Der Beauftragte für den Datenschutz
der Evangelischen Kirche in Deutschland

1. Tätigkeitsbericht 2015 / 2016

Herausgegeben vom

Beauftragten für den Datenschutz
der Evangelischen Kirche in Deutschland

Böttcherstraße 7
30419 Hannover

Tel. 0511 7681280
Fax 0511 76812820
info@datenschutz.ekd.de

Diesen Tätigkeitsbericht können Sie auch auf unserer Webseite abrufen unter
https://datenschutz.ekd.de

1. Tätigkeitsbericht

des Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland

für die Jahre 2015 und 2016

vorgelegt im Dezember 2016

Redaktionsschluss 31. Oktober 2016

INHALTSVERZEICHNIS

Vorwort

Datenschutz – Quo vadis? Diese Frage ist nicht ganz leicht zu beantworten. Im Ganzen lässt sich in allen praktischen, rechtlichen und politischen Bereichen vor allem in den letzten Jahren eine verstärkte Wahrnehmung und Beschäftigung mit dem Thema Datenschutz feststellen. Dabei haben die weltweit öffentlich und medial Aufsehen erregenden Geschichten um Edward Snowden und Julian Assange wie ein beschleunigender Motor für das Thema Datenschutz gewirkt. Aber auch im öffentlich weniger spektakulären Bereich vergeht kaum eine Woche, in der das Thema Datenschutz nicht präsent ist. Und erst recht im beruflichen und privaten Bereich schwingt das Thema ständig mit. Alles in allem ist der Dornröschenschlaf, den der moderne Datenschutz in seinem Mutterland zwischen dem sogenannten Volkszählungsurteil im Jahr 1983 und den Ereignissen nach dem 11. September 2001 weitgehend geführt hat, seit Jahren beendet. Vielmehr noch! Es werden intensive gesellschaftliche und politische Debatten geführt, und nicht wenige Datenschützer bezeichnen den „Datenschutz als den Umweltschutz des neuen Jahrtausends". Genau wie beim Umweltschutz geht es um den Schutz einer Lebensgrundlage, die in Gefahr ist: Es geht um den Schutz der Privatsphäre eines jeden Einzelnen!

Gerade in Zeiten terroristischer Bedrohungen für unsere Gesellschaften muss der Staat Sicherheit und Freiheit, Überwachung und Privatheit ständig aufs Neue ins Gleichgewicht bringen. Dabei kann der in letzter Zeit häufig zu hörende Satz „Keine Freiheit ohne Sicherheit" genauso gut umgekehrt gedacht werden. Doch auch neben dieser Bedrohung der Privatheit im Verhältnis zwischen dem Staat und dem Einzelnen ist die Privatheit des Einzelnen durch datensammelnde global handelnde Unternehmen in vielfältiger Weise in Gefahr. Beim Nutzen von Diensten im Internet genauso wie beim Nutzen von alltäglichen Gebrauchsgegenständen, die mit dem Internet verbunden sind - wie zum Beispiel Smartphones oder (moderne) Autos und (moderne) Haushaltsgegenstände -, werden ständig sehr große Mengen an Daten gesammelt und zusammengeführt. Diese unter dem Begriff „Big Data" stehende Entwicklung schreitet vor dem Hintergrund der schier grenzenlosen Speicherkapazitäten zügig voran und wird dem Endverbraucher immer wieder „schmackhaft" gemacht mit dem Versprechen der Optimierung einer speziell auf seine Bedürfnisse zugeschnittenen Nutzung der Dienste.

Demgegenüber ist es in der Europäischen Union im Mai diesen Jahres nach jahrelangen Bemühungen nunmehr zur gesetzlichen Regulierung dieser Entwicklungen mit dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung gelungen, in allen Mitgliedsstaaten ein einheitliches Datenschutzrecht zu verankern. Trotz vielerlei (berechtigter) Kritik kann dieser rechtlich-formale Aspekt neben den inhaltlichen Regelungsgegenständen im Blick auf die einheitliche Entwicklung des Datenschutzes in Europa nicht hoch genug gewertet werden. Auch inhaltlich konnte sich Deutschland mit seinen hohen Datenschutzstandards in vielen Punkten durchsetzen. Mit Art. 91 Europäische Datenschutz-Grundverordnung erhalten die evangelische und die römisch-katholische Kirche in Deutschland nun erstmalig eine gesetzliche Grundlage, eigenes (kirchliches) Datenschutzrecht setzen und dieses Recht mit eigenen (kirchlichen) Aufsichtsbehörden kontrollieren zu dürfen.

Dabei hat der Datenschutz in den christlichen Kirchen im Blick auf das Seelsorgegeheimnis und das Beichtgeheimnis eine jahrhundertelange – auch rechtliche – Tradition. Aus dieser Tradition heraus hat der Schutz der Daten von Gemeindegliedern und Mitarbeitenden und der Schutz der Daten von Menschen, die kirchliche Einrichtungen in Anspruch nehmen, für die Kirchen vor dem Hintergrund des kirchlichen Auftrags und des christlichen Menschenbildes von jeher eine besondere Bedeutung. Seine rechtliche Grundlage findet der Datenschutz in der evangelischen Kirche im EKD-Datenschutzgesetz. Zukünftig müssen wir beim Umgang mit dem Thema Datenschutz gerade als Kirche auch theologische und ethische Aspekte stärker in den Blick nehmen, Fragen stellen und nach Antworten suchen.

Auch das Thema Datenschutzaufsicht ist in der evangelischen Kirche nicht neu. So gab es bereits seit dem Inkrafttreten des ersten EKD-Datenschutzgesetzes im Jahr 1978 in den Gliedkirchen und bei der Diakonie eine funktionierende, kirchliche Datenschutzaufsicht. Mit meiner Berufung zum Beauftragten für den Datenschutz der EKD zum 01. Januar 2014 nehmen wir in Kirche und Diakonie die Datenschutzaufsicht in einer neuen Struktur und Organisation unter dem Dach der EKD stärker gemeinsam wahr und sind im Prozess der weiteren Professionalisierung und Vereinheitlichung unserer Arbeit. In den letzten drei Jahren haben 16 Gliedkirchen und sechs diakonische Landesverbände sowie die gliedkirchlichen Zusammenschlüsse die Datenschutzaufsicht auf die EKD übertragen. Die aus diesem Grund mit meiner Berufung neu installierte Dienststelle umfasst zwischenzeitlich 15 Mitarbeitende an vier deutschlandweiten Standorten. Die drei Hauptaufgaben unserer Arbeit sehen wir in den Bereichen Aufsicht, Beratung und Weiterbildung. Dabei widmen wir uns neben Fragen des rechtlichen Datenschutzes und der Organisation des Datenschutzes nunmehr auch verstärkt dem Aspekt des technischen Datenschutzes. Verschlüsselung stellt eine wichtige Maßnahme zur Sicherstellung des technischen Datenschutzes dar. Hier sehen wir im kirchlichen und diakonischen Bereich einen deutlichen Handlungsbedarf. Im Ganzen wollen wir im Rahmen unserer Aufgaben zur Verbesserung des kirchlichen Datenschutzes beitragen, indem wir beratend helfen und unterstützen, Mitarbeitende und Ehrenamtliche weiterbilden und jeden Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird!

Knapp drei Jahre nach meinem Dienstantritt und gut zwei Jahre nach der Vorlage eines ersten Sachstandsberichts zum Aufbau meiner Dienststelle lege ich zu Beginn des Jubiläumsjahres „500 Jahre Reformation“ den ersten ordentlichen Tätigkeitsbericht vor. Der Bericht beinhaltet zunächst eine kurze Darstellung über die Entwicklungen im Datenschutzrecht. Der Schwerpunkt liegt danach auf der Darstellung der Aufgabenerledigung meiner Dienststelle. Ergänzt und abgerundet wird der Bericht mit Erläuterungen zum Aufbau und zur Struktur meiner Dienststelle sowie zu den weiteren Aufgaben.

Vor dem Hintergrund vielfältiger rechtlicher, technischer und praktischer Herausforderungen ist das Thema Datenschutz gerade auch im Bereich von Kirche und Diakonie eine immer wieder an der Würde des Menschen auszurichtende Aufgabe. An dieser Aufgabe mitzuwirken, werde ich mich zusammen mit allen Mitarbeitenden in meiner Dienststelle als kirchliche Datenschutzaufsichtsbehörde weiterhin sehr gerne stellen!

Hannover, im Dezember 2016

Michael Jacob

Der Beauftragte für den Datenschutz
der Evangelischen Kirche in Deutschland

Über die Entwicklung des Datenschutzes

I

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 neuen Herausforderungen!

In der evangelischen Kirche

Die Ursprünge des kirchlichen Datenschutzes liegen von jeher in den (kirchenrechtlichen) Regelungen zum Seelsorge- und Beichtgeheimnis. Seit der Etablierung eines modernen staatlichen Datenschutzes in den 70er- und 80er-Jahren des letzten Jahrhunderts steht der kirchliche Datenschutz in einem engen Bezug zu den staatlichen Regelungen im Bundesdatenschutzgesetz, den Datenschutzgesetzen der Bundesländer sowie dem staatlichen Melderecht. Dort wird gefordert, dass die öffentlich-rechtlichen Religionsgesellschaften „ausreichende Datenschutzmaßnahmen" treffen müssen, wenn sie von öffentlichen Stellen personenbezogene Daten erhalten wollen (§ 15 Abs. 4 Bundesdatenschutzgesetz). Wortgleiche Regelungen finden sich in dem am 01. Mai 2015 in Kraft getretenen Bundesmeldegesetz (§ 42 Abs. 5 Bundesmeldegesetz) sowie dem bis dahin geltenden Melderechtsrahmengesetz (§ 19 Abs. 5 Melderechtsrahmengesetz). Da das kirchliche Meldewesen auf den von den staatlichen Meldebehörden übermittelten Daten basiert, müssen die Kirchen damit einen dem staatlichen Recht vergleichbaren Datenschutz vorweisen.

Das erste bereits im Jahr 1977 in Kraft getretene Datenschutzgesetz der EKD wurde in der Folgezeit immer wieder geändert oder neugefasst. Am 01. Januar 2013 trat die Neufassung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz - DSG-EKD) in Kraft (ABl.EKD 2013, S. 2). Damit wurde das kirchliche Datenschutzrecht an technische Entwicklungen und rechtliche Vorgaben angepasst. Das DSG-EKD gilt unmittelbar in allen Gliedkirchen der EKD, ohne dass es von den jeweiligen Synoden der Gliedkirchen beschlossen werden muss. Unabhängig davon können die Gliedkirchen für ihren Bereich zusätzlich Durchführungsbestimmungen und ergänzende Bestimmungen erlassen, soweit sie dem DSG-EKD nicht widersprechen.

Die Novellierung des DSG-EKD erfolgte vor allem im Lichte der Diskussion über den Vorschlag der Europäischen Kommission für eine „Verordnung des Europäischen Parlaments und des Rats zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogenen Daten und zum freien Datenverkehr" (Datenschutz-Grundverordnung). Dieser Entwurf wurde seit Anfang 2012 diskutiert, wobei für die beiden großen Kirchen in Deutschland die Frage im Vordergrund stand, ob ihre in Europa einmalige eigene Regelungskompetenz dieser Rechtsmaterie erhalten bleibt. Um das zu gewährleisten, mussten die kirchlichen Regelungen auf jeden Fall im Einklang mit dem Schutzniveau der EU-Verordnung stehen und eine völlig unabhängige Datenschutzaufsicht gewährleisten.

In diesem Zusammenhang hatte der Europäische Gerichtshof bereits in seinem Urteil vom 09. März 2010 verlangt, dass Datenschutzaufsichtsbehörden in größtmöglicher Eigenständigkeit und Unabhängigkeit handeln müssen. Dies hatte zu Änderungen beim Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen geführt. Auch deshalb war erforderlich, im DSG-EKD eine – vor allem auch institutionell sichtbare – stärkere Unabhängigkeit der Beauftragten für den Datenschutz sicherzustellen.

Die in den §§ 18, 18a und 18b DSG-EKD enthaltenen Regelungen für die Datenschutzbeauftragten innerhalb der EKD tragen diesen Überlegungen Rechnung. Jetzt stehen die Beauftragten für den Datenschutz einer eigenen Behörde vor und die Ausübung des Amtes geschieht „in organisatorischer und sachlicher Unabhängigkeit" (§ 18 Abs. 4 DSG-EKD). Diese Neuerungen sollen die Stellung des Datenschutzbeauftragten stärken und seine institutionelle Unabhängigkeit hervorheben. In Anlehnung an staatliche Bestimmungen gilt jetzt auch, dass Datenschutzbeauftragte die Befähigung zum Richteramt oder zum höheren Dienst besitzen müssen (§ 18 Abs. 3 DSG-EKD).

Die weitreichendste organisatorische Neuregelung besteht darin, dass die Gliedkirchen der EKD, sofern sie nicht selbst Beauftragte für den Datenschutz bestellen, deren Aufgaben dem oder der Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland übertragen können (§ 18 Abs. 1 DSG-EKD). Dieser gesetzlichen Möglichkeit, die Datenschutzaufsicht auf die EKD zu übertragen, war ein kirchen- und diakoniepolitischer Meinungsbildungsprozess vorausgegangen, die Datenschutzaufsicht zukünftig unter dem Dach der EKD stärker gemeinsam und einheitlich wahrzunehmen.

Einzelheiten zur praktischen Umsetzung und Ausgestaltung der Neuregelung der Datenschutzaufsicht innerhalb der EKD finden sich im zweiten Kapitel dieses Berichtes.

Neben weiteren Gesetzesänderungen (vor allem im Bereich der Organisation des Datenschutzes) wurde mit dem neu eingefügten § 9 Abs. 2 DSG-EKD das Thema IT-Sicherheit gesetzlich verbindlich geregelt und jede kirchliche Stelle verpflichtet, IT-Sicherheit zu gewährleisten. Nach einem längeren Beratungsprozess hat der Rat der EKD am 29. Mai 2015 zur weiteren Konkretisierung die Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung ITSVO-EKD) erlassen.

In der römisch-katholischen Kirche

Auch in der römisch-katholischen Kirche gilt mit der Anordnung über den kirchlichen Datenschutz (KDO) ein eigenes kirchliches Datenschutzrecht. Die KDO wurde zuletzt 2013 überarbeitet. Sie gilt jetzt in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 18.11.2013. Im Gegensatz zum Datenschutzgesetz der EKD muss die KDO von jedem Bischof für sein (Erz-)Bistum in Kraft gesetzt und im jeweiligen Amtsblatt bekannt gemacht werden. Dieser Prozess ist inzwischen abgeschlossen. Die Gründe für die Überarbeitung der KDO waren ähnlich wie bei der Novellierung des DSG-EKD. Insbesondere wurden die Bestimmungen über die Bestellung des Diözesandatenschutzbeauftragten, seine Rechtsstellung und seine Aufgaben überarbeitet. Es besteht die Möglichkeit, für mehrere Bistümer einen gemeinsamen Datenschutzbeauftragten zu bestellen.

Vor diesem Hintergrund haben die folgenden (Erz-)Bistümer zwischenzeitlich gemeinsame Diözesandatenschutzbeauftragte bestellt:

- Hamburg, Hildesheim und Osnabrück, Münster (oldenburgischer Teil) - Dienstsitz: Bremen
- Berlin, Magdeburg, Dresden-Meißen, Erfurt und Görlitz – Dienstsitz: bei Magdeburg
- Auf dem Gebiet des Bundeslandes Nordrhein-Westfalen (in der Rechtsform einer Körperschaft des öffentlichen Rechts) - Dienstsitz: Dortmund
- Schließlich ist bereits seit längerer Zeit für die (Erz-)Bistümer auf dem Gebiet des Freistaats Bayern ein gemeinsamer Diözesandatenschutzbeauftragter tätig.
- Die übrigen (Erz-)Bistümer ordnen die Datenschutzaufsicht gegenwärtig ebenfalls neu.

Im März 2015 hat die Rechtskommission des Verbands der Diözesen Deutschlands eine neue Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) beschlossen, die nunmehr in den (Erz-)Bistümern in Kraft zu setzen ist. Darin werden unter anderem Regelungen zur Gewährleistung der IT-Sicherheit, zur Nutzung privater Datenverarbeitungsanlagen zu dienstlichen Zwecken sowie zu Maßnahmen zu besonderen Gefährdungslagen (Fernwartung, Auftragsdatenverarbeitung u.a.) getroffen.

In der Bundesrepublik Deutschland

Datenschutzgesetzgebung des Bundes und der Länder

Am 01. Januar 1978 ist in der Bundesrepublik Deutschland das Bundesdatenschutzgesetz in Kraft getreten. Das Bundesdatenschutzgesetz hat seitdem zum Ziel, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Das Bundesdatenschutzgesetz regelt den Datenschutz bei der Datenverarbeitung der öffentlichen Stellen des Bundes und der nicht-öffentlichen Stellen (in der Privatwirtschaft und damit bei allen Unternehmen). Das Bundesdatenschutzgesetz wurde zuletzt durch das zweite Gesetz zur Änderung des Bundesdatenschutzgesetzes – Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund - und Errichtung einer obersten Bundesbehörde vom 25. Februar 2015 novelliert.

Entsprechend der föderalen Struktur der Bundesrepublik Deutschland regeln die Landesdatenschutzgesetze den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen des Landes, den Gemeinden und Gemeindeverbänden sowie den sonstigen juristischen Personen des öffentlichen Rechts, die der Aufsicht des Landes unterstehen.

Die staatlichen Datenschutzgesetze haben für die Ausgestaltung des kirchlichen Datenschutz(rechts) stets Vorbildwirkung entfaltet. Diese Wirkung resultiert aus § 15 Abs. 4 Bundesdatenschutzgesetz, wonach bei den Kirchen „ausreichende Datenschutzmaßnahmen" sichergestellt sein müssen, wenn ihnen durch öffentliche Stellen personenbezogene Daten übermittelt werden sollen. Die Landesdatenschutzgesetze haben entsprechende Bestimmungen. Für die Datenübermittlungen vom staatlichen ins kirchliche Meldewesen sind ausreichende Datenschutzmaßnahmen bei den Kirchen somit eine unabdingbare Voraussetzung.

Bundesmeldegesetz

Nach Änderung des Bundesmeldegesetzes (BMG) vom 03. Mai 2013 (BGBl I 2013, S. 1084) durch Art. 9 des Gesetzes vom 02. Februar 2015 (BGBl I 2015, S. 130) trat die jetzige Fassung des BMG am 01. November 2015 in Kraft. Damit ist die Meldedatenübermittlung an die öffentlich-rechtlichen Religionsgesellschaften jetzt bundesrechtlich geregelt. In § 42 BMG ist im Einzelnen aufgeführt, welche Daten die Meldebehörden den öffentlich-rechtlichen Religionsgesellschaften von deren Mitgliedern (§ 42 Abs. 1 BMG) und von den Familienangehörigen der Mitglieder (§ 43 Abs. 2 BMG) regelmäßig übermitteln dürfen. Die Regelung nimmt die Bestimmung auf, die bislang in § 19 Melderechtsrahmengesetz und den darauf basierenden Bestimmungen in den Landesmeldegesetzen enthalten waren. Der Datenkatalog wurde geringfügig erweitert. Da nunmehr auch Daten über eingetragene Lebenspartnerschaften an die Kirchen übermittelt werden, hat der Gesetzgeber durch das Gesetz vom 02. Februar 2015 in § 42 Abs. 1 BMG eine Formulierung eingefügt, die ausdrücklich klarstellt, dass die Datenübermittlung zur Erfüllung der Aufgaben der Religionsgesellschaften erfolgt, „nicht jedoch zu arbeitsrechtlichen Zwecken". Die beiden Kirchen hatten im Verlauf der Gesetzesberatung allerdings bereits erklärt, dass sie dies ohnehin so handhaben würden, weil sonst auch nach dem kirchlichen Datenschutzrecht eine nicht gerechtfertigte Datennutzung vorliegen würde (vgl. § 5 Abs. 5 DSG-EKD). Durch das neue Gesetz werden auch datenschutzrechtliche Fragestellungen von grundsätzlicher Natur aufgeworfen. Wie bisher schon ist eine Datenübermittlung nur dann zulässig, wenn sichergestellt ist, dass beim Datenempfänger ausreichend Maßnahmen zum Datenschutz getroffen sind. Die Feststellung darüber trifft eine durch Landesrecht zu bestimmende Behörde. Aus grundsätzlichen Erwägungen haben sich die Kirchen dafür verwendet, dass diese Feststellung – wie bisher – durch die zuständigen Landesministerien und nicht die Landesdatenschutzbeauftragten getroffen wird. Dort, wo die Länder die Neuregelung zum Anlass nehmen, die Feststellung eines ausreichenden Datenschutzes bei den Kirchen erneut zu treffen, wurde insbesondere nach kirchlichen

Datenschutzbestimmungen und Datenschutzkonzepten sowie nach der Struktur und Unabhängigkeit der Datenschutzaufsichtsbehörden gefragt.

