handeln zugerechnet. Im eigenen Interesse sollte eine kirchliche Stelle daher umfassend prüfen, welche Personen sie mit einem Ehrenamt, das den Zugang zu personenbezogenen Daten beinhaltet, betraut.

Zu **Beginn der ehrenamtlichen Tätigkeit** sind die Ehrenamtlichen wie auch alle übrigen Beschäftigten,

die personenbezogene Daten verarbeiten, auf das **Datengeheimnis zu verpflichten**. Um das Verantwortungsbewusstsein und die Bereitschaft von Ehrenamtlichen zu stärken, sollte die verantwortliche kirchliche Stelle die Ehrenamtlichen zu Beginn der Tätigkeit auch darauf hinweisen, dass die kirchliche Stelle selbst für den Umgang mit den personenbezogenen Daten verantwortlich ist und damit den Ehrenamtlichen mit der Betrauung ein hohes Maß an Vertrauen entgegengebracht wird.

Während der **Ausübung der ehrenamtlichen Tätigkeit** gelangen in vielen Fällen personenbezogene Daten in den **häuslichen Bereich** der Ehrenamtlichen. Dies ist für die verantwortliche kirchliche Stelle stets mit Risiken verbunden, da in diesem Fall ihre Kontrollmöglichkeiten bezüglich des datenschutzkonformen Umgangs mit den Daten erheblich eingeschränkt werden. In vielen Fällen werden beispielsweise E-Mails, die teilweise sensible personenbezogene Daten enthalten, an private E-Mail-Accounts von Ehrenamtlichen verschickt. Bei privaten E-Mail-Accounts ist jedoch in der Regel kein gleichwertiges Schutzniveau gegeben. Auch besteht das Risiko, dass private und dienstliche E-Mails miteinander vermischt werden und Unbefugte Einsicht nehmen können. Um den Versand an private E-Mail-Accounts zu verhindern, ist zu empfehlen, den Ehrenamtlichen **dienstliche E-Mail-Postfächer** zur Verfügung zu stellen. Darüber hinaus sollte mit den Ehrenamtlichen eine Vereinbarung dahingehend getroffen werden, dass sie für ihre ehrenamtliche Tätigkeit ausschließlich das zur Verfügung gestellte Postfach mittels eines Webbrowsers auf ihrem privaten Notebook oder Smartphone verwenden. Die **privaten Endgeräte** werden in diesem Fall lediglich als „Sichtfenster und Tastatur“ genutzt. Dienstliche Daten werden dabei nicht auf den privaten Endgeräten gespeichert. Zwar sind bei einer solchen Vorgehensweise nicht alle datenschutzrechtlichen und sicherheitstechnischen Fragen geklärt. Sie birgt aber deutlich weniger Risiken als auf privaten Geräten gespeicherte dienstliche Daten.

Die Risiken, die mit der Herausgabe von personenbezogenen Daten verbunden sind, können sich auch bei der **Beendigung der ehrenamtlichen Tätigkeit** realisieren. So beschäftigte sich der BfD EKD im Rahmen einer Anfrage mit dem Ausscheiden eines Gemeindeglieds, das langjährig in einem gemeindlichen Leitungsgremium mitgewirkt hat. Nach dem Ausscheiden verlangte die Leitung der Kirchengemeinde verschiedene Unterlagen von dem Ehrenamtlichen zurück, um diese datenschutzkonform vernichten zu können. Dazu gehörte auch die **Rückgabe eines elektronischen Datenträgers,** auf dem sensible personenbezogene Daten gespeichert waren. Trotz mehrfacher Aufforderungen zur Rückgabe durch die Kirchengemeinde und den örtlich Beauftragten für den Datenschutz kam der Ehrenamtliche dem nicht nach. In dem geschilderten Fall musste zunächst geklärt werden, ob das Handeln des ausgeschiedenen Ehrenamtlichen, der weiterhin personenbezogene Daten der Kirchengemeinde verwendete, noch der Kirchengemeinde zugerechnet werden konnte oder ob er als eigene verantwortliche Stelle anzusehen war. Sofern angenommen wurde, dass der Ehrenamtliche als eigene verantwortliche Stelle galt, war weiter zu fragen, ob er der kirchlichen oder der staatlichen Datenschutzaufsicht unterfällt. Die daraufhin angesprochene staatliche Aufsichtsbehörde sah im konkreten Fall jedoch weiterhin die Zuständigkeit der kirchlichen Aufsichtsbehörde als gegeben an. Eine fortgesetzte Verwendung von personenbezogenen Daten durch ausgeschiedene Ehrenamtliche sei Ausfluss einer früheren ehrenamtlichen Tätigkeit für eine kirchliche Stelle. Damit sei weiterhin die kirchliche Aufsichtsbehörde zuständig. Da die Weiterverwendung der personenbezogenen Daten durch den Ehrenamtlichen aufgrund seines Ausscheidens aus dem Amt nicht mehr zulässig war, konnte der Kirchengemeinde letztendlich nur empfohlen werden, den Rechtsweg zu beschreiten und die Dokumente bzw. den elektronischen Datenspeicher mit den personenbezogenen Daten heraus zu verlangen.