Kirchliche Datenschutzmaßnahmen stehen darüber hinaus auch im Zusammenhang mit der neuen Form der Datenübertragung zwischen den staatlichen Meldebehörden und den kirchlichen Stellen unter besonderer Aufmerksamkeit. Im Berichtszeitraum wurden die Voraussetzungen dafür geschaffen, dass die Datenübermittlung zwischen den Meldebehörden und den Kirchen nur noch elektronisch nach dem Standard OSCI-XMeld erfolgt. Dieser Standard wird bereits bei Datenübermittlungen zwischen staatlichen Stellen verwendet und wurde um eine Komponente für die Datenübermittlung an die Kirchen erweitert. Auf der Grundlage eines Beschlusses des Arbeitskreises I der Innenministerkonferenz kommt dieser Standard seit dem 01. November 2015 nun zum Einsatz. Im Mai 2016 hat es eine einmalige Bestandsdatenübermittlung gegeben (§42 Abs. 4a BMG). Die Teilnahme der Kirchen an diesem Verfahren setzt ebenfalls einen ausreichenden und an den staatlichen Vorgaben für das Meldewesen orientierten Datenschutz voraus.

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

Der Sicherheit der IT-Infrastrukturen wird im staatlichen Bereich bereits seit einiger Zeit erhöhte Aufmerksamkeit geschenkt. Schon der Koalitionsvertrag vom 27. November 2013 legte fest: „Wir schaffen ein IT-Sicherheitsgesetz mit verbindlichen Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen und die Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle".

Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz vom 17. Juli 2015, BGBl I 2015, S. 1324), das am 25. Juli 2015 in Kraft trat, wurde diese Ankündigung eingelöst. Das Gesetz soll vor allem dazu dienen, die IT-Sicherheit bei Unternehmen zu verbessern sowie das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu stärken und dessen Aufgaben zu erweitern. Während die Betreiber von Atomkraftwerken, öffentlichen Telekommunikationsnetzen und Telekommunikationsdiensten unmittelbar von den Regelungen des Gesetzes (Meldepflichten bei Sicherheitsvorfällen, Einhaltung eines Mindeststandards gemäß Vorgabe des BSI) betroffen sind, wird das IT-Sicherheitsgesetz für andere Betreiber kritischer Infrastrukturen (Energie, Transport und Verkehr, Gesundheitswesen, Wasserversorgung, Ernährung, Finanz- und Versicherungswesen) erst dann wirksam, wenn das Bundesministerium des Innern in einer Rechtsverordnung festgelegt hat, welche Einrichtungen als kritische Infrastrukturen im Sinne des IT-Sicherheitsgesetzes gelten. Vorher sind unter anderem die betroffenen Betreiber anzuhören. Eine entsprechende Rechtsverordnung ist bisher nicht in Kraft. Auch eine Anhörung kirchlicher Betreiber betroffener Strukturen – was allenfalls im Gesundheitswesen denkbar wäre – ist noch nicht erfolgt.

Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl I 2015, S. 2218) wurde eine – seit langem umstrittene – Regelung zur zeitlich befristeten Speicherung von Verkehrsdaten zur Strafverfolgungsvorsorge und zur Gefahrenabwehr (sogenannte Vorratsdatenspeicherung) geschaffen. Mit dem Gesetz will der Gesetzgeber die Anliegen von Strafverfolgung und Gefahrenabwehr auf der einen sowie die Beachtung des Rechts auf informationelle Selbstbestimmung auf der anderen Seite im Lichte des Urteils des Bundesverfassungsgerichts zur Vorratsdatenspeicherung vom 02. März 2010 berücksichtigen und ins richtige Verhältnis setzen. Kernstück des Gesetzes ist die Verpflichtung für die Erbringer öffentlich zugänglicher Kommunikationsdienste, Verbindungsdaten (etwa die Rufnummern der beteiligten Anschlüsse sowie Beginn und Ende der Kommunikation) für zehn Wochen zum Zwecke der Strafverfolgung und zur Gefahrenabwehr zu speichern. Sogenannte Standortdaten müssen vier Wochen gespeichert werden. Staatliche Stellen können unter den engen Voraussetzungen eines Richtervorbehalts während der Speicherfrist auf diese Daten zugreifen.

Von der Speicherpflicht ausgenommen sind Verbindungen zu Anschlüssen von Personen, Behörden oder Organisationen im sozialen und kirchlichen Bereich, die den grundsätzlich anonym bleibenden Anrufern (ausschließlich oder überwiegend) telefonische Beratung in seelischen oder sozialen Notlagen anbieten – also z.B. die Telefonseelsorge.

Berufsgeheimnisträger sind von der Speicherung ihrer Verkehrsdaten nicht ausgenommen. Das Gesetz legt aber fest, dass die Strafverfolgungsbehörden Verkehrsdaten aller Personen, denen nach § 53 StPO ein Zeugnisverweigerungsrecht zusteht – also auch Geistliche im Hinblick auf das, was ihnen in ihrer Eigenschaft als Seelsorger anvertraut oder bekannt geworden ist – nicht erheben dürfen. Zufallsfunde unterliegen dem Verwertungsverbot.

Nach Inkrafttreten des Gesetzes wurden verschiedene Klagen beim Bundesverfassungsgericht eingereicht. Auch nach Ansicht der staatlichen Datenschutzbeauftragten räumt das neue Gesetz die erheblichen Bedenken gegen die Vorratsdatenspeicherung nicht aus. Es bleibt abzuwarten, ob die Neuregelung der gerichtlichen Überprüfung standhalten wird.

Datenschutzaufsicht des Bundes und der Länder

Am 19. Dezember 2013 hat der Deutsche Bundestag Andrea Voßhoff zur Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt. Am 06. Januar 2014 hat sie dieses Amt von ihrem Vorgänger Peter Schaar übernommen.

In das erste Amtsjahr der neuen Bundesbeauftragten fiel die Erarbeitung des Zweiten Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund durch Errichtung einer obersten Bundesbehörde. Die Bundesregierung hatte dazu im Sommer 2014 einen Gesetzesentwurf vorgelegt und damit die Konsequenz aus dem Urteil des Europäischen Gerichtshofs zur Unabhängigkeit der österreichischen Datenschutzkommission aus dem Jahr 2012 gezogen. Da die österreichische Rechtskonstruktion, auf welche sich das Urteil bezog, der deutschen Konstruktion sehr ähnlich war, gab es Handlungsbedarf. Das Gesetz wurde schließlich noch im Dezember 2014 im Bundestag beschlossen und im März 2015 im Bundesgesetzblatt verkündigt (BGBl I 2015, Nr. 7, S. 162). Es ist am 01. Januar 2016 in Kraft getreten. Die wichtigste Neuerung besteht darin, dass der oder die Bundesbeauftragte eine oberste Bundesbehörde ist und damit vollständig aus dem Bundesministerium des Inneren herausgelöst wird. Der oder die Bundesbeauftragte unterliegt nur noch der politischen Kontrolle durch den Deutschen Bundestag. Deutschland erfüllt somit die europäischen Anforderungen an die Unabhängigkeit der Datenschutzaufsicht.

Im Blick auf die im Urteil des Europäischen Gerichtshofs geforderte Unabhängigkeit der Datenschutzaufsicht wurden auch in den Datenschutzgesetzen der Bundesländer (zum Beispiel § 21 Niedersächsisches Datenschutzgesetz) entsprechende gesetzliche Anpassungen zur Unabhängigkeit und Eigenständigkeit der Datenschutzaufsichtsbehörden vorgenommen.

In allen Bundesländern - außer in Bayern - sind die Datenschutzbeauftragten seit einigen Jahren zugleich auch die Aufsichtsbehörden für den nicht-öffentlichen Bereich. In Bayern existieren weiterhin zwei getrennte Ämter: Der Bayerische Landesbeauftragte für den Datenschutz für den öffentlichen Bereich (mit Sitz in München) und das Landesamt für Datenschutz für den nicht-öffentlichen Bereich (mit Sitz in Ansbach).

In der Europäischen Union

Europäische Datenschutz-Grundverordnung

Nach vierjährigen Verhandlungen in den Organen der Europäischen Union ist die Europäische Datenschutz-Grundverordnung (EU-DSGVO) am 14. April 2016 vom Europaparlament beschlossen worden und am 25. Mai 2016 in Kraft getreten. Die EU-DSGVO löst damit die EU-Datenschutzrichtlinie von 1995 ab. Im Gegensatz zu Richtlinien, die von den einzelnen Mitgliedsstaaten in nationales Recht umgesetzt werden müssen, gilt die EU-DSGVO unmittelbar in allen Mitgliedsstaaten der Europäischen Union. Nach einer Übergangszeit von zwei Jahren nach Inkrafttreten der EU-DSGVO wird somit ab dem 25. Mai 2018 in allen Mitgliedsstaaten der Europäischen Union ein einheitliches Datenschutzrecht gelten.

Neben der notwendigen Modernisierung des Datenschutzrechts soll die EU-DSGVO sowohl die Position der Bürger verbessern – unter anderem dadurch, dass ein sogenanntes Recht auf Vergessenwerden (Art. 17 EU-DSGVO) eingeführt wird – als auch für die Wirtschaft Vorteile bringen. Dieser ist vor allem wichtig, dass künftig das sogenannte Marktortprinzip gilt (Art. 3 EU-DSGVO). Damit werden in allen Mitgliedsstaaten der Europäischen Union einheitliche Standards eingeführt.

Eine Anpassung oder Aufhebung nationaler Bestimmungen muss in dem Übergangszeitraum von zwei Jahren nach Inkrafttreten der Verordnung erfolgen. In Deutschland werden bis zu 300 Bundesgesetze angepasst werden müssen. Außerdem werden teilweise Konkretisierungen durch Bundes- und Ländergesetzgebung notwendig werden.

Für die evangelische und die römisch-katholische Kirche in Deutschland ist nach umfangreichen Bemühungen erreicht worden, dass sie auch künftig ein eigenes Datenschutzrecht anwenden und eine eigene Datenschutzaufsicht haben können. Diese Rechte finden ihre gesetzliche Grundlage in Artikel 91 EU-DSGVO:

> ***Artikel 91***
> ***Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften***
>
> *(1) Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedsstaat 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.*

In einer Arbeitsgruppe des Kirchenamtes der EKD werden zurzeit Vorschläge zur Anpassung des DSG-EKD erarbeitet. Es ist geplant, der Synode der EKD im November 2017 ein entsprechendes Änderungsgesetz zur Beschlussfassung vorzulegen. Einzelheiten zu den gesetzlichen Auswirkungen im staatlichen und kirchlichen Bereich können deshalb erst in einem künftigen Bericht mitgeteilt werden.

Europäischer Gerichtshof

Im Berichtszeitraum hat der Europäische Gerichtshof zudem mehrere Grundsatzurteile gefällt, die von großer Bedeutung für den Datenschutz sind:

Mit Urteil vom 08. April 2014 (C-293/12 und V-594/12) hat der Europäische Gerichtshof die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsnetze erzeugt oder verarbeitet werden, für ungültig erklärt. Er hat dabei festgestellt, dass die Vorratsdatenspeicherung von Daten, um mögliche schwere Kriminalität zu bekämpfen, zwar eine dem Gemeinwohl dienende Aufgabe ist, beim Erlass der Richtlinie aber der Grundsatz der Verhältnismäßigkeit überschritten wurde (vor allem zu lange Speicherung und zu weiter Straftatenkatalog). Der deutsche Gesetzgeber hat darauf mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist reagiert.

Zum Recht auf Vergessen in Suchmaschinen hat der Europäische Gerichtshof am 15. Mai 2014 ein Urteil gefällt (C-131/12 – Google Spain und Google). Im Kern geht es darum, dass Suchmaschinenbetreiber dazu verpflichtet werden, unter bestimmten Voraussetzungen von der Ergebnisliste, die im Anschluss an eine anhand eines Namens einer Person durchgeführten Suche angezeigt wurde, Links zu entfernen, sofern diese auf von Dritten veröffentlichte Internetseiten verweisen. Es ist unerheblich, ob die Information auf diesen Internetseiten gleichzeitig gelöscht wird. Dabei ist auch abzuwägen, wie das Verhältnis der Grundrechte der betroffenen Person zum Informationsinteresse der Öffentlichkeit ist - dies insbesondere dann, wenn es sich um eine „Person des öffentlichen Lebens“ handelt.

Große Aufmerksamkeit erlangte das Urteil des Europäischen Gerichtshofs zum sogenannten Safe Harbour-Abkommen (Urteil vom 06. Oktober 2015, C-362/14 (RS Schrems)). Das Abkommen, das streng genommen nur eine Entscheidung der EU-Kommission war, die nach Verhandlungen mit den USA getroffen wurde, wurde für ungültig erklärt. Es diente seit dem Jahr 2000 den Unternehmen in den Mitgliedsstaaten der Europäischen Union als Rechtsgrundlage für Datenübermittlungen in die USA. Der Europäische Gerichtshof hielt das Abkommen für unvereinbar mit dem europäischen Datenschutzrecht und hat dies im Wesentlichen damit begründet, dass US-Unternehmen nach US-Recht den Geheimdiensten im großen Umfang Zugriff auf personenbezogene Daten gewährten. Die USA sei somit gerade kein „sicherer Hafen“ für europäische Daten. Seitens der Europäischen Union bestand daher großes Interesse, den dadurch entstandenen Zustand der Rechtsunsicherheit so schnell wie möglich zu beenden. Am 12. Juli 2016 ist das Nachfolgeabkommen EU-US Privacy Shield in Kraft getreten.

Der Europäische Gerichtshof hat schließlich am 19. Oktober 2016 ein Urteil zu dynamischen IP-Adressen gefällt (C-582/14, (RS Patrick Breyer / Bundesrepublik Deutschland)). Er hat darin festgestellt, dass eine dynamische IP-Adresse ein personenbezogenes Datum sein kann, wenn ein Webseitenbetreiber, der die Adresse speichert, über die rechtlichen Mittel verfügt, die es ihm erlauben, den betreffenden Benutzer zu bestimmen. Er muss also die Möglichkeit haben an Zusatzinformationen zu gelangen, über die nur der Internetzugangsanbieter des Nutzers verfügt.

II

Über die Datenschutzaufsicht in der evangelischen Kirche

Mit Wirkung zum 01. Januar 2014 hat der Rat der Evangelischen Kirche in Deutschland Michael Jacob zum Beauftragten für den Datenschutz der EKD berufen, der seitdem für weite Teile der evangelischen Kirche die Datenschutzaufsicht wahrnimmt. In einigen Gliedkirchen gibt es weiterhin eigene Beauftragte für den Datenschutz.

Rahmenbedingungen

Vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofes zur Unabhängigkeit von Datenschutzaufsichtsbehörden wurden mit der Novellierung des EKD-Datenschutzgesetzes zum 01. Januar 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.

---

§ 18

Rechtsstellung der Beauftragten für den Datenschutz

(1) Die Evangelische Kirche in Deutschland, ihre Gliedkirchen und ihre gliedkirchlichen Zusammenschlüsse bestellen je für ihren Bereich Beauftragte für den Datenschutz, soweit die Wahrnehmung nicht nach § 18b Absatz 1 übertragen worden ist.

(2) 1 Die Amtszeit soll mindestens vier, höchstens acht Jahre betragen und setzt sich bis zum Amtseintritt der Nachfolge fort. 2 Die erneute Bestellung ist zulässig. 3 Die Tätigkeit ist hauptamtlich auszuüben. 4 Nebentätigkeiten sind nur zulässig, soweit dadurch das Vertrauen in die Unabhängigkeit und Unparteilichkeit nicht gefährdet wird und die Voraussetzungen der §§ 46 bis 48 des Kirchenbeamtengesetzes der EKD erfüllt sind.

(3) 1 Zu Beauftragten für den Datenschutz dürfen nur Personen bestellt werden, welche die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. 2 Sie müssen die Befähigung zum Richteramt oder zum höheren Dienst besitzen. 3 Sie müssen einer Gliedkirche der Evangelischen Kirche in Deutschland angehören. 4 Die beauftragte Person ist auf die gewissenhafte Erfüllung ihrer Amtspflichten und die Einhaltung der kirchlichen Ordnung zu verpflichten.

(4) 1 Die Beauftragten für den Datenschutz stehen einer eigenen Behörde vor und sind in Ausübung ihres Amtes an Weisungen nicht gebunden und nur dem kirchlichen Recht unterworfen. 2 Die Ausübung des Amtes geschieht in organisatorischer und sachlicher Unabhängigkeit. 3 Die Dienstaufsicht ist so zu regeln, dass dadurch die Unabhängigkeit nicht beeinträchtigt wird. 4 In der Ausübung ihres Amtes dürfen sie nicht behindert und wegen ihres Amtes als Beauftragte für den Datenschutz weder benachteiligt noch begünstigt werden.

(...)

§ 18a

Der oder die Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland

Der Rat der Evangelischen Kirche in Deutschland bestellt für den Bereich der Evangelischen Kirche in Deutschland und ihres Evangelischen Werkes für Diakonie und Entwicklung sowie für die gesamtkirchlichen Werke und Einrichtungen eine oder einen Beauftragten für den Datenschutz.

§ 18b

Beauftragte für den Datenschutz der Gliedkirchen der Evangelischen Kirche in Deutschland

(1) Die Gliedkirchen der EKD und ihre gliedkirchlichen Zusammenschlüsse bestellen einzeln oder gemeinschaftlich Beauftragte für den Datenschutz, soweit deren Aufgaben nicht dem oder der Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland übertragen werden.

(2) Die Gliedkirchen der EKD können bestimmen, dass für ihren diakonischen Bereich besondere Beauftragte für den Datenschutz bestellt werden.

Der Beauftragte für den Datenschutz der EKD

Der Beauftragte für den Datenschutz der EKD (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 am Ende des Berichtszeitraums nach vertraglicher Übertragung für 16 Gliedkirchen, die gliedkirchlichen Zusammenschlüsse und im Bereich von sechs diakonischen Landesverbänden wahr. Zur Wahrnehmung der gesetzlich normierten sowie der vertraglich 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)". Diese Behörde wird von der Person des Beauftragten geleitet und hat ihren Hauptsitz in Hannover. Vier Gliedkirchen (vergleiche Abbildung 1) und mehrere diakonische Landesverbände nehmen die Datenschutzaufsicht weiterhin eigenständig wahr.

Seit dem 01. Januar 2014 haben die nachfolgenden Gliedkirchen und gliedkirchlichen Zusammenschlüsse sowie diakonischen Landesverbände die Datenschutzaufsicht vertraglich auf die EKD übertragen (Stand: 31. Oktober 2016):

- Baden
- Berlin-Brandenburg-schlesische Oberlausitz
- Bremen
- Hessen und Nassau
- Lippe
- Oldenburg
- Rheinland
- Westfalen
- Bayern
- Braunschweig
- Hannover
- Kurhessen-Waldeck
- Mitteldeutschland
- Reformiert
- Schaumburg-Lippe
- Württemberg

- Union Evangelischer Kirchen in der EKD (UEK)
- Herrnhuter Brüdergemeine
- Vereinigte Evangelisch-Lutherische Kirche Deutschlands (VELKD)
- Konföderation evangelischer Kirchen in Niedersachsen

- Diakonisches Werk Berlin-Brandenburg-schlesische Oberlausitz e.V.
- Diakonisches Werk in Hessen und Nassau und Kurhessen-Waldeck e.V.
- Diakonisches Werk Rheinland-Westfalen-Lippe e.V.
- Diakonisches Werk Bremen e.V.
- Diakonisches Werk der Ev.-Luth. Kirche in Oldenburg e.V.
- Diakonisches Werk der evangelischen Kirche in Württemberg e.V.

Darüber hinaus zeichnet sich ab, dass weitere diakonische Landesverbände Interesse haben, die Datenschutzaufsicht in absehbarer Zeit auf die EKD zu übertragen.

Die Vertragsverhandlungen werden für die EKD auf Grundlage eines Mustervertrages vom Kirchenamt der EKD geführt.

Die Datenschutzregionen des BfD EKD

Zur regionalen Gliederung der vertraglich 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 wurde eine Außenstelle errichtet (Nord: Hannover; Ost: Berlin; Süd: Ulm; Mitte-West: Dortmund). Die regionale Zuordnung ist der folgenden Karte zu entnehmen.

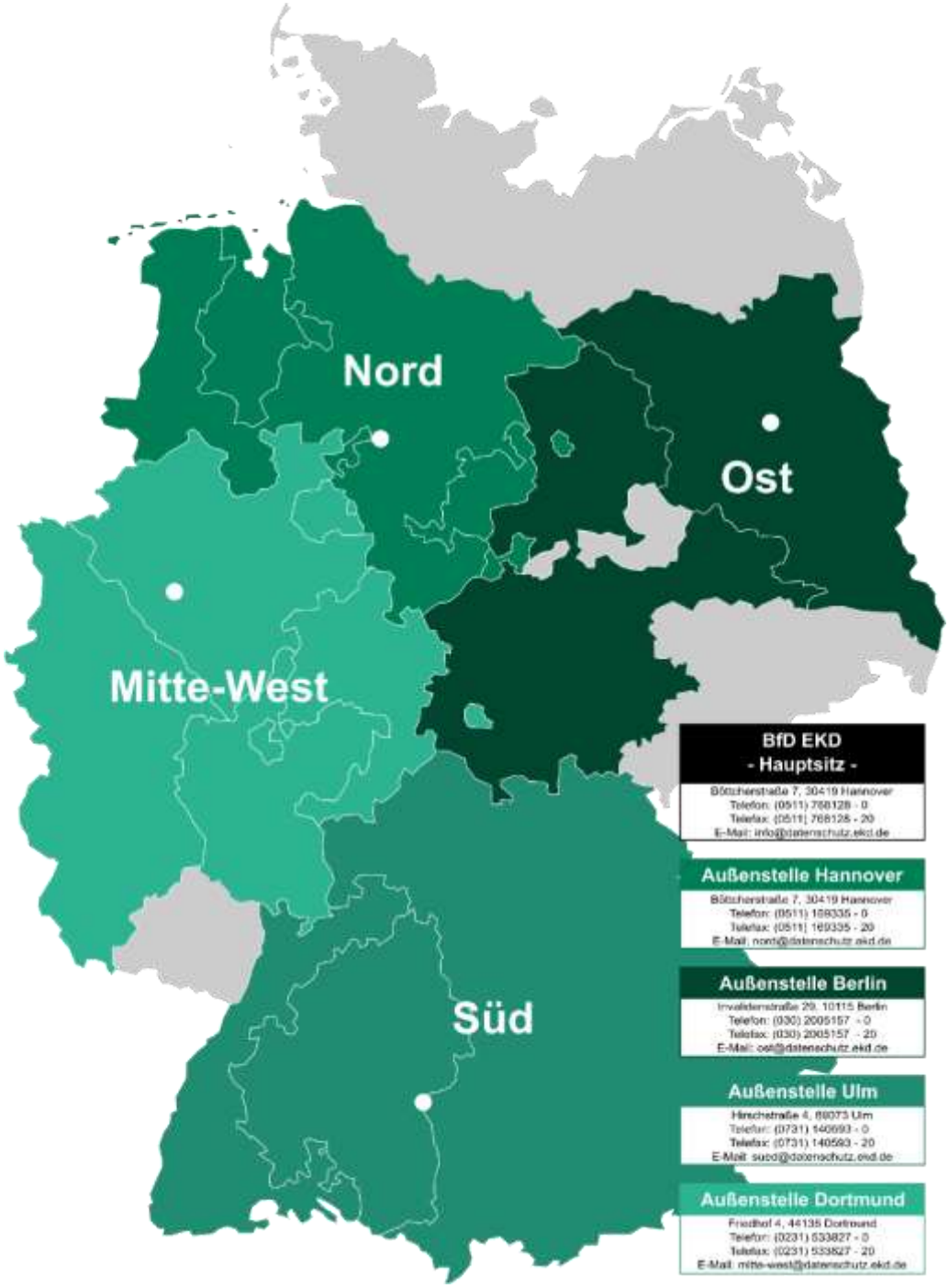

Abb. 1: Karte mit Datenschutzregionen und Außenstellen
(Die Gliedkirchen mit eigenständiger Datenschutzaufsicht sind grau hinterlegt.)

Die Dienststelle des BfD EKD

Im Rahmen des Aufbaus der Dienststelle wurde im Jahr 2014 eine komplette sachliche, technische und rechtliche Behördeninfrastruktur aufgebaut. Der personelle Aufbau der Dienststelle erfolgt(e) sukzessive entsprechend der tatsächlichen Aufgaben und der finanziellen Ausstattung der Dienststelle. Die Dienststelle zählt zurzeit sechzehn Mitarbeitende. Die Aufbauorganisation des BfD EKD zum 31. Oktober 2016 ist dem folgenden Organigramm zu entnehmen.

Abb. 2: Organigramm des BfD EKD (Stand 31. Oktober 2016)

Die Kosten der Dienststelle (Personal- und Sachkosten) werden durch Umlagen finanziert. Die Umlagen werden im Bereich verfasste Kirche und im Bereich Diakonie durch zwei getrennte Schlüssel ermittelt.

Einzelheiten zur (sachlichen, technischen, rechtlichen) Infrastruktur, zu Personal und Finanzen sowie zu sonstigen Aspekten der Dienststelle des BfD EKD sind im vierten Kapitel zu finden.

III

Über die Aufgaben und die Tätigkeit des BfD EKD

Die Aufgaben sind vielfältig! In Erfüllung des gesetzlichen Auftrags wacht der BfD EKD über die Einhaltung des Datenschutzes. Dabei will er vor allem beraten, helfen und unterstützen. Zu den Aufgaben des Beauftragte für den Datenschutz gehört aber auch, die Einhaltung des Datenschutzes zu kontrollieren und zu überwachen. Über allem Handeln steht dabei der Zweck jedes modernen Datenschutzes: Jeder Einzelnen ist davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. In diesem Kapitel wird umfassend über die Aufgaben und Tätigkeiten des BfD EKD als Datenschutzaufsichtsbehörde informiert.

Überblick

Der BfD EKD ist inhaltlich in den Bereichen rechtlicher Datenschutz, technischer Datenschutz und Organisation des Datenschutzes tätig. Mehr als in der Vergangenheit werden seit Errichtung der Dienststelle des BfD EKD auch alle wichtigen Aspekte des technischen Datenschutzes bearbeitet und nach vorne gebracht. Sämtliche Tätigkeiten des BfD EKD im Rahmen seiner Datenschutzaufsicht sind den drei Aufgaben Aufsicht, Beratung und Weiterbildung zugeordnet. Eine grobe Übersicht über die Tätigkeiten des BfD EKD ist der folgenden Aufgaben-Tätigkeitsmatrix zu entnehmen:

Tabelle 1: Aufgaben-Tätigkeitsmatrix für den 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
Bearbeiten von Beschwerden	X	X	X						
Etablieren einer (pro-)aktiven Datenschutzaufsicht	X	X	X						
Materialdienst (standardisierte Beratung)				X	X	X			
einzelfallbezogen	X	X	X	X	X	X			
einheitliches und aufeinander abgestimmtes (modulares) Weiterbildungsangebot für Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz							X	X	X
individuelles Angebot für andere Zielgruppen							X	X	X
schwerpunktsetzend	X	X	X	X	X	X	X	X	X

Neben den regelmäßigen Aufgaben (Aufsicht, Beratung, Weiterbildung) beschäftigt sich der BfD EKD mit dem Thema Datenschutz auch unter Berücksichtigung von vier Schwerpunktthemen (Kinder und Jugendliche, Mitarbeitende, Ehrenamt und Diakonie). Jede Außenstelle bearbeitet ein Schwerpunktthema. Ziel ist es, zu jedem Schwerpunktthema spezielles Expertenwissen zu erlangen und vorzuhalten. Zurzeit werden für jedes Schwerpunktthema Konzepte erarbeitet, wie das Thema unter Berücksichtigung von datenschutzrechtlichen Aspekten zukünftig behandelt werden soll.

Mit Sachstandsbericht vom September 2014 hatte der BfD EKD dem Rat der EKD erste grundsätzliche Überlegungen zu den Aufgaben und Herausforderungen für die Dienststelle des BfD EKD vorgelegt. Im weiteren Verlauf dieses Tätigkeitsberichts wird am Beginn der Ausführungen zu den Aufgaben Aufsicht, Beratung und Weiterbildung auf die entsprechenden Ausführungen im Sachstandsbericht 2014 Bezug genommen. Die sonstigen Aufgaben des BfD EKD werden im vierten Kapitel dieses Berichts dargestellt.

Tabelle 2: Statistik über die Anzahl der Tätigkeiten im Jahr 2015 (Stand 31. Dezember 2015)

	Aufsicht	Beratung	Weiterbildung	Summe
Hauptstelle	11	43	12	66
AS Hannover	6	79	3	88
AS Berlin	5	73	14	92
AS Ulm	22	125	2	149
AS Dortmund	8	97	3	108
Summe	52	417	34	503

Tabelle 3: Statistik über die Anzahl der Tätigkeiten im Jahr 2016 (Stand 31. Oktober 2016)

	Aufsicht	Beratung	Weiterbildung	Summe
Hauptstelle	9	45	16	70
AS Hannover	15	91	4	110
AS Berlin	12	75	4	91
AS Ulm	18	182	16	216
AS Dortmund	30	160	11	201
Summe	84	553	51	688

Aufsicht

Zum Thema Aufsicht wird im Sachstandsbericht des BfD EKD auf den Seiten 18 und 19 ausgeführt:

> *„Im Rahmen einer ersten internen Bestandsaufnahme stellte sich heraus, dass Datenschutzaufsicht im engeren Sinne bisher überwiegend ‚reaktiv' wahrgenommen wurde; d. h. die Datenschutzbeauftragten haben auf Anfragen und Beschwerden entsprechend reagiert. Zukünftig soll die Datenschutzaufsicht stärker auch ‚aktiv' wahrgenommen werden. (...)*
>
> *Zur Umsetzung einer aktiven Datenschutzaufsicht soll in einer ersten Phase im Rahmen von sog. strukturierten Datenschutzgesprächen mit Landeskirchenämtern / Konsistorien / Diakonischen Spitzenverbänden eine Bestandsaufnahme zum Thema Datenschutz durchgeführt werden."*

Im Rahmen der Etablierung einer (pro-)aktiven Datenschutzaufsicht ist beabsichtigt, in einem dreijährigen Rhythmus mit allen (Landes-) Kirchenämtern / Konsistorien / Oberkirchenräten und diakonischen Spitzenverbänden, die die Datenschutzaufsicht auf die EKD übertragen haben, sogenannte „große" strukturierte Datenschutzgespräche zu führen. Diese Gespräche werden auf Seiten des BfD EKD vom Beauftragten und / oder seinem Vertreter zusammen mit der oder dem Regionalverantwortlichen aus der zuständigen Außenstelle geführt. Es wird gebeten, dass als Gesprächspartner die Dienststellenleitung oder der zuständige Vorstand sowie die oder der Datenschutzreferent und die oder der Betriebsbeauftragte oder örtlich Beauftragte für den Datenschutz und die oder der IT-Leitende zur Verfügung stehen. Weitere Gesprächsteilnehmer können hinzugezogen werden. Die Gespräche werden in der „ersten" Runde auf der Grundlage eines im Vorfeld zugeschickten Fragebogens geführt. Am Ende werden Handlungsempfehlungen ausgesprochen und Verabredungen getroffen. In den Jahren 2015 und 2016 haben die ersten „großen" strukturierten Datenschutzgespräche stattgefunden. Es ist geplant, bis Ende 2017 im ersten dreijährigen Rhythmus 28 „große" strukturierte Datenschutzgespräche zu führen. Im Berichtszeitraum wurden bereits folgende Gespräche geführt:

- Kirchenamt der EKD
- Konsistorium der Ev. Kirche Berlin-Brandenburg-schlesische Oberlausitz
- Landeskirchenamt der Ev.-Luth. Landeskirche Schaumburg-Lippe
- Landeskirchenamt der Ev. Kirche von Westfalen
- Oberkirchenrat der Ev. Landeskirche in Baden
- Landeskirchenamt der Ev.-Luth. Kirche in Bayern
- Landeskirchenamt der Ev.-luth. Landeskirche in Braunschweig
- Landeskirchenamt der Ev. Kirche in Mitteldeutschland
- Evangelisches Werk für Diakonie und Entwicklung e.V.
- Landeskirchenamt der Ev. Kirche Kurhessen-Waldeck
- Diakonisches Werk Berlin-Brandenburg-schlesische Oberlausitz e.V.
- Diakonisches Werk der evangelischen Kirchen in Württemberg e.V.
- Landeskirchenamt der Lippischen Landeskirche

In der Zeit zwischen den „großen" strukturierten Datenschutzgesprächen führen die Außenstellen des BfD EKD mit den Handelnden vor Ort sogenannte „kleine" strukturierte Datenschutzgespräche.

Um auch im Bereich des technischen Datenschutzes eine (pro-)aktive Datenschutzaufsicht zu etablieren, sind erste automatische Tests für die Überprüfung von Transportverschlüsselungen durch den BfD EKD entwickelt worden. Der BfD EKD beabsichtigt, diese automatisierten Tests in Zukunft in regelmäßigen Abständen durchzuführen und die Ergebnisse zur Verfügung zu stellen. Es ist geplant, weitere automatisierte Tests zu entwickeln und durchzuführen.

Wie in der Vergangenheit wurden die im Berichtszeitraum eingegangenen Beschwerden und Eingaben ordnungsgemäß bearbeitet. Einzelheiten sind den folgenden Ausführungen in diesem Kapitel zu entnehmen.

Hauptsitz

Im Bereich des aufsichtlichen Handelns des BfD EKD sind neben der Wahrnehmung einer aktiven Datenschutzaufsicht insbesondere eingehende Beschwerden zu bearbeiten. Um zu vermeiden, dass Beschwerden entstehen, verfolgt der BfD EKD das Ziel, kirchliche Stellen und diakonische Einrichtungen datenschutzrechtlich frühzeitig zu beraten und zu schulen. Im Ganzen erreichten den Hauptsitz somit deutlich weniger Beschwerden als Beratungsanfragen.

Zuständigkeit

Im Berichtszeitraum wurde immer wieder die Frage gestellt, ob der Beauftragte für den Datenschutz der EKD (bzw. eine andere evangelische Datenschutzaufsichtsbehörde) zuständig sei oder eine staatliche Datenschutzaufsichtsbehörde. Voraussetzung für die Zuständigkeit einer evangelischen Datenschutzaufsichtsbehörde ist die in § 1 Abs. 2 Satz 1 DSG-EKD geregelte Geltung des DSG-EKD. Neben den juristischen Personen des öffentlichen und des privaten Rechts im Bereich der verfassten Kirche und der Diakonie ist die Frage der Zuordnung zum kirchlichen Bereich, insbesondere von privatrechtlichen Rechtssubjekten, nicht immer einfach und leicht zu beantworten. In diesem Zusammenhang ist es gemäß § 1 Abs. 2 Satz 3 DSG-EKD die gesetzliche Aufgabe der Gliedkirchen und der EKD jeweils für ihren Bereich eine Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit zu führen, für die das DSG-EKD gilt. Dem BfD EKD kommt dabei keine eigene Prüfungs- und Entscheidungskompetenz zu, welche kirchlichen Werke und Einrichtungen dem kirchlichen Bereich zuzuordnen sind und somit unter die Datenschutzaufsicht des BfD EKD fallen. Der BFD EKD ist zu diesen Übersichten mit allen Gliedkirchen und der EKD im Kontakt, damit die Übersichten beim BfD EKD zukünftig immer auf dem aktuellen Stand vorliegen.

Mitteilungen im Amtsblatt

Im Rahmen einer Beschwerde über die Veröffentlichung des Verlusts der Rechte aus der Ordination im (analogen) Amtsblatt und in der Onlineversion des Amtsblattes wurde festgestellt, dass es für die Veröffentlichung in der Onlineversion des Amtsblattes keine Rechtsgrundlage gab. Somit war die Personalnachricht über den Verlust der Ordinationsrechte aus der Onlineversion des Amtsblattes zu entfernen. Zwischenzeitlich hat der Gesetzgeber eine entsprechende Rechtsgrundlage geschaffen.

Strukturierte Datenschutzgespräche

Bei den strukturierten Datenschutzgesprächen im Kirchenamt der EKD und im Evangelischen Werk für Diakonie und Entwicklung wurde anhand des vorab entwickelten Fragebogens der Status Quo des Datenschutzes erörtert. Dabei wurden im Kirchenamt auch Fragen zur Organisation des Datenschutzes besprochen und Hinweise zur Etablierung eines örtlich Beauftragten für den Datenschutz gegeben.

Darüber hinaus haben der BfD EKD und der Vertreter des Beauftragten mit Unterstützung der jeweiligen Regionalverantwortlichen im Berichtszeitraum weitere elf strukturierte Datenschutzgespräche geführt, die in der jeweiligen Datenschutzregion näher beschrieben werden.

Datenschutzregion Nord

Im Bereich des aufsichtlichen Handelns des BfD EKD sind neben der Wahrnehmung einer aktiven Datenschutzaufsicht insbesondere eingehende Beschwerden zu bearbeiten. Um zu vermeiden, dass Beschwerden entstehen, verfolgt der BfD EKD das Ziel, kirchliche Stellen und diakonische Einrichtungen datenschutzrechtlich frühzeitig zu beraten und zu schulen. Im Ganzen erreichten die Datenschutzregion Nord somit deutlich weniger Beschwerden als Beratungsanfragen. Beschwerden betrafen häufig den Umgang mit personenbezogenen Daten in Gemeindebriefen, Adress(-management)systemen und E-Mail-Verteilern. Im Rahmen der Aufsicht wurden in der Datenschutzregion Nord im Berichtszeitraum 13 Fälle bearbeitet. Exemplarisch werden einige Beschwerden geschildert:

Veröffentlichung im Gemeindebrief

Ein Ehepaar beschwerte sich darüber, dass trotz fehlender Einwilligung ihre Geburtsdaten im Gemeindebrief abgedruckt wurden. Das Ehepaar hatte sogar im Vorfeld einen Brief bekommen, in dem es um die Einwilligung gebeten wurde, diesen Brief beantworteten sie allerdings nicht. In der Gemeinde wurde vor dem Druck des Gemeindebriefes der Eingang der Einwilligungen nicht ordnungsgemäß überprüft. Die Gemeinde räumte den Fehler ein. In Zukunft soll besser darauf geachtet werden, dass die Einwilligungen auch tatsächlich vorliegen, bevor Geburtsdaten im Gemeindebrief abgedruckt werden.