Die beim BfD EKD eingegangenen Anfragen zeigen deutlich, dass das Gelangen von personenbezogenen Daten in den häuslichen Bereich der Ehrenamtlichen für die verantwortliche Stelle sowohl während der ehrenamtlichen Arbeit als auch nach dem Ausscheiden aus dem Amt mit **Risiken** verbunden ist. Die verantwortliche Stelle sollte daher prüfen, ob die Herausgabe von Dokumenten, elektronischen Speichergeräten und Ähnlichem tatsächlich zur Aufgabenerfüllung der Ehrenamtlichen erforderlich ist oder ob im Einzelfall auch eine Einsichtnahme in die personenbezogenen Daten ausreichend ist. Alternativ ist auch eine technische Lösung in Form einer **digitalen Plattform** denkbar, auf der sich Ehrenamtliche, Beschäftigte oder auch Gemeindeglieder unter Angabe des Benutzernamens und eines Kennworts

anmelden können. Den jeweiligen Benutzern können dann die Daten zur Verfügung gestellt werden, die sie für ihre Arbeit benötigen. Bei der technischen Realisierung einer digitalen Plattform muss beachtet werden, dass Ehrenamtlichen in der Regel keine dienstlichen Geräte zur Verfügung stehen und sie daher mit ihren privaten Geräten auf die Plattform zugreifen werden. In einigen Landeskirchen und diakonischen Werken wurde bereits die Umsetzung solcher digitalen Plattformen realisiert.

Die Beachtung der datenschutzrechtlichen Bestimmungen im Bereich der ehrenamtlichen Tätigkeit stellt sowohl die verantwortlichen kirchlichen Stellen als auch die Ehrenamtlichen vor großen Herausforderungen. Der BfD EKD beabsichtigt daher zukünftig mehr Weiterbildungsangebote und Gesprächskreise speziell auch für Ehrenamtliche anzubieten.

Telefonverzeichnis auf der Internetseite

Ein **ehemaliger Mitarbeiter** einer kirchlichen Verwaltungsstelle beschwerte sich beim BfD EKD darüber, dass sein Name noch mehrere Jahre nach seinem Ausscheiden im **Telefonverzeichnis** auf der **Internetseite** seines ehemaligen Arbeitgebers genannt wurde und über Suchmaschinen auffindbar war.

Wenngleich eine Veröffentlichung eines Telefonverzeichnisses von Beschäftigten zur Aufgabenerfüllung im kirchlichen Interesse im Einzelfall rechtmäßig sein kann, so entfällt dieser Zweck spätestens mit der **Beendigung des jeweiligen Arbeitsverhältnisses**. Die entsprechenden Daten sind nach § 21 DSG-EKD zu löschen.

Erst im Rahmen der Beschwerdebearbeitung wurde der verantwortlichen Stelle bewusst, dass auf ihrer Internetseite nicht nur das aktuelle Telefonverzeichnis, sondern zusätzlich die Vorgängerversionen einsehbar waren.

Fazit: Die verantwortlichen kirchlichen und diakonischen Stellen müssen die Angaben von Beschäftigtendaten auf ihren Internetseiten regelmäßig prüfen und gegebenenfalls in ihrem Löschkonzept berücksichtigen.

Anforderungen an die Aktenvernichtung

Neben den Anforderungen des Datenschutzes bei der Löschung automatisiert verarbeiteter Daten darf auch die Vernichtung von analogen Daten (Papierakte) nicht aus dem Blickfeld geraten. Hierbei gibt es einige Fragen und Unsicherheiten, die im Berichtszeitraum in Anfragen verschiedener Einrichtungen zum Ausdruck kamen.

Papierakten, die personenbezogene Daten enthalten, dürfen nicht im normalen Hausmüll entsorgt werden. Es muss die sogenannte **DIN 66399 „Büro-und Datentechnik – Vernichtung von Datenträgern“** beachtet werden. Dort werden drei Schutzklassen (normal, hoch und sehr hoch) und sieben Sicherheitsstufen definiert. Üblich ist die Vernichtung von Papierakten mithilfe von Aktenvernichtern („Schreddern“), die es in verschiedenen Sicherheitsausführungen gibt. Je vertraulicher die Daten sind, desto höher ist auch der Schutzbedarf, der bei der Vernichtung zu beachten ist. Es ist dann ein Gerät mit einer höheren Sicherheitsstufe einzusetzen. Beispielsweise ist für Personal- und Finanzdaten der Einsatz eines Gerätes mit Sicherheitsstufe P-4 und für die Vernichtung von Gesundheitsdaten mindestens ein Gerät der Stufe P-5 erforderlich.