Info-E-Mails

Ein Gemeindeglied nahm privat an einer Weiterbildung einer kirchlichen Einrichtung teil. Es erhielt im Nachgang E-Mails mit Jobangeboten. Dafür wurde im Kurs eine Einwilligung eingeholt. Per E-Mail zog das Gemeindeglied diese Einwilligung später zurück. Trotz Widerspruchs wurden die E-Mails weiter gesendet. Es handelte sich dabei um ein technisches Problem. Die Einrichtung war auch vor dem Eingang der Beschwerde schon bemüht das Problem zu beheben.

Adressmanagementsystem

In einer komplexeren Organisationseinheit wurde ein neues Adressmanagementsystem eingeführt. Daten aus dem alten System sollten synchronisiert werden. Ein Mitarbeitender bemängelte, dass der Datenbestand nicht aktuell sei und die Berechtigungsstufen nicht ordnungsgemäß verteilt seien. Tatsächlich waren Datensätze teilweise veraltet bzw. in falschen Feldern eingetragen, so dass Daten für einen größeren Personenkreis sichtbar waren als sie es hätten sein sollen. In welcher Form die Synchronisation datenschutzkonform geschehen kann, wurde in einem Vor-Ort-Termin besprochen. Es wurde im Gespräch auch festgehalten, wie wichtig die Aktualität der Datensätze und das Berechtigungskonzept sind. Ebenso wurde vereinbart, dass das System um eine Löschfunktion erweitert wird. Bisher konnten die veralteten Daten nicht dauerhaft aus dem neuen System wieder gelöscht werden. Eine neu eingestellte Mitarbeitende soll in Zukunft den Datenbestand aktualisieren und das System pflegen. Das Berechtigungskonzept wurde ebenfalls überarbeitet. Die Mitarbeitenden, die Daten ins System einpflegen können, wurden in einer Schulung gezielt auf den Datenschutz hingewiesen. In einem zweiten Termin vor Ort wurden die Ergebnisse der bisherigen Arbeit besprochen. Die Pflege der Daten muss noch abgeschlossen werden.

E-Mail-Verteiler

In einem Kirchenkreis wurde ein falscher Verteiler für das Versenden eines Protokolls genutzt. Das Protokoll wurde weder als verschlüsselte E-Mail verschickt, noch war das Protokoll an sich verschlüsselt. Zügig erfolgte durch die Leitung des Kirchenkreises die Bitte die E-Mail ungelesen zu löschen. Es erfolgte eine Mitteilung über die Datenpanne an alle Betroffenen. Durch den BfD EKD wurde angeregt, die Protokolle in Zukunft nur noch verschlüsselt zu versenden. Eine Anleitung für das Verschlüsseln von Dateien wurde zur Verfügung gestellt.

Strukturiertes Datenschutzgespräch

Bei strukturierten Datenschutzgesprächen mit dem Landeskirchenamt der Ev.-Luth. Landeskirche Schaumburg-Lippe und der Ev.-luth. Landeskirche in Braunschweig wurde jeweils die aktuelle Situation im Hinblick auf Fragen zum Datenschutz und zur Datensicherheit erfragt und die kurz-, mittel- sowie langfristige Planung diskutiert. Im Verlauf der Gespräche wurde außerdem über ein jeweils vorab vorgelegtes Datenschutzkonzept diskutiert.

Im Datenschutzgespräch wurde auch über den Aufbau sowie die Arbeit und das Selbstverständnis des BfD EKD informiert. Auch Fragen der Zusammenarbeit mit dem BfD EKD wurden besprochen.

Es ist geplant, zukünftig rechtzeitig und regelmäßig über Fortschritte und Probleme ins Gespräch zu kommen.

Datenschutzregion Ost

Im Bereich des aufsichtlichen Handelns des BfD EKD sind neben der Wahrnehmung einer aktiven Datenschutzaufsicht insbesondere eingehende Beschwerden zu bearbeiten. Um zu vermeiden, dass Beschwerden entstehen, verfolgt der BfD EKD das Ziel, kirchliche Stellen und diakonische Einrichtungen datenschutzrechtlich frühzeitig zu beraten und zu schulen. Im Ganzen erreichten die Datenschutzregion Ost somit deutlich weniger Beschwerden als Beratungsanfragen. Beschwerden betrafen in erster Linie den Umgang mit personenbezogenen Daten in kirchlichen und diakonischen Einrichtungen. Im Rahmen der Aufsicht wurden in der Datenschutzregion Ost im Berichtszeitraum 21 Fälle bearbeitet. Exemplarisch werden einige Beschwerden geschildert:

Erfassungsbogen Anmeldung Konfirmation

Ein Petent wies die Dienststelle auf den Erhebungsbogen zur Konfirmation einer Gemeinde hin. Er war der Auffassung, dass auf diesem Erhebungsbogen personenbezogene Daten genannt werden, die nicht für die Anmeldung zur Konfirmation eines Kindes erforderlich sind. Es handelte sich um einen einheitlich gestalteten Erhebungsbogen der Landeskirche. Die Landeskirche informierte den BfD EKD darüber, dass nach der Novellierung des einschlägigen Gesetzes der Erlass einer Verordnung bevorstehe. In dieser Verordnung sollen deutlich weniger personenbezogene Daten erhoben werden. Gegen die in der Verordnung geplante Erhebung von personenbezogenen Daten bestehen keine Einwände. Stichtag ist der 01.01.2017.

Videoüberwachung

Ein Petent beschwerte sich bei der Dienststelle über die fehlende Kennzeichnung der Videoüberwachung an den Dienstgebäuden einer kirchlichen Stelle. Die betreffende Stelle wurde informiert und die deutliche Kennzeichnung der Videokamera gefordert. Bei einer Ortsbegehung seitens der Außenstelle wurde die Umsetzung der geforderten Maßnahme überprüft. Anlässlich der Beschwerde wurde weiterhin festgestellt, dass die kirchliche Stelle ihrer Dokumentationspflicht gemäß § 7a Abs. 7 DSG-EKD bislang nicht

nachgekommen ist. Bei der Begehung wurden – auf Grundlage des vom BfD EKD zur Verfügung gestellten Musters – der örtlich Beauftragten Hinweise zur Ausgestaltung der Dokumentation gegeben.

Erhebungsbogen eines kirchlichen Krankenhauses

Eine Patientin beschwerte sich über einen Erhebungsbogen in der Geriatrie eines Krankenhauses. Den Patienten der geriatrischen Abteilung wurde bei der Einlieferung ein Erhebungsbogen zur sozialen wie persönlichen Situation vorgelegt. Der Erhebungsbogen beinhaltete Fragen zur Wohnsituation sowie zur finanziellen Situation der Patienten. Weiterhin wurde aber auch die persönliche Situation bis hin zum psychischen Befinden erfragt. Der Erhebungsbogen enthielt keinen Hinweis auf die Freiwilligkeit der Beantwortung der Fragen. Auch fand keine Betrachtung in Fallgruppen statt, vielmehr wurde allen Patienten der Geriatrie der gleiche Erhebungsbogen vorgelegt. Bei den Fragen zur persönlichen und finanziellen Situation handelte es sich um personenbezogene Daten, die nicht direkt mit der Behandlung im Zusammenhang standen. Sie bezogen sich vielmehr auf den Bereich der Nachsorge.

Das Krankenhaus wurde darauf hingewiesen, dass im Erhebungsbogen Hinweise zur Freiwilligkeit ergänzt werden müssen. Auch der Zweck, zu dem die personenbezogenen Daten erhoben und dann später verarbeitet werden, muss deutlich aus dem Bogen ersichtlich sein. Außerdem wurde empfohlen, auch organisatorisch die Einholung des Erhebungsbogens zu ändern und Fallgruppen zu bilden, die dem Grundsatz der Datensparsamkeit und Datenvermeidung besser gerecht werden.

Strukturierte Datenschutzgespräche

Bei strukturierten Datenschutzgesprächen mit dem Konsistorium der Ev. Kirche Berlin-Brandenburg-schlesische Oberlausitz, dem Landeskirchenamt der Ev. Kirche in Mitteldeutschland und dem Diakonischen Werk Berlin-Brandenburg-schlesische Oberlausitz e.V. wurde jeweils die aktuelle Situation im Hinblick auf Fragen zum Datenschutz und zur Datensicherheit erfragt und die kurz-, mittel- sowie langfristige Planung diskutiert. Im Verlauf der Gespräche wurde außerdem über ein jeweils vorab vorgelegtes Datenschutzkonzept diskutiert.

Im Datenschutzgespräch wurde auch über den Aufbau sowie die Arbeit und das Selbstverständnis des BfD EKD informiert. Auch Fragen der Zusammenarbeit mit dem BfD EKD wurden besprochen.

Es ist geplant, zukünftig rechtzeitig und regelmäßig über Fortschritte und Probleme ins Gespräch zu kommen.

Datenschutzregion Süd

Im Bereich des aufsichtlichen Handelns des BfD EKD sind neben der Wahrnehmung einer aktiven Datenschutzaufsicht insbesondere eingehende Beschwerden zu bearbeiten. Um zu vermeiden, dass Beschwerden entstehen, verfolgt der BfD EKD das Ziel, kirchliche Stellen und diakonische Einrichtungen frühzeitig datenschutzrechtlich zu beraten und zu schulen. Im Ganzen erreichten die Datenschutzregion Süd somit deutlich weniger Beschwerden als Beratungsanfragen. Beschwerden betrafen in erster Linie den Umgang mit personenbezogenen Daten in kirchlichen und diakonischen Einrichtungen. Im Rahmen der Aufsicht wurden in der Datenschutzregion Süd im Berichtszeitraum 40 Fälle bearbeitet. Exemplarisch werden einige Beschwerden geschildert:

Veröffentlichung im Gemeindebrief

Im Zuge der unzulässigen Veröffentlichung eines personenbezogenen Datums im örtlich verteilten Gemeindebrief schlug die betroffene Person vor, in nachfolgenden Gemeindebriefen falsche Werte für das

in Frage stehende Datum zu veröffentlichen, um so durch ein Verwirrspiel die möglichen Folgen der Veröffentlichung zu begrenzen.

Dieses Verwirrspiel lässt sich nicht mit den Bestimmungen des Datenschutzgesetzes vereinbaren, wonach personenbezogene Daten berichtigt werden müssen, wenn sie unrichtig sind. Das schließt auch eine Veröffentlichung unrichtiger Daten aus, selbst wenn die betroffene Person es als Schadensbehebungsmaßnahme vorschlägt. Auf die Frage, ob die verantwortliche Stelle auch aus anderen rechtlichen Gründen keine falschen Angaben veröffentlichen darf, kommt es in diesem Zusammenhang nicht an.

Wahl zur Vertrauensperson der Schwerbehinderten

Bei Wahlen zu Mitarbeitervertretungen werden Wählerlisten erstellt. Der Zweck, zu dem Wahlvorstände Wählerlisten erstellen und den Wahlberechtigten einsehbar machen, ist, diesen eine Kontrollmöglichkeit zu eröffnen, ob bei den dort genannten Mitarbeitenden die Voraussetzungen gegeben sind, an der Wahl teilzunehmen. Mögliche Streitigkeiten sollen schon im Vorfeld ausgeräumt werden. Am Wahltag kann nur wählen, wer in die Wählerliste eingetragen ist.

Das Datum, dass eine Person schwerbehindert ist, gehört zu den besonderen Arten personenbezogener Daten, die in erhöhtem Maße schutzwürdig sind. Die Nutzung dieser Daten ohne Einwilligung der Betroffenen setzt eine spezielle Rechtsgrundlage oder die sich aus den Normen des EKD-Datenschutzgesetz ergebende Erforderlichkeit voraus. Dabei ist stets zu beachten, dass die Nutzung personenbezogener Daten an dem Ziel auszurichten ist, so wenige personenbezogene Daten wie möglich zu nutzen.

Zur Wahl der Vertrauensperson der Schwerbehinderten sind nur schwerbehinderte Mitarbeitende berechtigt. Geregelt ist, dass die Wahl der Vertrauensperson der Schwerbehinderten „entsprechend" der Wahl der Mitarbeitervertretung durchzuführen ist. Das heißt, dass eine Wählerliste erstellt wird, die die zur Wahl der Vertrauensperson der Schwerbehinderten berechtigten Personen auflistet, diese Liste diesem Personenkreis bekannt gegeben wird und dass dafür gesorgt wird, dass an der Wahl nur teilnehmen kann, wer auf dieser Liste eingetragen ist.

Eine Bekanntgabe dieser Liste auch den nicht schwerbehinderten Mitarbeitenden geht über das Kriterium „entsprechend" hinaus und ist auch nicht erforderlich.

Vielmehr ist es als Ausdruck ihres Grundrechts auf informationelle Selbstbestimmung, dass schwerbehinderte Mitarbeitende selbst entscheiden, wen sie in welchem Umfang über ihre Behinderung informieren. Nicht alle Behinderungen sind unmittelbar wahrnehmbar, und es genügt häufig, dass Vorgesetzte oder Kollegen, mit denen eine engere Zusammenarbeit besteht, darüber informiert sind.

Allerdings müssen es die schwerbehinderten Mitarbeitenden hinnehmen, dass im Zuge der Wahl der Vertrauensperson andere schwerbehinderte Mitarbeitende mittels der Wählerliste zur Wahl der Vertrauensperson von ihrer Behinderung erfahren.

Bewerbungsunterlagen

Bewerbungsunterlagen sind grundsätzlich spätestens mit der Besetzung einer Stelle den Bewerbern, die bei der Stellenbesetzung nicht berücksichtigt worden sind, zurückzuschicken. Allerdings kann diesen Bewerbern angeboten werden, ihre Unterlagen weiter vorzuhalten, um sie im Zuge einer künftigen Stellenausschreibung nochmals zu berücksichtigen. Eine Rechtsgrundlage für die weitere Aufbewahrung von Bewerbungsunterlagen ohne Einverständnis der betroffenen Personen gibt es nicht.

Dies gilt auch für elektronisch eingegangene Bewerbungsunterlagen. Bei diesen Unterlagen muss im Rahmen des Berechtigungssystems zusätzlich sichergestellt werden, dass nur solche Mitarbeitenden Einblick nehmen können, die dies zur Erledigung ihrer Aufgaben benötigen.

Auch eine Löschung elektronisch eingegangener Bewerbungsunterlagen muss datenschutzgerecht erfolgen, d.h. ein Wiederherstellen der Bewerbungsunterlagen darf nach der Löschung nicht mehr möglich sein. Deshalb muss auch die Löschung in den Datensicherungen gewährleistet sei. Dies ist technisch häufig nicht einfach und bedarf dafür eines Löschkonzepts.

Ausscheiden von Mitarbeitenden

Eine ausgeschiedene Mitarbeiterin einer kirchlichen Sozialstation beschwerte sich darüber, dass ihre dienstliche E-Mail-Adresse auch nach ihrem Ausscheiden weiter verwendet wurde.

Zunächst wurde festgestellt, dass nicht – wie gesetzlich vorgeschrieben – ein Betriebsbeauftragter für den Datenschutz bestellt war, dass für die Wartung der EDV-Anlage und der Homepage kein Vertrag über eine Datenverarbeitung im Auftrag vorlag, die Datenschutzerklärung auf der Homepage Mängel hatte und auch kein in Grundzügen erkennbares IT-Sicherheitskonzept vorhanden war.

Das Ausscheiden von Mitarbeitenden hat eine Reihe von Datenschutzaspekten und muss im Rahmen eines organisierten Prozesses vollzogen werden. Das Postfach sollte über einen bestimmten Zeitraum weiter vorgehalten werden, damit ein Abwesenheitsassistent die Absender darüber informieren kann, wer in der Nachfolge Ansprechperson ist. Daten zur Gesundheit sollten grundsätzlich nicht automatisch weitergeleitet werden, damit sichergestellt ist, dass vertrauliche Daten nur die vom Absender gewollten Empfänger erreichen. Ist damit zu rechnen, dass Patienten, Klienten oder Betreute sich weiterhin an ausgeschiedene Mitarbeitende wenden wollen, muss eine effektive Löschregel geschaltet werden.

Strukturierte Datenschutzgespräche

Bei strukturierten Datenschutzgesprächen mit dem Oberkirchenrat der Ev. Landeskirche in Baden, dem Landeskirchenamt der Ev.-Luth. Kirche in Bayern und dem Diakonischen Werk der evangelischen Kirche in Württemberg e.V. wurde jeweils die aktuelle Situation im Hinblick auf Fragen zum Datenschutz und zur Datensicherheit erfragt und die kurz-, mittel- sowie langfristige Planung diskutiert. Im Verlauf der Gespräche wurde außerdem über ein jeweils vorab vorgelegtes Datenschutzkonzept diskutiert.

Im Datenschutzgespräch wurde auch über den Aufbau sowie die Arbeit und das Selbstverständnis des BfD EKD informiert. Auch Fragen der Zusammenarbeit mit dem BfD EKD wurden besprochen.

Es ist geplant, zukünftig rechtzeitig und regelmäßig über Fortschritte und Probleme ins Gespräch zu kommen.

Datenschutzregion Mitte-West

Im Bereich des aufsichtlichen Handelns des BfD EKD sind neben der Wahrnehmung einer aktiven Datenschutzaufsicht insbesondere eingehende Beschwerden zu bearbeiten. Um zu vermeiden, dass Beschwerden entstehen, verfolgt der BfD EKD das Ziel, kirchliche Stellen und diakonische Einrichtungen frühzeitig datenschutzrechtlich zu beraten und zu schulen. Im Ganzen erreichten die Datenschutzregion Mitte-West somit deutlich weniger Beschwerden als Beratungsanfragen. Beschwerden betrafen häufig den Umgang mit Auskunftsansprüchen sowie den Umgang mit personenbezogenen Daten bei einer Videoüberwachung. Im Rahmen der Aufsicht wurden in der Datenschutzregion Mitte-West im Berichtszeitraum 38 Fälle bearbeitet. Exemplarisch werden einige Beschwerden geschildert:

Auskunftsansprüche

Soweit sich betroffene Personen mit dem Vortrag, in ihren persönlichen Rechten verletzt worden zu sein, an den BfD EKD gewandt haben, handelte es sich oftmals um Fälle, in denen Auskunftsansprüche nicht oder nicht vollständig erfüllt wurden. Entsprechend des Prinzips der Transparenz kann jede betroffene Person Auskunft über die zu ihr gespeicherten Daten, auch soweit sie sich auf Herkunft oder empfangende Stellen dieser Daten beziehen, die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und den Zweck der Speicherung verlangen. Da von diesem Anspruch jedoch in der Praxis nicht allzu häufig Gebrauch gemacht wird, sind die verantwortlichen Stellen teilweise nicht vorbereitet oder unwissend, wie der Anspruch ordnungsgemäß zu gewähren ist.

Soweit die verantwortliche Stelle sich diesem Anspruch erstmalig ausgesetzt sieht, kann die Gewährung der gewünschten Informationen mit erheblichem Aufwand verbunden sein. Bevor die vollständigen Informationen zusammengetragen werden, hat die verantwortliche Stelle darüber zu befinden, wie sie sich hinsichtlich der Identität des Antragstellers verhält. Sofern verantwortliche Stellen mit dem Verfahren nicht vertraut sind, kann es passieren, dass diese den ersten Schritt, nämlich die fehlerfreie Identifikation des Antragstellers, nicht ordnungsgemäß durchführen. Hierauf ist jedoch besonderes Augenmerk zu legen, da es datenschutzrechtlich höchst problematisch wäre, personenbezogene Daten an Unberechtigte zu übermitteln und so gleichsam selber einen erheblichen Datenschutzverstoß zu verursachen. Im besten Fall ist von einem persönlich eingereichten Antrag mit persönlicher Übergabe einer (teilweise geschwärzten) Kopie des Personalausweises sowie der dokumentierten Zustellung an eine verifizierte Adresse auszugehen. Auch bei der Zusammenstellung der vollständigen Informationen kommt es teilweise zu Problemen. Es handelt sich eben nicht nur um die gespeicherten, personenbezogenen Daten selbst, welche aus zahlreichen verschiedenen EDV-Anwendungen entnommen werden müssen, sondern auch um die Herkunft und die Empfänger, an welche diese Daten übermittelt wurden sowie um den konkreten Zweck der Speicherung.

Da es sich um ein elementares Betroffenenrecht handelt, wird in der Kommunikation mit den jeweiligen verantwortlichen Stellen dazu geraten, sich bereits im Vorfeld organisatorisch auf Auskunftsersuchen vorzubereiten und die Gewährung bereits vorab im Workflow abzubilden. Im Rahmen der Tätigkeit des BfD EKD als Datenschutzaufsicht werden die verantwortlichen Stellen über den Umfang des Anspruchs aufgeklärt, um die praktische Umsetzung sicherstellen zu können.

Videoüberwachung

Mehrere Beschwerden bezogen sich auf Videoüberwachungen unter Einsatz von optisch-elektronischen Einrichtungen. Sowohl im verfasst-kirchlichen Bereich als auch im Bereich von diakonischen Einrichtungen ist vermehrt der Einsatz von Videoanlagen zu beobachten.

In einem konkreten Fall ließ die Geschäftsführung eines Krankenhauses ohne Hinzuziehung des Betriebsbeauftragten für den Datenschutz großflächige Videoüberwachungen installieren. Gerade wegen der hohen Eingriffsintensität sind an den ordnungsgemäßen Einsatz von Videoanlagen zahlreiche Anforderungen zu stellen. Zunächst ist zwischen der reinen Videobeobachtung und der Videoaufzeichnung, die mit einer Speicherung der Aufnahmen einhergeht, zu unterscheiden. Da die Speicherung die Möglichkeit der nachträglichen genauen Analyse der Aufnahmen bietet, sind entsprechend höhere Anforderungen an den Einsatz zu stellen.

Die Videobeobachtung ist nur zulässig, soweit sie in Ausübung des Hausrechts der kirchlichen Stelle zum Schutz von Personen und Sachen oder zur Überwachung von Zugangsberechtigungen erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dabei ist insbesondere zu prüfen, ob der Einsatz wirklich erforderlich ist, d.h. ob der verfolgte Zweck nicht auch mit einem weniger schwer in Grundrechte eingreifenden Mittel zu erzielen ist. Die reine Videobeobachtung überträgt ein Live-Bild auf einen Monitor. Ein Mitarbeitender kann hier das Bild beobachten, um z.B. Zugangsberechtigungen von Mitarbeitenden zu kontrollieren.

Soweit eine Videoaufzeichnung stattfinden soll – was im konkreten Fall bei allen Kameras gegeben war – erhöhen sich die datenschutzrechtlichen Anforderungen abermals. Aufgezeichnet werden dürfen die Daten in diesem Fall grundsätzlich nur dann, wenn mit einer Verletzung der Rechtsgüter (Personen und Sachen) künftig zu rechnen ist. Der rein präventive Einsatz von Videoaufzeichnung ist datenschutzrechtlich unzulässig. Wenn es - wie im konkreten Fall - in der Vergangenheit zu keinen dokumentierten Straftaten gekommen ist und auch sonst keine konkreten Tatsachen vorliegen, die die Annahme rechtfertigen, dass künftig mit der Verletzung der Rechtsgüter zu rechnen ist, hat der Einsatz von Videoaufzeichnung zu unterbleiben.

Die Videobeobachtung als auch die Videoaufzeichnung sind für die Betroffenen kenntlich zu machen. Zum einen sollen sie darüber informiert werden, dass sie sich in einem videoüberwachtem Bereich befinden. Somit haben die Betroffenen grundsätzlich die Möglichkeit zu entscheiden, ob sie sich diesem Eingriff aussetzen wollen oder nicht. Zum anderen können Betroffene nur so ihre Rechte effektiv geltend machen, denn sie müssen wissen, wer für die Videoüberwachung verantwortlich ist und an wen sie sich wenden können. Die Kenntlichmachung wird in der Praxis - wie auch im konkreten Fall - oft vergessen, was zu einem Datenschutzverstoß führt. Die Rechtmäßigkeit einer ansonsten rechtmäßigen Videoüberwachung wird durch diesen Umstand jedoch nicht berührt.

Bewerbungsbögen

Den BfD EKD erreichte die Eingabe eines Bewerbers, der sich bei einem Krankenhaus beworben hatte und der die Rechtmäßigkeit der abgefragten Daten im Rahmen seiner Bewerbung überprüfen lassen wollte. Tatsächlich ging der Fragebogen weit über das hinaus, was der Arbeitgeber im Rahmen seines Fragerechts im Bewerbungsverfahren erheben darf. Das Fragerecht des Arbeitgebers ist im Rahmen des Bewerbungsvorgangs auf Fragen beschränkt, an deren Beantwortung der Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat. Die Fragen müssen insbesondere auch einen unmittelbaren Zusammenhang zu der zukünftigen Tätigkeit aufweisen. Daher kann es in der Regel gerade nicht darauf ankommen, welche Angaben der Arbeitgeber als nützlich oder interessant empfindet. Die Einholung solcher Daten stellt eine unzulässige Datenerhebung dar. Auch kann das Fragerecht nicht durch die Einholung einer Einwilligung des Bewerbers erweitert werden, da die Beschränkungen des Fragerechts damit unterlaufen würden. Gleiches gilt grundsätzlich auch für den Hinweis auf die Freiwilligkeit bestimmter Angaben. Im konkreten Fall wurden sowohl grundsätzlich unzulässige Fragen – wie die nach dem Beruf des Vaters und dem Gesundheitszustand der Familie – als auch im Kontext unzulässige Fragen – wie die zum bisherigen Einkommen – gestellt.

Strukturierte Datenschutzgespräche

Bei strukturierten Datenschutzgesprächen mit dem Landeskirchenamt der Ev. Kirche von Westfalen, der Ev. Kirche Kurhessen-Waldeck und der Lippischen Landeskirche wurde jeweils die aktuelle Situation im Hinblick auf Fragen zum Datenschutz und zur Datensicherheit erfragt und die kurz-, mittel- sowie langfristige Planung diskutiert. Im Verlauf der Gespräche wurde außerdem über ein jeweils vorab vorgelegtes Datenschutzkonzept diskutiert.

Im Datenschutzgespräch wurde auch über den Aufbau sowie die Arbeit und das Selbstverständnis des BfD EKD informiert. Auch Fragen der Zusammenarbeit mit dem BfD EKD wurden besprochen.

Es ist geplant, zukünftig rechtzeitig und regelmäßig über Fortschritte und Probleme ins Gespräch zu kommen.

Beratung

Zum Thema Beratung heißt es im Sachstandsbericht des BfD EKD auf Seite 20:

> *„Beratungen finden auch in der Aufbauphase fortlaufend statt. Insbesondere an der Nahtstelle zwischen IT/IT-Sicherheit und Datenschutz gibt es eine Fülle technischer Anfragen. Dabei spielen die Themen Cloud Computing und Verschlüsselung eine sehr große Rolle. Im rechtlichen Bereich drehen sich viele Anfragen um die Themen Auftragsdatenverarbeitung und Veröffentlichungen im Internet."*

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 einer weiteren Standardisierung und Professionalisierung der Beratung - zu den im Sachstandsbericht genannten Themen bereits mehrere Materialien erarbeitet worden. Die Materialien sind den fünf unterschiedlichen Formaten Entschließung, Handreichung, Kurzinformation, Muster und Sensibilisierung zugeordnet. Die Verbreitung dieser Materialien erfolgt insbesondere über die Rubrik Infothek auf der Homepage des BfD EKD und in Papierform (Homepage ist unter https://datenschutz.ekd.de aufrufbar).

- Entschließung
  - Cloud Computing
  - Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz (geplant für 2017)
- Handreichung
  - Verschlüsselte Versendung von Protokollen bei elektronischer Kommunikation mit Ehrenamtlichen
  - Datenschutzhinweise zum Betrieb von Windows 10
  - Datenschutz im Gemeindebrief
  - Datenschutzkonformes Versenden von E-Mails an E-Mailverteiler
- Muster
  - Vereinbarung „Durchführung einer Auftragsdatenverarbeitung mit Adressdaten"
  - Arbeitshilfe mit Erläuterungen zur Vereinbarung über die Verarbeitung personenbezogenen Daten gemäß § 11 EKD-Datenschutzgesetz
  - Dokumentation bei Maßnahmen zur Videoüberwachung
  - Verpflichtungserklärung und Merkblatt für Mitarbeitende auf das Datengeheimnis
  - Verpflichtungserklärung und Merkblatt für Ehrenamtliche auf das Datengeheimnis
- Kurzinformation
  - Datenschutz in Kindertagesstätten
- Sensibilisierung
  - Passwortkarte
  - Postkarte
  - Posterkampagne „Datenschutz beginnt bei mir!"

Sämtliche Beratungsanfragen wurden von der Dienststelle des BfD EKD ordnungsgemäß bearbeitet. Einzelheiten sind den folgenden Ausführungen in diesem Kapitel zu entnehmen.

Hauptsitz

Personal Ausland

Im Jahr 2015 fand ein Beratungsgespräch in der Auslandsabteilung des Kirchenamtes der EKD in Hannover statt. Hierbei wurden Hinweise zur Verbesserung der Prozesse bei der Besetzung einer Pfarrstelle in einer deutschsprachigen Gemeinde im Ausland gegeben. Beispielsweise wurde empfohlen, die Auskunftspflichten der Bewerber auf das erforderliche Maß zu beschränken. Weiterhin wurde empfohlen, die Personalbögen insbesondere hinsichtlich des Grundsatzes der Datensparsamkeit zu überarbeiten. Auf die Namen von Partnern und Kindern sollte verzichtet werden und stattdessen lediglich Zahl und Alter der Kinder abgefragt werden.

Personalverwaltung

In einer kirchlichen Einrichtung wurde Anfang 2015 ein Projekt zur Einführung eines Personalverwaltungsprogramms aufgesetzt. Der BfD EKD wurde Ende 2015 erstmalig über die Einführung informiert. Der Anforderungskatalog an ein Personalverwaltungsprogramm wurde durch eine Projektgruppe erarbeitet, an der auch der BfD EKD teilgenommen hat. Die datenschutzrechtlichen Anforderungen wurden in mehreren Projektgruppensitzungen eingebracht und auch schriftlich festgehalten. Die Endfassung der Leistungsbeschreibung wurde Mitte 2016 vorgelegt. Darin wurde zugesichert, dass die Anforderungen an das Thema Verschlüsselung und Langzeitarchivierung erfüllt werden. Das Umsetzungsprojekt zur Einführung des Personalverwaltungsprogramms wird vom örtlich Beauftragten für den Datenschutz der kirchlichen Einrichtung begleitet.

Adressverwaltung

Eine kirchliche Stelle suchte ein Nachfolgeprodukt für die bestehende und mittlerweile veraltete Adressverwaltung. Kurz nach Kontaktaufnahme zum BfD EKD mit der Bitte um Beratung wurden mehrere Produkte vorgestellt. An dieser Produktvorstellung hat der BfD EKD teilgenommen. Dabei wurde schnell deutlich, dass der Funktionsumfang der vorgestellten Produkte über die Anforderungen an eine „reine" Adressverwaltung deutlich hinausging. Viele Funktionen waren eher dem Bereich eines Customer Relation Management-Systems (CRM-System) zuzuordnen. Dadurch ergaben sich spezielle datenschutzrechtliche Anforderungen. Basierend auf der Produktvorstellung erfolgte eine schriftliche Stellungnahme des BfD EKD zu den datenschutzrechtlichen Anforderungen der angestrebten Lösung. Da für diese kirchliche Stelle mittlerweile ein örtlich Beauftragter für den Datenschutz bestellt worden ist, findet eine direkte Einbindung des BfD EKD in den Prozess nicht mehr statt.

Onlineseelsorge

Im Bereich der Diakonie wurde der BfD EKD zur Beratung bei der Entwicklung einer geschützten und datenschutzkonformen Seelsorge und Onlineberatung hinzugezogen. Dadurch war es möglich, bereits bei der Leistungsbeschreibung konkret beratend tätig zu werden.

Cloud Computing

Viele Anfragen erreichen den BfD EKD zum Thema Cloud Computing. Immer mehr Anwendungen werden nicht mehr lokal auf einem Rechner betrieben, sondern in einer Cloud. Weitaus verbreiteter ist aber die Tatsache, dass aktuelle Anwendungen Daten nicht mehr lokal auf dem Rechner, sondern in einer Cloud im Internet ablegen. Dies bringt den entscheidenden Vorteil, dass Anwender nun von überall auf die Anwendung und die Daten zugreifen und sogar von verschiedenen Standorten gemeinsam an Projekten arbeiten können. Daher geht es im Beratungsbereich vermehrt um die datenschutzrechtliche Zulässigkeit der verschiedenen Systeme.

Das Datenschutzgesetz der EKD knüpft die rechtliche Verantwortlichkeit für die Datenverarbeitung personenbezogener Daten an die inhaltliche Verantwortlichkeit über die Entscheidung des Umgangs mit den Daten. Nutzt eine Einrichtung Cloud Computing, werden die Daten zumindest im Rahmen der Nutzung in der Cloud - und damit in der Regel bei einem externen Anbieter - gespeichert. Handelt es sich dabei um personenbezogene Daten, verarbeitet der Cloud-Anbieter diese Daten für die Einrichtung als Auftragnehmer. Verantwortlich für den Datenschutz bleibt aber die Einrichtung selbst. Nutzt die Einrichtung Cloud Computing, hat sich die Einrichtung über die Sicherheit auf Seiten des Auftragnehmers zu versichern, mit ihm entsprechende Verträge abzuschließen und dafür Sorge zu tragen, dass die Mitarbeitenden des Auftragnehmers auf das Datengeheimnis nach § 6 DSG-EKD verpflichtet werden. Dazu sind entsprechende Muster erarbeitet worden, bei deren Anwendung der BfD EKD beratend zur Seite steht.

Gemäß § 11 Abs. 2 DSG-EKD ist die Verarbeitung durch externe Dienstleister außerhalb eines Mitgliedsstaats der Europäischen Union nicht zulässig. Das bedeutet, dass Cloud-Dienste vor allem aus den Vereinigten Staaten von Amerika grundsätzlich nicht genutzt werden dürfen. Im besten Falle ist es für die Einrichtungen möglich, die Cloud im lokalen Netzwerk zu realisieren. In diesem Fall ist ein Zugriff aus dem Internet möglich, die Verarbeitung findet aber lokal in der Einrichtung statt, so dass datenschutzrechtliche Bedenken hinsichtlich einer Auftragsdatenverarbeitung ausscheiden.

Um der allgemeinen Bedeutung des Themas im kirchlichen und diakonischen Umfeld gerecht zu werden, hat der BfD EKD zusammen mit den anderen eigenständigen Datenschutzaufsichtsbehörden in der EKD die Entschließung Cloud Computing erarbeitet und verabschiedet. Die Entschließung hat in allen Gliedkirchen der EKD und in der Diakonie Verbindlichkeit, da sie mit allen Datenschutzaufsichtsbehörden in der EKD abgestimmt ist. Die Entschließung formuliert in Kürze die wichtigsten Anforderungen des rechtlichen und technischen Datenschutzes, die bei der Einführung und Nutzung von Cloud-Diensten zu beachten sind. So kann die Entschließung bei jeder Beratung zu diesem Thema verwendet werden und dient einer grundlegenden Orientierung.

Office 365

Ein Beispiel für einen Cloud-Dienst ist Office 365. Microsoft drängt zurzeit mit attraktiven Lizenzbedingungen für dieses Produkt in den kirchlichen Bereich. In diesem Zusammenhang wurde der BfD EKD bei der Beratung zum Thema hinzugezogen, als eine Landeskirche im Kirchenamt der EKD einen Antrag auf Zulassung von Office 365 gemäß § 11 DSG-EKD gestellt hat. Nach Auffassung des BfD EKD ist eine Zulassung einzelner Dienste nach dem DSG-EKD nicht vorgesehen. Dennoch haben sich der BfD EKD und das Kirchenamt der EKD mit der Frage nach dem datenschutzkonformen Einsatz dieses Produkts auseinander gesetzt. Nach Beratungen, auch direkt mit Microsoft, hat der BfD EKD festgestellt, dass eine Nutzung der Office 365 Cloud-Dienste auf Grundlage des DSG-EKD nicht zulässig ist. Auch eine lokale Nutzung von Office 365 im Rahmen einer Cloud-Lizenz ist ohne zusätzliche technische und organisatorische Maßnahmen nicht zulässig. Der Einsatz des Produkts ist deswegen nicht zulässig, weil – im Zeitpunkt der Überprüfung – zwangsweise die personenbezogenen dienstlichen E-Mail-Adressen an ein Active Directory der Firma Microsoft in den USA übermittelt wurden.

Zum Zeitpunkt der Berichtserstellung liegt dem BfD EKD erneut die Einführung von Office 365 in einer Landeskirche zur Prüfung vor. Die Ausgangslage hat sich mittlerweile geändert, da diese Landeskirche Office 365 in der in Deutschland durch die Deutsche Telekom treuhänderisch betriebenen Cloud betreiben will. Aktuell liegen noch keine detaillierten Informationen der Firma Microsoft vor, so dass eine abschließende datenschutzrechtliche Bewertung noch nicht möglich ist. Die wesentlichen zu klärenden Fragen sind: Abschluss eines Vertrages zur Auftragsdatenverarbeitung auf der Grundlage des DSG-EKD, Standort des verwendeten Active Directory und Zugriff im Supportfall.

Kirchencloud

Die sogenannte Kirchencloud ist ein Cloud-Dienst eines kirchlichen Dienstleisters, der auf dem Produkt OwnCloud basiert. Hierbei handelt es sich um eine Open Source-Anwendung, die von jedermann kostenfrei genutzt werden kann. Bei der Einführung des Angebotes in einer kirchlichen Stelle wurde der BfD EKD in einer frühen Phase beteiligt. In dieser Phase ging es im Besonderen um die Ausgestaltung von Gruppenkonzepten und um den Umgang mit Logindaten. Mittlerweile wird dieser Dienst verwendet. Der BfD EKD ist allerdings in den Prozess der Implementierung nicht mehr eingebunden worden. Somit hat bisher auch keine abschließende datenschutzrechtliche Überprüfung stattgefunden.

KirchenApp

Die KirchenApp ermöglicht es dem Nutzer, mit Hilfe einer sogenannten Umkreissuche Kirchen aufzufinden. Die App bietet außerdem Zusatzinformationen wie Gottesdienst- und Öffnungszeiten. Bei teilnehmenden Kirchen kann die Kirche außerdem über eine Audio-Kirchenführung entdeckt werden. Der BfD EKD wurde bei der Frage der Einbindung einer möglichen Spendenfunktion in die KirchenApp involviert. Zunächst war geplant, den Bezahldienst PayPal in die KirchenApp einzubinden. Nach Klärung der Datenflüsse musste der BfD EKD feststellen, dass im konkreten Fall PayPal die Funktion einer Auftragsdatenverarbeitung für die Kirchengemeinden übernehmen würde. Somit war § 11 DSG-EKD anzuwenden, in dem formuliert ist, dass eine Auftragsdatenverarbeitung außerhalb der Mitgliedsstaaten der Europäischen Union nicht zulässig ist. Da PayPal seine Daten aber auch in Rechenzentren außerhalb der Europäischen Union verarbeitet, konnte PayPal nicht genutzt werden. Der BfD EKD hat stattdessen gemeinsam mit dem Anfragenden eine alternative Lösung erarbeitet.

Sonstiges

Der BfD EKD wurde häufiger zur Beratung und Klärung von Vertragsfragen hinzugezogen. Oftmals handelte es sich um Fragen zum Thema Auftragsdatenverarbeitung. Auch der datenschutzkonforme Umgang mit Testdaten und die daraus resultierenden vertraglichen Regelungen wurden angefragt.