Möchte eine kirchliche oder diakonische Stelle die Aktenvernichtung an einen **externen Dienstleister** auslagern, dann wird dieses Unternehmen als Auftragsverarbeiter tätig. Folglich muss neben dem Geschäftsbesorgungs- bzw. Dienstleistungsvertrag noch ein Vertrag zur Auftragsverarbeitung gemäß § 30 DSG-EKD geschlossen werden. Bei der Frage der Datenträgervernichtung ist auf die geltende DIN-Norm und die Klassifizierung der vorhandenen Daten in die entsprechenden Schutzklassen hinzuweisen.

Ein weiterer zu beachtender Aspekt ist der Ort der Vernichtung. Werden Akten erst in eine Entsorgungsfirma transportiert und dort vernichtet, so muss auch beim **Transport und bei der nachfolgenden Lagerung** sichergestellt sein, dass kein unbefugter Zugriff bis zur endgültigen Vernichtung erfolgen kann. Dies kann z. B. durch speziell verschließbare Container realisiert werden. Ein Nachweis der Firmen über die Einhaltung der oben genannten Normen sollte durch ein geeignetes Zertifikat wie z. B. vom TÜV SÜD nachgewiesen werden.

Zusätzlich müssen bei der Erstellung eines **Entsorgungskonzeptes** immer auch etwaige gesetzliche Regelungen (z. B. Aufbewahrungspflichten oder Löschungsfristen) beachtet werden.

Ausblick

Beim Blick nach vorne ...

... fallen mir als Datenschützer einige Themen ein, die in Nach-Corona-Zeiten wieder in den Vordergrund rücken müssen. Dann werden die Debatten um rechtliche und ethische Fragen bei den Themen Künstliche Intelligenz, Big Data oder Gesichtserkennung wieder neu aufgegriffen und Diskussionen um Zukunftstechnologien neue Herausforderungen im Datenschutz mit sich bringen.

Aber dessen ungeachtet beschäftigt mich seit meinem Dienstantritt vor knapp acht Jahren ein anderes „weiches" Datenschutz-Thema, dessen Vernachlässigung unsere Gesellschaft in den letzten Jahren bereits spürbar verändert hat. Ich rede vom Verschwinden der Privatheit und des Geheimnisses! Und dabei meine ich nicht die großen Geheimnisse, denen man durch Forschung und Wissenschaft auf die Spur kommen kann. Ich meine die persönlichen Geheimnisse einer und eines jeden Einzelnen von uns. Diese zum Menschsein dazugehörenden Geheimnisse ziehen sich kulturell und anthropologisch durch die Menschheitsgeschichte und sind mehr und mehr „vom Aussterben bedroht".

Wie häufig habe ich in den letzten Jahren – oft von jüngeren Leuten und vor allem beim Einsatz neuer Technologien – zur Rechtfertigung eines geringeren Schutzes der Privatsphäre den Satz gehört: „Ich habe doch nichts zu verbergen!" Ich kann diesen Satz als Mensch und Datenschützer nicht mehr hören. Regelmäßig antworte ich darauf mit einem einzigen Wort: „Schade!"

Damit in Zeiten der dringend erforderlichen uneingeschränkten Aufklärung und Aufarbeitung von sexueller Gewalt auch in unserer Kirche keine Missverständnisse entstehen: Ich spreche vom freien und selbstverantworteten Geheimnis eines erwachsenen Menschen, das nicht der Vertuschung und Verdeckung einer Straftat oder eines grenzüberschreitenden Verhaltens dient. Jede Instrumentalisierung des Geheimnisschutzes widerspricht in eklatanter Weise der Würde eines jeden Menschen, unseren christlichen Grundüberzeugungen und der Intention und dem Geist des Datenschutzes.

Neben theologischen, soziologischen, philosophisch-anthropologischen und kulturhistorischen Zugängen zum Thema „Geheimnis" gibt es sogar einen rechtlichen Zugang. Das Geheimnis ist in unserem Rechtssystem an vielen Stellen geschützt. Denken wir an das Steuergeheimnis und das Bankgeheimnis. Bei der ärztlichen Schweigepflicht steht die Verletzung sogar unter Strafe. Und im kirchlichen Bereich stehen das Seelsorge- und das Beichtgeheimnis seit jeher unter einem besonderen Schutz. Im Datenschutz unterstreicht das Datengeheimnis, dass die unbefugte Verarbeitung von personenbezogenen Daten untersagt ist.

In diesem Sinne wünsche ich mir beim Blick nach Vorne: Ermutigen wir Menschen ihre Privatheit zu schützen und verschaffen wir dem frei verantworteten Geheimnis wieder den Stellenwert, der ihm gebührt. Denn schließlich verkündigen wir als Christinnen und Christen mit dem leeren Grab am Ostersonntag vom größten Geheimnis aller Zeiten!

https://datenschutz.ekd.de