Der BfD EKD hat ebenfalls einige kirchliche Stellen im Bereich der Dienstanweisungen zur IT-Nutzung beraten. In diesen Fällen waren häufig Fragen zu Kontrollrechten zu klären. Damit einhergehend musste immer auch der datenschutzkonforme Umgang mit Protokolldaten sichergestellt werden.

Daneben gab es mehrere Beratungsanfragen von Mitarbeitervertretungen und Rechnungsprüfungseinrichtungen zu speziellen Fragen an der Schnittstelle zum Thema Datenschutz.

Datenschutzregion Nord

In der Datenschutzregion Nord gibt es in allen Landeskirchen und diakonischen Einrichtungen einen erheblichen Beratungsbedarf zum Thema Datenschutz. Die Anfragen kommen überwiegend von hauptamtlich Beschäftigten (zum Beispiel Pastorinnen und Pastoren sowie Mitarbeitenden aus Kindertagesstätten, Verwaltungsmitarbeitende aus Kirchenkreisämtern und Landeskirchenämtern). Aus den Gemeinden wenden sich auch Ehrenamtliche (vor allem Kirchenvorstände) direkt an die Außenstelle Hannover. Ein erheblicher Beratungsbedarf ist ebenfalls bei den örtlich Beauftragten für den Datenschutz vorhanden, da viele Bestellungen erst in den letzten Monaten erfolgt sind.

Die Anfragen sind breit gestreut und beziehen sich häufig auf die Frage nach der rechtmäßigen Weitergabe von personenbezogenen Daten. Dazu einige Beispiele:

Themenüberblick

- Wunsch des Kirchenvorstandes, Geburtstage in Gemeindebriefen und Zeitungen zu veröffentlichen
- Einsichtnahme in Kirchenbücher zum Zwecke der Ahnenforschung
- Veröffentlichung von Mitarbeitendendaten im Internet
- Zugriff eines Vereins zur Förderung einer Kindertagesstätte auf alle Adressdaten der Gemeindeglieder zu Werbezwecken
- Übermittlung von personenbezogenen Daten (Impfnachweise) von den Kindertagesstätten an die Gesundheitsämter
- Übermittlung von Daten an das Landesamt für Statistik
- Bekanntmachung von Wählerlisten im Rahmen der MAV-Wahl
- Anonymisierung von Patientendaten zu Forschungszwecken
- Vernichtung von Akten
- Erstellung eines Fragebogens zur Begehung in der Gemeinde

Im Rahmen dieser Anfragen erfolgte häufig unmittelbar eine Zusammenarbeit mit den örtlich Beauftragten für den Datenschutz.

Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz

Bei der Bestellung von örtlich Beauftragten tauchten zudem immer wieder bestimmte Fragen auf, z. B.: „Wie muss bestellt werden?“ (Antwort: schriftlich), „Ist die MAV zu beteiligen?“ (Antwort: wird empfohlen, ist aber nicht zwingend) oder „Darf ein Systemverwalter als örtlich Beauftragter bestellt werden?“ (Antwort: Einzelfallprüfung). Voraussetzungen, Aufgaben und Rahmenbedingungen sind im DSG-EKD zwar beschrieben, dennoch gab es dazu immer wieder Rückfragen, die im Einzelfall geklärt wurden.

Überarbeitung von Rechtsgrundlagen

Die Überarbeitung von Satzungen, Ordnungen, Dienstvereinbarungen sowie von Mustern oder sonstigen Materialien ist häufig Anlass, um das Beratungsangebot des BfD EKD in Anspruch zu nehmen. Die Spannbreite reicht z. B. von der Änderung der Friedhofsordnung (im Hinblick auf Videoüberwachung) über eine Dienstvereinbarung zur Einsichtnahme in E-Mail-Konten bis hin zur Musterdienstvereinbarung für Home Office.

Materialdienst

Folgende Muster bzw. Merkblätter werden häufig nachgefragt:

- Einwilligung in die Veröffentlichung von personenbezogenen Daten (z. B. in Gemeindebriefen)
- Einverständniserklärung zur Verwendung von Fotos
- Datenschutzerklärung für Websites
- Speicherung und Verwendung von personenbezogenen Daten bei Seminarveranstaltungen
- Merkblatt zur Verpflichtung auf das Datengeheimnis (allgemein, aber auch speziell für Kindertagesstätten)

Einführung von Software

Häufig führt auch die Einführung einer neuen Software zu der Frage, ob und wie diese Software datenschutzkonform eingesetzt werden kann. Eine generelle Antwort wird der Komplexität der verwendeten Programme häufig nicht gerecht. In der Regel muss eine Einzelfallprüfung vorgenommen werden. Dennoch zeichnen sich bei der Einführung einer Software im Blick auf eine Auftragsdatenverarbeitung (ADV) nach § 11 DSG-EKD allgemeine Aspekte ab, die immer wieder zu benennen sind:

- Sofern mit der Einführung der Software eine Auftragsdatenverarbeitung vorliegt, muss hierüber ein schriftlicher Vertrag (ADV-Vertrag) geschlossen werden.
- Eine Auftragsdatenverarbeitung von personenbezogenen Daten außerhalb eines Mitgliedsstaates der Europäischen Union ist unzulässig.

In einer Landeskirche werden Online-Shops angeboten. Im Rahmen einer Beratung wurde darauf hingewiesen, dass eine Mandantentrennung erforderlich ist. Dies führt zu Mehrkosten, die aber unvermeidlich sind.

Bei der Einführung eines Personalinformationssystems in einer Landeskirche wurde eine Beratungsanfrage gestellt. Im Ergebnis wurde eine verbesserte Steuerung der Zugriffsberechtigungen eingerichtet.

Aus einer Landeskirche wurde die Zulässigkeit der Verwendung von „google webfonts“ auf kirchlichen Servern angefragt. Eine Auswertung der Metadaten durch Google führt unter Umständen zur Speicherung von Profilen mit personenbezogenen Daten in den USA. Dies ist unzulässig und schließt somit eine Verwendung von „google webfonts“ im kirchlichen Bereich aus.

Es liegt eine Anfrage zur Zulässigkeit eines webbasierten Kitaplaners vor. Die Prüfung erfolgt in Zusammenarbeit mit den anderen Datenschutzregionen und ist noch nicht abgeschlossen.

Für den Einsatz von Windows 10 wurde eine Handreichung erarbeitet, die detaillierte Hinweise gibt, wie eine datenschutzfreundliche Einstellung des Betriebssystems ermöglicht werden kann.

Datenschutzregion Ost

Bestellung Betriebsbeauftragte oder örtlich Beauftragte für den Datenschutz

Ein häufiges Thema bei Beratungsanfragen waren die Bestellung sowie die Stellung und die Aufgaben von Betriebsbeauftragten sowie örtlich Beauftragten für den Datenschutz. Die Anfragen wurden von Leitungen sowie von potenziellen Beauftragten gestellt.

Eine Frage richtete sich darauf, wann Betriebsbeauftragte oder örtlich Beauftragte für den Datenschutz bestellt werden müssen. Dies ist gemäß § 22 Abs. 1 DSG-EKD der Fall, „wenn in der Regel mehr als neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind“. Hierbei muss bei hauptamtlich Mitarbeitenden genauso wie bei ehrenamtlich Mitarbeitenden im Einzelfall konkret geprüft werden, ob diese „ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind“.

Hinsichtlich der Frage, welche Voraussetzungen Betriebsbeauftragte sowie örtlich Beauftragte für den Datenschutz mitbringen müssen, wurde auf die Fachkunde und die persönliche Eignung hingewiesen. Die Fachkunde muss sowohl auf die rechtlichen, technischen sowie organisatorischen Anforderungen in der jeweiligen Einrichtung im Hinblick auf den Datenschutz gegeben sein. Hierbei sind aufgrund der unterschiedlichen Arbeitsschwerpunkte der Einrichtungen unterschiedliche Gewichtungen vorzunehmen und Schwerpunkte zu legen. Neben der Fachkunde muss auch die persönliche Eignung gegeben sein.

Gemäß § 22 Abs. 7 DSG-EKD sollen sowohl ein Vertreter der Leitung der Einrichtung, aber auch der Leiter der IT nicht als Betriebsbeauftragter bzw. Betriebsbeauftragter oder örtlich Beauftragte oder Beauftragter für den Datenschutz bestellt werden. Hier entsteht eine Interessenkollision, da die Leitung sich nicht selbst kontrollieren kann und IT-Leitung und Datenschutzbeauftragter unterschiedliche Zielsetzungen verfolgen. Da es sich um eine Soll-Regelung handelt, ist dies im Ausnahmefall doch möglich.

Auch der Umfang der Aufgaben von Betriebsbeauftragten oder örtlich Beauftragten wurde erfragt. Neben den in § 22 Abs. 6 DSG-EKD genannten Aufgaben sind die Betriebsbeauftragen und örtlich Beauftragten für den Datenschutz insbesondere auch für die Führung und Bereithaltung der Dokumentation

über die Durchführung einer Videoüberwachung gemäß § 7a Abs. 7 DSG-EKD sowie die Durchführung von Vorabkontrollen gemäß § 21 Abs. 3 DSG-EKD zuständig.

Auch die unterschiedlichen Verantwortlichkeiten im Bereich des Datenschutzes wurden nachgefragt. Die Verantwortlichkeit für den Datenschutz liegt bei der Leitung der kirchlichen Stelle. Daran ändert sich auch nach der Bestellung eines oder einer Betriebsbeauftragten oder örtlich Beauftragten für den Datenschutz nichts. Weiterhin ist die Vertretung des Betriebsbeauftragten oder örtlich Beauftragten zu regeln, d.h. ein stellvertretender Beauftragter muss benannt werden.

Bei mehreren Fragen zur Stellung der Betriebsbeauftragten oder der örtlich Beauftragten für den Datenschutz wurde auf die Unabhängig der Beauftragten hingewiesen. Er oder sie ist in der inhaltlichen Bewertung datenschutzrechtlicher Fragen weisungsfrei und ist unmittelbar dem Leitungsorgan unterstellt. Er oder sie hat so jederzeit die Möglichkeit, sich direkt an die Leitung zu wenden. Die Leitung hat aber nicht in allen möglichen Belangen eine Informationspflicht.

Auf Anfrage wurden konkrete Hinweise zu möglichen Maßnahmen zu Beginn der Tätigkeit eines Datenschutzbeauftragten gegeben. Hierbei wurden die Information der Mitarbeitenden in der Einrichtung (Rundschreiben, Aushang, Intranet, Aufnahme in das Organigramm falls vorhanden etc.) genannt. Ein weiterer wichtiger Punkt ist die Kontaktaufnahme mit den wichtigsten Ansprechpartnern. Beispiele hierfür sind die MAV (oft „Verbündeter“ des örtlich Beauftragten aufgrund der ähnlichen Aufgabenstellung), die Leitung der Personalabteilung und die IT-Leitung. Sowohl die Erstellung eines Schulungs- und Verpflichtungskonzepts für Mitarbeitende als auch die Überprüfung (und Anpassung) der bestehenden Praxis hinsichtlich der Verpflichtung auf das Datengeheimnis in der Einrichtung bieten sich zum Tätigkeitsbeginn der Betriebsbeauftragten oder örtlich Beauftragten für den Datenschutz als Einstieg an.

Home Office

Bei der Prüfung eines Home Office-Vertrages wurde darauf hingewiesen, dass bei der Planung der Einrichtung von Home Office-Arbeitsplätzen durch den Arbeitgeber konkret in die Abwägung einbezogen werden muss, um welche Tätigkeit es sich handelt und folglich welche Daten im Rahmen des Home Office verarbeitet und übermittelt werden sollen. Bei besonders hoher Sensibilität – etwa Daten über Beurteilungen und Erkrankungen im Beschäftigtendatenschutz – kann dies zum Ausschluss der Option Home Office führen. In jedem Fall ist immer besonderes Augenmerk auf die technisch-organisatorischen Maßnahmen zu legen.

Weiterhin ist die Missbrauchsgefahr, welche bei den konkreten Arbeitsabläufen zu erwarten sind, in die Abwägung, ob eine Tätigkeit im Home Office möglich ist, einzubeziehen. Eine vollelektronische Datenverarbeitung ohne Medienbruch ist hierbei beispielsweise anders zu beurteilen als eine Tätigkeit, bei der ständig Akten vom Büro nach Hause hin und her transportiert werden müssen. Bei ersterer sind dann etwa Verschlüsselungsverfahren nach dem Stand der Technik notwendig. Im konkreten Fall wurde die Aufnahme der Punkte Virtual Private Network (VPN), Ende-zu-Ende-Verschlüsselung, keine Umleitung von beruflichen E-Mails und Telefonaten auf private Anschlüsse in den Vertragstext empfohlen. Hinsichtlich des Schutzes von Datenträgern wurde konkret empfohlen, Datenträger und Unterlagen nie unbeaufsichtigt zu lassen sowie Datenträger nur verschlüsselt und Papierunterlagen nur in verschlossenen Behältnissen zu transportieren.

Im Ganzen wurde auf die notwendige frühzeitige Beteiligung des oder der örtlich Beauftragten für den Datenschutz hingewiesen.

Führen von digitalen Kalendern

Im Rahmen einer Anfrage wurde thematisiert, welche Informationen über Abwesenheiten im gemeinsamen Kalender einer Gemeinde vermerkt werden dürfen, in den alle Mitarbeitenden der Gemeinde Einsicht haben. Konkret bezog sich die Frage auf Urlaubsabwesenheiten.

Keine datenschutzrechtlichen Bedenken bestehen dagegen, dass Vorgesetzte sich Angaben über geplante Abwesenheitszeiten für einen gewissen Zeitraum - z. B. Urlaubsjahr - notieren, um so die Funktionsfähigkeit ihrer Organisationseinheit im Hinblick auf Abwesenheitszeiten von Beschäftigten steuern und sicherstellen zu können. Auch für die Zusammenarbeit von Mitarbeitenden ist die Kenntnis von Abwesenheiten wesentlich. Soweit dies in automatisierter Form geschieht, sind unter anderem die Beteiligung der oder des örtlich Beauftragten für den Datenschutz und die Mitbestimmungsrechte der MAV zu beachten. Wichtig ist weiterhin, dass die zur Arbeitsorganisation genutzten Daten der Mitarbeitenden wieder gelöscht werden, wenn sie für deren konkrete Aufgaben nicht mehr benötigt werden.

Um den notwendigen Schutz besonderer personenbezogener Daten zu gewährleisten, wurde empfohlen, auf eine Differenzierung zwischen verschiedenen Abwesenheitsarten zu verzichten und stattdessen sowohl Urlaubs- als auch Fortbildungszeiten - einheitlich nur mit „abwesend“ auszuweisen. Alte Kalendereinträge sollten regelmäßig gelöscht werden.

Sollte die Einrichtung an einer differenzierten Darstellung nach Urlaub und anderen Abwesenheitsgründen festhalten, muss vor Veröffentlichung die schriftliche Einwilligung der Betroffenen eingeholt werden.

Verpflichtung auf das Datengeheimnis

Bei mehreren Anfragen ging es um Rechtsgrundlage und Inhalt der Verpflichtungserklärung auf das Datengeheimnis.

Eine Verpflichtung auf das Datengeheimnis findet bei kirchlichen Stellen gemäß § 6 DSG-EKD statt. Beim notwenigen Inhalt der Verpflichtungserklärung wurde auf die vorgehaltenen Muster hingewiesen und gebeten, das Landeskirchenamt bzw. Konsistorium zu kontaktieren.

Begehung der MAV-Räume durch Betriebsbeauftragte

Bei einer Beratungsanfrage durch eine Mitarbeitervertretung (MAV) wurde die Frage aufgeworfen, ob die oder der Betriebsbeauftragte für den Datenschutz im Rahmen seiner Tätigkeit ein Kontrollrecht gegenüber der MAV hat. Der Beauftragte beabsichtigte in den Räumen der MAV eine Begehung durchzuführen, wie er es auch in anderen Bereichen der Einrichtung zu tun pflegt.

Im Verhältnis zwischen der MAV und dem Betriebsbeauftragten ist die besondere und unabhängige Stellung der MAV von entscheidender Bedeutung.

Nach Auffassung des Bundesarbeitsgerichts unterliegt der Betriebsrat nicht der Kontrolle des Datenschutzbeauftragten. Wesentliches Argument des BAG war, dass der betriebliche Datenschutzbeauftragte trotz seiner gesetzlich verbürgten unabhängigen Stellung dem Arbeitgeber zuzuordnen sei. Ihm die Kontrolle des Betriebsrats zu übertragen, würde deshalb die Unabhängigkeit des Betriebsrats gefährden. Der Betriebsrat sei hinsichtlich der Einhaltung des Datenschutzes dem Arbeitgeber keine Rechenschaft schuldig.

Nach einhelliger Meinung wird der Betriebsrat aus diesem Grund in Bezug auf die Einhaltung datenschutzrechtlicher Vorschriften betriebsintern ausschließlich durch sich selbst kontrolliert. Ein Arbeitgeber kann sich bei einem Zugriff auf Unterlagen, die im Betriebsratsbüro vorliegen, oder bei einem Zugriff auf Dateien, die vom Betriebsrat abgespeichert wurden, nicht darauf berufen, er habe die Einhaltung datenschutzrechtlicher Vorschriften kontrollieren müssen.

Eine andere Bewertung für den kirchlichen Datenschutz ist nicht ersichtlich. Aus diesem Grund gilt auch hier die Aussage, dass eine Kontrolle der MAV durch den örtlich Beauftragten nicht erfolgt. Eine Kontrolle erfolgt lediglich durch den Beauftragten für den Datenschutz als Datenschutzaufsicht. Eine Beratung oder Weiterbildung der MAV kann jedoch jederzeit durch den örtlich Beauftragten bzw. Betriebsbeauftragten für den Datenschutz erfolgen.

Krankenhausseelsorge

Die datenschutzrechtlichen Grenzen der Tätigkeit eines Krankenhausseelsorgers in einem evangelischen Krankenhaus wurden im Rahmen einer Beratung thematisiert. Die Erhebung, Verarbeitung und Nutzung von Daten bedarf in jedem Fall einer Rechtsgrundlage oder einer wirksamen Einwilligung der Betroffenen. Eine gesetzliche Ermächtigung für die Tätigkeit eines Krankenhausseelsorgers besteht nicht. Folglich muss eine wirksame Einwilligung der Betroffenen vorliegen. Bei der Aufnahme in das Krankenhaus sollte den Patienten die Möglichkeit gegeben werden, ihre Konfession freiwillig auf dem Aufnahmebogen anzugeben bzw. anzukreuzen.

Darüber hinaus ist die ärztliche Schweigepflicht zu beachten. Aus diesem Grund darf der Krankenhausseelsorger keinen Einblick in Patientendaten haben, es sei denn, der Betroffene hat hierzu seine wirksame Einwilligung gegeben.

Akteneinsicht

In einem Fall verlangten Eltern Akteneinsicht in die auf ihr Kind bezogene Dokumentation einer Kindertagesstätte. Gemäß § 15 Abs. 1 DSG-EKD haben Betroffene auf Antrag ein Auskunftsrecht, welche Daten eine kirchliche Stelle über sie gespeichert hat sowie über die Herkunft oder empfangenden Stellen dieser Daten. Eltern können als Personensorgeberechtigte den Anspruch für ihre Kinder geltend machen. Zunächst wurde darauf hingewiesen, dass gemäß § 15 Abs. 2 Satz 3 DSG-EKD die verantwortliche Stelle, also ihre Einrichtung, das Verfahren und auch die Form der Auskunftserteilung nach pflichtgemäßem Ermessen bestimmt. Das bedeutet, dass die Einrichtung entscheiden kann, ob die Auskunft schriftlich, mündlich oder in der Form der Akteneinsicht erfolgt. Hintergrund für diese Regelung ist der Schutz der jeweiligen Einrichtung oder Stelle vor einer Überforderung durch Auskunftsersuchen. Weiterhin wurde deutlich gemacht, dass die Auskunft unter anderem dann nicht erteilt werden muss, wenn die Daten wegen überwiegender Interessen Dritter geheim gehalten werden müssen und das Informationsinteresse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

Im konkreten Fall wurde darauf hingewiesen, dass aus diesem Grund die Einrichtung entscheiden kann, wie sie dem Auskunftsrecht nachkommt. So kann Akteneinsicht gewährt werden oder lediglich schriftlich die Auskunft erteilt werden. Bei subjektiven Interpretationen – wie im vorliegenden Fall – wurde darauf hingewiesen, dass diese möglicherweise allein aus sich heraus nicht verständlich sind. Deshalb kann es sinnvoll sein, bei der Auskunftserteilung die Möglichkeit von Rückfragen an das jeweilige pädagogische Personal zu geben.

Weiterhin muss eine Abwägung zwischen dem Informationsinteresse der Eltern und den Interessen anderer Personen, etwa von pädagogisch Mitarbeitenden, stattfinden, wenn Anhaltspunkte dahingehend bestehen, dass diese ein überwiegendes Interesse an der Geheimhaltung von Daten haben.

Löschung von Daten

Anlässlich einer Anfrage zu Löschungsfristen in einer Kindertagesstätte wurde zunächst auf den Grundsatz hingewiesen, dass personenbezogene Daten nur solange zu speichern sind, wie dies für die konkrete Aufgabenerfüllung erforderlich ist. Das heißt, dass eine Aufbewahrung nach der Erledigung des jeweiligen Zwecks grundsätzlich unzulässig ist. Etwas anderes gilt dann, wenn die Daten im Rahmen eines Gerichtsverfahrens noch notwendig sind oder wenn eine vertragliche oder gesetzliche Aufbewahrungsfrist besteht.

Die Anfrage richtete sich darauf, wie lange Entwicklungsunterlagen bzw. Notizen aus dem pädagogischen Alltag aufbewahrt werden können. In der Vergangenheit waren diese im Rahmen von Sorgerechtsverfahren gelegentlich vom Familiengericht angefordert worden. Dies konnte auch für die Zukunft nicht ausgeschlossen werden.

Es wurde darauf hingewiesen, dass es nicht ausreicht, wenn die Aufbewahrung lediglich als wünschenswert betrachtet wird. Vielmehr müssen konkrete Anhaltspunkte dafür vorliegen, dass die Unterlagen in einem künftigen Prozess benötigt werden.

Da es sich bei den genannten Unterlagen um Daten handelt, die konkret Rückschlüsse auf die Entwicklung des jeweiligen Kindes erlauben, ist besondere Zurückhaltung geboten. Bei Sorgerechtsstreitigkeiten handelt es sich nicht um Verfahren, in die die Kita direkt eingebunden ist, wie etwa bei Schadensersatzklagen. Weiterhin ist möglich, die jeweilige Erzieherin oder den jeweiligen Erzieher als Zeugen zu hören. Falls dieser sich nicht mehr konkret an die Dinge, über die er oder sie befragt wird, erinnern kann, dann hat er oder sie das im jeweiligen Verfahren so auszusagen.

Aus diesem Grund ist nur in absoluten Ausnahmefällen davon auszugehen, dass Entwicklungsunterlagen bzw. Notizen über den Zeitpunkt hinaus, an dem ein Kind die Kindertagesstätte verlässt, aufbewahrt werden dürfen. Ein bei Gericht zu dem Zeitpunkt, an dem das Kind die Kita verlässt, schon anhängiges Sorgerechtsverfahren könnte ein solcher Einzelfall sein.

Datenschutzregion Süd

Verantwortliche Stelle

Nicht immer ist unmittelbar klar, wer eigentlich die verantwortliche Stelle ist. Ein Beispiel dafür sind Anfragen bei Einbindung von ehrenamtlichen Helfern in Projekte der Flüchtlingshilfe, wenn diese Projekte von Kirchengemeinden in Zusammenarbeit mit kommunalen oder katholischen Trägern organisiert werden. Auch hinter Beratungsstellen stehen immer häufiger „Zusammenschlüsse“ von evangelischen, katholischen, staatlichen und/oder freien Trägern. Betroffene, die sich durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt fühlen, müssen aber wissen, wer die verantwortliche Stelle ist und an welche Aufsichtsbehörde sie sich wenden können. Umgekehrt müssen auch die staatlichen Aufsichtsbehörden wissen, ob die staatliche oder die kirchliche Zuständigkeit gegeben ist.

Erweiterte Führungszeugnisse

Ein mit dem Datenschutz eng zusammenhängender Aspekt ist der Umgang mit Führungszeugnissen von Ehrenamtlichen und beruflich Mitarbeitenden. Erweiterte Führungszeugnisse werden verlangt, wenn die Tätigkeit intensive Kontakte zu Jugendlichen mit sich bringt. Allgemein birgt die Vorlage solcher Führungszeugnisse das datenschutzrechtliche Problem, dass darin Angaben zu jeglichen Delikten enthalten sein können. Mit den staatlichen Datenschutzaufsichtsbehörden wurde geklärt, dass bei Ehrenamtlichen ein Vorhalten solcher Zeugnisse nicht erforderlich ist, sondern lediglich ein Aktenvermerk gemacht werden muss, dass sie vorgelegt und gesichtet wurden. Dass es zulässig ist, bei haupt- und nebenamtlich

tätigen Personen solche Führungszeugnisse vorzuhalten, stößt auf Datenschutzbedenken. Dass diese Bedenken relevant werden können, zeigt das Verlangen eines Landratsamtes zur Vorlage der Beschäftigtendaten einer Kindertagesstätte, um die Verwendung der Gelder entsprechend der Förderrichtlinien überprüfen zu können. Mit dem Landratsamt wurde im konkreten Fall Einvernehmen dahingehend erzielt, dass die Führungszeugnisse der Beschäftigten nicht Gegenstand der Überprüfung der Einhaltung der Förderrichtlinien sind, wohl aber die Art der Arbeitsverhältnisse, insbesondere die Qualifikationen.

Kontrollen durch staatliche Stellen

Das Verlangen staatlicher Stellen, die Verwendung der an kirchliche Stellen gegebenen Finanzmittel zu überprüfen, wächst, insbesondere im Bereich der Diakonie. Dieses Verlangen kann eine Übermittlung personenbezogener Daten mit sich bringen, die den Betroffenen in der Regel nicht bewusst ist. Gegenüber kirchlichen und diakonischen Stellen, mit denen die Betroffenen direkt zu tun haben, offenbaren sie sich gelegentlich sehr viel weitergehender, als dies bei einer Orientierung an den Bestimmungen des Sozialgesetzbuches verlangt werden kann. Dieses „Mehrwissen" der kirchlichen und diakonischen Stellen ist häufig Voraussetzung für eine erfolgreiche Arbeit. Dieses Mehrwissen wird aber gefährdet, wenn die Hilfesuchenden damit rechnen müssen, dass alles, was sie in einem als vertraulich empfundenen Rahmen offenbaren, an staatliche Stellen übermittelt wird. Daran, dass die von ihnen eingesetzten Mittel mit Erfolg angewendet werden, haben auch die staatlichen Sozialhilfeträger ein originäres Interesse. Vor diesem Hintergrund entwickelt sich ein konstruktives Miteinander, das dem Bedürfnis der Betroffenen - ihre Daten beschränkt auf einem kleinen, überschaubaren Kreis verwendet zu wissen - und dem Interesse der Sozialhilfeträger - an einer nachprüfbaren Verwendung ihrer Mittel - Rechnung trägt.

Kontakt zu Ehrenamtlichen

Auch Fragen im Bereich des technischen Datenschutzes hängen mit der Tätigkeit von Ehrenamtlichen zusammen. Es liegt sehr im Interesse kirchlicher und diakonischer Stellen, dass die Anforderungen in diesem Bereich so erfüllt werden, dass mit geringen Aufwendungen an Arbeitszeit und Kosten ein gutes Sicherheitsniveau erreicht wird. Mit Interesse wird deshalb der Austausch mit einer Gruppe von Ehrenamtlichen mit sehr guten IT-Kenntnissen gepflegt, die den Dekan eines Kirchenbezirks darin unterstützen, die IT-Sicherheit in den Stellen seines Zuständigkeitsbereichs zu gewährleisten. Es handelt sich dabei um Personen, die beruflich viel mit EDV zu tun haben oder in ihrem Berufsleben zu tun hatten, und nun ihre Erfahrung und ihr Wissen der Kirche zur Verfügung stellen. Dadurch, dass sich in dieser Gruppe weitere Personen engagieren, die sich auf andere Weise in der Gemeindearbeit engagieren, werden die Probleme an „der Basis" adressiert. Hier muss der Stand, sinnvoll über die Anforderung eines Grundschutzes nach BSI-Norm (BSI ist die Bundesanstalt für Sicherheit in der Informationstechnik) oft überhaupt erst erreicht werden. Schon ganz elementare Maßnahmen wie die, dass es für einen eingesetzten PC einen Verantwortlichen geben muss und nur der die unter Sicherheitsaspekten sehr kritischen Administrationsrechte hat, müssen einsichtig gemacht und durchgesetzt werden. Ernüchternd war und ist die Feststellung, dass die Verwendung einigermaßen sicherer Passworte immer noch ein Thema ist.

Outsourcing von IT

Zunehmend treten Fragen zum Auslagern (Outsourcing) von Datenverarbeitungen, etwa in die Cloud auf. Datenschutzrechtlich bedeutet das eine Handhabung des Instruments einer Datenverarbeitung im Auftrag. Insbesondere zum Aspekt der (Software-)Wartung, die dann, wenn damit eine Einsichtnahme in personenbezogene Daten verbunden ist, eben auch eine Datenverarbeitung ist, wurden Anfragen gestellt. Das dazu vom BfD EKD in Kooperation mit landeskirchlichen Vertretern entwickelte Muster kann als Hilfsmittel dienen, einen solchen Vertrag aufzusetzen und kann auf der Homepage des BfD EKD heruntergeladen werden

Homepages kirchlicher Stellen

Datenschutz bei Homepages kirchlicher Stellen ist ein immer wiederkehrendes Thema, häufig zum Beispiel im Blick auf die Zulässigkeit der Veröffentlichung von Bildern.

Homepages sind heutzutage auch „Datenschutz-Visitenkarten", die – etwa auf das Vorhandensein einer Datenschutzerklärung – automatisiert abgeprüft werden können. Auch bei kirchlichen Homepages finden sich häufig Datenschutzerklärungen, die ganz offensichtlich Sachverhalte ansprechen, die für den jeweiligen Internetauftritt keine Relevanz haben. Solche Datenschutzerklärungen bestärken in der Regeln nicht das Vertrauen in den Datenschutz, sondern befördern das Misstrauen gegenüber dem Datenschutz.

Ein weiterer wichtiger Datenschutzaspekt bezieht sich auf die auf Homepages häufig vorgehaltenen Kontaktformulare, insbesondere wenn es sich um Stellen handelt, die mit gesundheitlichen Daten umgehen und bei denen damit gerechnet werden muss, dass über das Kontaktformular auch besondere personenbezogene Daten der verantwortlichen Stelle zugestellt werden. Dabei verarbeitet in der Regel ein serverseitiges Skript die im Kontaktformular gemachten Angaben und verwendet den serverseitigen Mailserver, um eine E-Mail zu generieren, die an einen bestimmten Mitarbeitenden geschickt wird.

Datenschutzrechtlich ist in diesem Zusammenhang zu beanstanden, dass diese Daten in der Regel unverschlüsselt übermittelt werden. Es ist also zwingend notwendig, den Internetauftritt mindestens mittels Transportverschlüsselung (HTTPS) zu sichern. Kann nicht sichergestellt werden, dass die übermittelten Daten auf den Servern des Webhosters oder einer betreuenden EDV-Firma nicht mitgelesen werden können, so muss darüber hinaus auch eine Ende-zu-Ende-Verschlüsselung aktiviert werden.

Datenschutzregion Mitte-West

Kita-Software

Vermehrt ist der Einsatz von sogenannter Kita-Software zu beobachten. Dabei geht es in der Regel um eine EDV-Lösung, die zur zentralen Kindertagesstätten-Planung eingesetzt werden kann und die administrativen Aufgaben erleichtern soll. Insbesondere sollen damit „Doppelanmeldungen" verhindert werden. Die Software gibt es von zahlreichen Herstellern und in verschiedensten Ausführungen (z.B. easykid, earlybird, Kita-Büro, Kita-Planer V.2 etc.).

In der Regel sind die Programme so angelegt, dass eine trägerübergreifende Vernetzung stattfinden soll und so über eine staatliche oder kirchliche übergeordnete Verwaltungseinheit eine transparente Planung realisiert werden kann. Der Einblick in diese zentralen Wartelisten und Auslastungsstatistiken ermöglicht, die aktuellen Kapazitäten und eventuelle freie Plätze ständig im Blick zu haben und auf Anfragen schnell und komfortabel reagieren zu können. Gerade die Auslastungsstatistiken sind für die Kommunen und Kreise wichtig, da sie sich so einen Überblick verschaffen können, wo und wie das Betreuungsangebot weiter auszubauen ist. Auf der anderen Seite können sich Eltern über bestehende Betreuungsangebote einfach im Internet informieren und über das das entsprechende Eltern-Portal direkt auf ihre Wunschplätze bewerben. Der Anwendungsbereich ist jedoch nicht darauf begrenzt. Vielmehr können auch weitere Dateien wie Betreuungsverträge, Entwicklungsberichte oder Bilder in der Kita-Software abgelegt und verwaltet werden. Insbesondere wegen der Dokumentation des Entwicklungsstandes der Kinder handelt es sich teilweise um besondere Arten personenbezogener Daten nach § 2 Nr. 11 DSG-EKD, die einem besonderem Schutz unterliegen.

Gerade an der Schnittstelle zur staatlichen Behörde – wo die Daten der evangelischen Träger den internen Bereich verlassen und mithin eine Übermittlung im datenschutzrechtlichen Sinne stattfindet – ist genau zu prüfen, welche personenbezogen Daten zu welchem Zweck übertragen werden. Den staatlichen

Akteuren ist an einem möglichst weitreichenden Informationsaustausch gelegen, insbesondere deswegen, weil ihre Planung so möglichst genau und umfangreich erstellt werden kann. Bereits bei der Konzeption der Programme müssen die datenschutzrechtlichen Grundprinzipien wie Datenvermeidung und Datensparsamkeit angelegt sein. Wie bei allen IT-basierten Systemen ist darauf zu achten, dass entsprechend differenzierte Benutzergruppen existieren und diese mit den passenden Rechten ausgestattet sind. Hier ist insbesondere darauf zu achten, dass die Nutzer auch nur Zugang zu den personenbezogenen Daten haben, die sie zur Erfüllung ihrer Aufgabe benötigen. Dabei sind verschiedene Benutzerkonzepte vorgegeben, insbesondere für die Eltern zwecks Anmeldung, die Kita-Mitarbeitenden und die Sachbearbeitenden der staatlichen Behörden zur Abrechnung und zur übergreifenden Planung. Dies ist in der Praxis teilweise nicht einfach umzusetzen, da die entsprechenden Zugriffrechte der einzelnen Rollen nicht über die gesamten Eingabemasken getrennt werden können. Die Mitarbeiterin einer Kindertagesstätte braucht keinen Zugang auf Abrechungsinformationen ihrer Kolleginnen oder über die Einkommensverhältnisse der Eltern zu haben. Genauso wenig braucht die Sachbearbeiterin in der Kommune detaillierte Einsicht in die Entwicklungsdokumentation eines Kindes oder benötigt für ihre Planung den tatsächlichen Namen des Kindes.

Weiterhin gilt es hier zu untersuchen, wie das Programm technisch ausgeführt wird. Wo laufen die Programme? Wo werden die Daten gespeichert? Wie werden die Daten untereinander übertragen? Wichtig ist eine verschlüsselte Übertragung. Doch auch wenn die Daten ihren Zielort erreicht haben, müssen sie dort ordnungsgemäß vor dem Zugriff Unberechtigter geschützt werden. In der Regel werden die Programme von den staatlichen Behörden betrieben oder in deren Auftrag in ausgelagerten Rechenzentren, teilweise auch von Externen betrieben. Verantwortlich für die personenbezogenen Daten ist grundsätzlich die Stelle, die die Daten erhoben hat, also gegebenenfalls eine evangelische Kindertagesstätte bzw. deren Träger. Tatsächlich physisch verarbeitet werden die Daten jedoch außerhalb ihres unmittelbaren Zugriffsbereichs. Daher haben sich die verantwortlichen Stellen vertraglich abzusichern. In dieser Situation liegt eine Auftragsdatenverarbeitung nach § 11 DSG-EKD vor, welche eine entsprechende Vereinbarung zwischen den Akteuren notwendig macht. Insbesondere hat die verantwortliche Stelle dafür Sorge zu tragen, dass das Datenschutzgesetz der EKD eingehalten wird. Dies hat unter anderem zur Folge, dass sämtliche mit den Daten in Berührung kommenden Mitarbeitenden auf das Datengeheimnis nach § 6 DSG-EKD zu verpflichten sind. Dies wird in diesen Konstellationen zumindest im Rahmen der Planung oftmals übersehen.

Teilweise erlauben die Kita-Programme mehr zu erheben als notwendig ist. Insoweit ist auch im laufenden Betrieb durch die Betriebsbeauftragten oder örtlich Beauftragten für den Datenschutz sicherzustellen, dass das Programm datenschutzkonform genutzt wird. Insbesondere sogenannte Freifelder verführen dazu, Daten zu erheben, die möglicherweise nicht erforderlich sind und auf die dann auch andere Personen Zugriff haben, die diese Daten im Rahmen ihrer Aufgabe nicht benötigen.

Überdies muss der technische Datenschutz gewährleistet sein, wobei insbesondere die Vorgaben aus der Anlage zu § 9 DSG-EKD zu erfüllen sind. Soweit der Betrieb des Programms in einem Rechenzentrum sowie die Nutzung an den Endgeräten in den Kindertagestätten auseinanderfallen, sind die Anforderungen an den technischen Datenschutz sowohl im Rechenzentrum als auch in der Kindertagesstätte zu erfüllen. Das bedeutet in den Kindertagesstätten, dass neben den erwähnten aufgabentypischen Zugangsrechten zu personenbezogenen Daten bereits der Zugang zu den PCs geschützt sein muss. Dies hat mindestens über individuelle Logins zu erfolgen, die nach einer Inaktivität automatisch ausloggen. Wie auch grundsätzlich geht es dabei um Revisionssicherheit, also um die Frage, ob nachträglich zurückverfolgt werden kann, wer welchen Eintrag vorgenommen oder gelöscht hat.

Die neue Kita-Software bringt insbesondere hinsichtlich der Planung sowie des administrativen Ablaufs erhebliche Vorteile mit sich. Gerade wegen der Sensibilität der Daten ist es jedoch von der Planung über die Realisierung bis hin zum Betrieb wichtig, alle datenschutzrechtlichen Vorgaben zu überprüfen und deren Anwendung sicherzustellen.

Veröffentlichungen im Gemeindebrief

Viele Beratungsanfragen beschäftigen sich mit der Frage, was wie im Gemeindebrief veröffentlicht werden darf. Das Datenschutzgesetz der EKD hat dazu keine speziellen Regelungen. Vielmehr ist aus den grundsätzlichen Regelungen zu entnehmen, dass Veröffentlichungen zur Wahrnehmung des kirchlichen Auftrags zulässig sind, wobei stets das Prinzip der Erforderlichkeit zu berücksichtigen ist.

Die Gliedkirchen in der Datenschutzregion Mitte-West haben jedoch von der Möglichkeit Gebrauch gemacht, ergänzende Bestimmungen zu erlassen, und so in den entsprechenden Durchführungsverordnungen detailliert geregelt, welche Daten zu welchen Anlässen auch ohne vorherige Einwilligung veröffentlicht werden dürfen. Insofern existieren in der Datenschutzregion Mitte-West mit fünf Gliedkirchen unterschiedliche Regelungen.

Überdies ist zu beobachten, dass zunehmend Gemeindebriefe im Internet veröffentlicht werden. War es in der Vergangenheit regelmäßig so, dass die Gemeindebriefe nur in der Kirchengemeinde, teilweise auch in der Kommune verteilt wurden und der Empfängerkreis überschaubar war, ist durch eine Veröffentlichung im Internet die ganze Welt nun potenzieller Empfänger und bekommt einen Einblick in das Gemeindeleben. Insofern haben hier andere Vorgaben gerade hinsichtlich der Einwilligung zu gelten. Insbesondere bei der Veröffentlichung von Fotos ist genau darauf zu achten, dass die abgebildeten Personen sowohl über das neue Medium informiert und auf die Gefahren hingewiesen werden als auch mit der Veröffentlichung des konkreten Bildes einverstanden sind.

Für weitere detaillierte Informationen steht die Handreichung „Datenschutz im Gemeindebrief“ auf der Homepage des BfD-EKD zur Verfügung.

Outsourcing im Krankenhaus

Auch in Krankenhäusern wird im Rahmen der Optimierung der Arbeitsabläufe regelmäßig geprüft, ob durch Outsourcing einzelne Aufgaben kostengünstiger von externen Firmen erledigt werden können. Dabei geht es häufig um Fragen der IT oder der Archivierung bzw. Vernichtung von Unterlagen.

Hierbei gilt es zu bedenken, dass nicht nur besondere Arten personenbezogener Daten gemäß § 2 Nr. 11 DSG-EKD – in diesem Zusammenhang Gesundheitsdaten - betroffen sind, sondern zusätzlich auch die ärztliche Schweigepflicht bzw. das Ärzte-Patienten-Geheimnis berührt ist.

Die Erledigung im Rahmen einer Auftragsdatenverarbeitung scheitert an der Tatsache, dass die ärztliche Schweigepflicht in der Regel gerade nicht ohne Einwilligung zu durchbrechen ist und daher eine detaillierte Aufklärung der Patienten über den Verbleib ihrer Daten im Voraus stattzufinden hat. Ein Patient kann damit rechnen, dass seine Gesundheitsdaten im Rahmen der Behandlung im Krankenhaus verschiedenen Ärzten und Mitarbeitenden zwecks Durchführung der einzelnen Arbeitsschritte zugänglich gemacht werden. Dass seine Daten jedoch den geschützten Bereich des Krankenhauses verlassen und Dritten im Rahmen von externen Dienstleistungen (z.B. Archivierung) offenbart werden, ist nicht vorauszusetzen.

Insoweit bedarf es bei Planung jeglicher Outsourcing-Vorhaben zunächst der Prüfung, ob eine solche Ausgliederung erforderlich ist und wie eine entsprechende Information der Patienten stattzufinden hat.

Weiterbildung

Zum Thema Weiterbildung heißt es im Sachstandsbericht des BfD EKD auf den Seiten 18 und 20:

> *„Ein weiteres wichtiges internes Ziel zur Etablierung eines eigenen effizienten Datenschutzes wird in der flächendeckenden Implementierung von Betriebsbeauftragten und örtlich Beauftragten für den Datenschutz gesehen. Aufbauend auf den gesetzlichen Regelungen in § 22 DSG-EKD ist in der Zwischenzeit zur Orientierung für alle Beteiligten ein Aufgabenkatalog für diese Personengruppe erarbeitet worden. In einem nächsten Schritt muss ein entsprechendes Weiterbildungskonzept entwickelt und umgesetzt werden." (...)*
>
> *„Zurzeit wird (...) in einer Arbeitsgruppe mit landeskirchlichen Mitarbeitenden an einem Weiterbildungskonzept für Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz gearbeitet. Es wird angestrebt, im Frühjahr 2015 am Ort der Außenstellen Auftaktveranstaltungen im Rahmen einer umfassenden Weiterbildung für Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz durchzuführen."*

Der BfD EKD setzt neben den Aufgaben Aufsicht und Beratung einen weiteren Schwerpunkt seiner Arbeit im Bereich Weiterbildung.

Dabei sind die Betriebsbeauftragten und örtlich Beauftragten für den Datenschutz als strategische Partner des BfD EKD eine wichtige Zielgruppe im Bereich Weiterbildung. Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz benötigen für die Erfüllung ihrer Aufgaben gemäß § 22 Abs. 2 DSG-EKD die erforderliche Fachkunde. Diese Fachkunde vermittelt der BfD EKD den Betriebsbeauftragten und örtlich Beauftragten für den Datenschutz mit einem umfangreichen Weiterbildungsprogramm. Dabei werden mehrere Seminararten und Veranstaltungsformen angeboten (Einzelheiten auf der Homepage des BfD EKD unter https://datenschutz.ekd.de):

- Grundseminare für Datenschutzbeauftragte
- Aufbauseminare für Datenschutzbeauftragte
- Inhouse-Seminare
- Datenschutz-Infotage (Regionalkonferenzen)
- Erfahrungsaustauschkreise

Grundseminare für Datenschutzbeauftragte

Das dreitägige Grundseminar richtet sich an Betriebsbeauftragte und 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. Hierbei ist es unerheblich, ob der Beauftragte bereits zum Betriebsbeauftragten oder örtlich Beauftragten bestellt ist oder erst bestellt werden soll. Die umfangreichen Seminarunterlagen sind im Jahr 2015 erarbeitet worden und wurden für die vier im Jahr 2016 durchgeführten Grundseminare einheitlich verwendet. Die Grundseminare sind bisher vom Hauptsitz des BfD zusammen mit den Außenstellen durchgeführt worden. Im Jahr 2017 werden acht Grundseminare für Datenschutzbeauftragte angeboten, wobei in jeder Datenschutzregion zwei Grundseminare durchgeführt werden. Die Durchführungsverantwortung für die Grundseminare liegt ab dem Jahr 2017 bei den jeweiligen Außenstellen.

Im Grundseminar für Datenschutzbeauftragte wird eine Basisqualifikation zum Datenschutz vermittelt. Schulungsinhalte sind unter anderem:

- Einführung und Sensibilisierung
- Gesetzliche Grundlagen
- Grundzüge des DSG-EKD
- Daten: Erhebung, Verarbeitung, Nutzung
- Rechte der betroffenen Personen
- Bereichsspezifischer Datenschutz
- Praktische Fallbeispiele

- IT-Systeme für Anfänger
- IT-Sicherheit
- Technische und organisatorische Maßnahmen

- Rechtsstellung und Aufgaben des Beauftragten
- Datenschutzorganisation
- Die ersten 100/300 Tage des Datenschutzbeauftragten
- Datenschutzaufsicht

Die Teilnahme am Grundseminar berechtigt zur Teilnahme an den Aufbauseminaren. Die Teilnahmegebühr für das Grundseminar einschließlich Unterbringung und Verpflegung beträgt zurzeit 290,00 €.

Aufbauseminare für Datenschutzbeauftragte

Das Aufbauseminar für Datenschutzbeauftragte ist ein dreitägiges Seminar, das inhaltlich auf der Basisqualifikation vom Grundseminar aufbaut und erstmalig im Frühjahr 2017 angeboten wird. Eine vorherige Teilnahme am Grundseminar für Datenschutzbeauftragte ist von daher Voraussetzung für die Teilnahme an den Aufbauseminaren. Die Aufbauseminare werden getrennt für Datenschutzbeauftragte im Bereich der sogenannten verfassten Kirche und im Bereich Diakonie angeboten und durchgeführt. Die inhaltlichen Themen zum Datenschutz werden entsprechend unterschiedlich gewichtet. Das Aufbauseminar schließt mit einer Hausaufgabe ab. Umfangreiche Seminarunterlagen werden zurzeit erarbeitet und für die jeweiligen Aufbauseminare dann einheitlich verwendet. Die Durchführungsverantwortung der beiden im Jahr 2017 geplanten Aufbauseminare liegt beim Hauptsitz.

Inhouse-Seminare

Zusätzlich werden landeskirchlichen Oberbehörden und diakonischen Landesverbänden eintägige sog. Inhouse-Seminare vor Ort angeboten. Für die Organisation dieser Seminare ist die anfragende Einrichtung zuständig. Der Beauftragte für den Datenschutz der EKD sorgt bei dieser Seminarform für die Inhalte und stellt die Referenten. Bei einem Inhouse-Seminar wird eine kurze Einführung in den rechtlichen und technischen Datenschutz sowie zur Organisation des Datenschutzes gegeben. Die Seminarunterlagen sind im Vorfeld erarbeitet worden und werden für die jeweiligen Seminare einheitlich verwendet. Die Durchführungsverantwortung liegt beim Hauptsitz zusammen mit der jeweiligen Außenstelle.

Datenschutz-Infotag

Außerdem veranstaltet der BfD EKD seit 2015 einmal jährlich in jeder Datenschutzregion mit dem sog. Datenschutz-Infotag deutschlandweit vier Regionalkonferenzen. Bei dieser Tagesveranstaltung wird ein aktuelles Datenschutzthema ausführlich in mehreren Fachvorträgen aus rechtlicher, technischer und praktischer Sicht behandelt. Die Datenschutz-Infotage werden vom Hauptsitz geplant und zusammen mit der jeweiligen Außenstelle durchgeführt.

Erfahrungsaustauschkreise
Zudem finden in allen Datenschutzregionen seit 2015 mehrmals im Jahr Erfahrungsaustauschkreise (sog. Erfa-Kreise) statt. Hier können sich die Betriebsbeauftragten und örtlich Beauftragten untereinander vernetzen und Informationen austauschen. Die Durchführungsverantwortung liegt bei der jeweiligen Außenstelle.

Sensibilisierung
Daneben wird auch die Sensibilisierung von anderen Beschäftigten und (Leitungs-) Gremien zum Thema Datenschutz mit individuellen Weiterbildungen weiter vorangetrieben. Eine (erste) Sensibilisierung ist bei unterschiedlichen Anlässen und in unterschiedlichen Formaten möglich. Im Berichtszeitraum hat der BfD EKD diverse Termine wahrgenommen.

Sensibilisierungen folgender Beschäftigtengruppen sind vom BfD EKD im Berichtszeitraum durchgeführt worden oder folgen in nächster Zeit:

- Gemeindesekretärinnen (auf einer berufsbezogenen Tagung / Weiterbildung)
- Küsterinnen und Küster (auf einer berufsbezogenen Tagung / Weiterbildung)
- Pfarrerinnen und Pfarrer (auf einer Pfarrkonferenz)
- Verwaltungsleitungen (auf einer Verwaltungsleitertagung)
- Superintendenten (auf einer Superintendentenkonferenz)
- Mitarbeitendenvertretungen

Sensibilisierungen folgender (Leitungs-) Gremien sind vom BfD EKD im Berichtszeitraum durchgeführt worden oder folgen in nächster Zeit:

- (Landes-/ Kreis-) Synoden
- „kirchenleitende" Gremien
- Ausschüsse

Zukünftig kann von diesen Angeboten des BfD EKD noch stärker Gebrauch gemacht werden.

Hauptsitz

Seminare
Von Herbst 2015 bis Ende 2016 wurden vom Hauptsitz insgesamt vier Grundseminare für Datenschutzbeauftragte durchgeführt. Die Grundseminare fanden im Johanniterhaus Kloster Wennigsen, im Spenerhaus Frankfurt, in der Evangelischen Bildungsstätte auf Schwanenwerder und im Einkehrhaus der Evangelischen Landeskirche in Württemberg Stift Urach statt. Die Grundseminare waren jeweils ausgebucht. Ein im September 2016 geplantes sog. Zusatzseminar für Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz mit Vorkenntnissen musste wegen zu weniger Anmeldungen abgesagt werden. Im Jahr 2017 werden vom Hauptsitz zwei Aufbauseminare für Datenschutzbeauftragte durchgeführt. Im Frühjahr wird das Aufbauseminar für Datenschutzbeauftragte aus der verfassten Kirche im Johanniterhaus Kloster Wennigsen stattfinden, im Herbst das Aufbauseminar für Datenschutzbeauftragte aus der Diakonie in Haus Villigst, Tagungsstätte der Evangelischen Kirche von Westfalen, bei Schwerte. Inhouse-Seminare fanden im März 2016 im Evangelischen Oberkirchenrat in Karlsruhe und im Oktober 2016 im Landeskirchenamt in Hannover statt. Für Februar 2017 ist ein Inhouse-Seminar beim Oberkirchenrat in Stuttgart geplant.

Datenschutz-Infotage

Im Jahr 2015 und im Jahr 2016 fanden jeweils im April die Datenschutz-Infotage an den vier Standorten der Dienststelle (Berlin, Ulm, Dortmund und Hannover) statt. Die Datenschutz-Infotage standen im Jahr 2015 unter dem Hauptthema „IT-Sicherheit", im Jahr 2016 unter dem Hauptthema „Verschlüsselung". Sowohl im Jahr 2015 als auch im Jahr 2016 haben deutschlandweit an allen vier Datenschutz-Infotagen ca. 250 Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz teilgenommen.

Sensibilisierungen

Daneben sind vom Hauptsitz im Berichtszeitraum Einführungen in den kirchlichen Datenschutz insbesondere auf folgenden Veranstaltungen gegeben worden:

- Tagung der Arbeitsgemeinschaft der Leitungen der kirchlichen Rechnungsprüfungsämter in der EKD (kirpag) am 11. März 2015 in Hildesheim
- Tagung des Westfälisch-Lippischen Verbandes der Mitarbeiterinnen und Mitarbeiter im evangelisch-kirchlichen Verwaltungsdienst (WLV) am 20. April 2015 in Bethel
- 2. Tagung der 12. Landessynode der Evangelischen Landeskirche in Baden am 24. April 2015 in Bad Herrenalb
- Konferenz der Internetbeauftragten in der EKD am 04. Mai 2015 in Berlin
- Arbeitskreis Revision Rechnungswesen Datenschutz (Diakonie) am 22. September 2015 in Hildesheim
- Konferenz der Superintendentinnen und Superintendenten in der Evangelischen Kirche im Rheinland am 29. September 2015 in Wuppertal
- Austausch mit den Jugenddelegierten der EKD-Synode am 05. Oktober 2015 in Hannover
- Austausch im Kirchenamt der EKD, Hauptabteilung III am 12. November 2015 in Hannover
- Austausch mit den IT-Leitenden in der EKD am 15. März 2016 in Hannover
- Konferenz der Verwaltungsleitenden im Evangelischen Missionswerk in Deutschland am 17. März 2016 in Wuppertal
- Studienkurs der VELKD am 08. April 2016 in Pullach
- Chrismon, Redaktionssitzung am 06. Juli 2016 in Frankfurt am Main

Zur Sensibilisierung von Mitarbeitenden startete am 26. Mai 2016 eine zwölfwöchige Posterkampagne unter dem Motto „Datenschutz beginnt bei mir!". Jede Woche wurde ein neues Poster zu den Themen Bildschirmsperre, Passwortstärke und Vertraulichkeit veröffentlicht. Die Poster waren im Kirchenamt der EKD ausgehängt, über die Homepage https://datenschutz.ekd.de verfügbar und konnten in Papierform direkt beim BfD EKD bestellt werden.

Datenschutzregion Nord

Die Mitarbeitenden der Außenstelle Hannover haben im Berichtszeitraum insbesondere folgende individuelle Weiterbildungen durchgeführt:

Workshop für Kirchenvorsteher

In Osnabrück fand im März 2015 ein Workshop für Kirchenvorsteher zum Thema Datenschutz statt. Dabei ging es zum einen um die Vorstellung der Dienststelle und zum anderen um eine rechtliche Einführung in den kirchlichen Datenschutz. Gemeinsam wurden Berührungspunkte mit dem Datenschutz in der Kirchenvorstandsarbeit erörtert. Der Workshop wurde im Februar 2016 wiederholt.

Am 09. März 2016 wurde von der Bremischen Evangelischen Kirche für Kirchenvorsteher ein Workshop zu den Themen Datenschutz und IT-Sicherheitskonzept ausgerichtet. Zum Thema Datenschutz gab die Regionalverantwortliche für die Datenschutzregion Nord eine Einführung in den kirchlichen Datenschutz.

Mitarbeitendenschulung Diakonisches Werk
Am 09. November 2015 wurde im Rahmen einer Schulung des Diakonischen Werks der Ev.-Luth. Kirche in Oldenburg e.V. die Dienststelle des BfD EKD vorgestellt und ein Überblick über das DSG-EKG gegeben.

Jahrestagung Leitende der Kirchenkreisämter
Auf der Jahrestagung der Leiterinnen und Leiter der Kirchen(kreis)ämter der hannoverschen Landeskirche wurden am 25. Mai 2016 über die Aufgaben des Beauftragten für den Datenschutz der EKD und die Aufgaben der örtlich Beauftragten für den Datenschutz referiert.

Tagung zur Informationstechnik
Auf dem jährlichen Treffen der Systemverwalter der hannoverschen Landeskirche wurde am 21. September 2016 eine Einführung in den kirchlichen Datenschutz gegeben. Dabei lag der Schwerpunkt auf den technischen und organisatorischen Maßnahmen.

Erfahrungsaustauschkreise
Für die Betriebsbeauftragten und die örtlich Beauftragten für den Datenschutz gab es am 23. September 2015, am 02. März 2016 und am 28. September 2016 Erfahrungsaustauschkreise. In erster Linie geht es darum, einen Austausch unter den Beauftragten und mit den Mitarbeitenden der Außenstelle Hannover des BfD EKD zu ermöglichen. Die Beauftragten haben im Vorfeld die Möglichkeit Fälle zu schildern und Fragen mitzuteilen, die dann beim Erfahrungsaustauschkreis besprochen werden. Beim ersten Termin standen die Aufgaben eines Betriebsbeauftragten bzw. örtlich Beauftragten für den Datenschutz noch im Vordergrund. Beim zweiten Termin hingegen standen das praktische Herangehen an diese Aufgaben und einige inhaltliche Fragen im Fokus. Beim letzten Erfa-Kreis gab es den Schwerpunkt E-Mail-Verschlüsselung in der Praxis und eine Einführung in das Thema Schweigepflicht. Geplant sind künftig zwei Erfahrungsaustauschkreise pro Jahr.

Datenschutzregion Ost

Die Mitarbeitenden der Außenstelle Berlin haben im Berichtszeitraum insbesondere folgende individuelle Weiterbildungen durchgeführt:

Küsterkurs
Im Rahmen des so genannten „Küsterkurses“ wurden am 02. Oktober 2015 und am 24. Juni 2016 Schulungen zum Thema Datenschutz durchgeführt. Neben einer allgemeinen Einführung in das DSG-EKD wurden besonders relevante Themen für Küsterinnen und Küster thematisiert, beispielsweise, welche personenbezogenen Daten im Gemeindebrief veröffentlicht werden dürfen.

Mitarbeitervertretung
Auf Bitte der Hauptmitarbeitervertretung der EKBO (HMAV) wurde am 23. Mai 2015 eine Schulung zum Thema Datenschutz durchgeführt. Neben allgemeinen Fragen des Datenschutzes wurden auch spezielle Themen zu Datenschutz und der Arbeit der HMAV angesprochen, so etwa die besonderen Anforderungen bei technischen und organisatorischen Maßnahmen gemäß § 9 Abs. 1 DSG-EKD.

Amtsleiterrunde
In einer Sitzung der AG der Vorstände und Amtsleitenden der Kirchenverwaltungsämter der EKBO am 10. Juni 2015 wurde ein Kurzvortrag zum Thema Datenschutz gehalten. Ein Schwerpunkt war die Vorstellung der Dienststelle des BfD EKD, ihr Aufbau und die einzelnen Aufgaben. Interessiert wurde aber auch der Hinweis auf das bevorstehende Inkrafttreten der ITSVO-EKD aufgenommen.

AG Verwaltungsverantwortliche der evangelischen Kommunitäten
Bei einer Tagung der AG der Verwaltungsverantwortlichen des Netzwerks der Konferenz der evangelischen Kommunitäten im Kloster Volkenroda wurde am 01. und 02. Februar 2016 eine Schulung zum Thema kirchlicher Datenschutz und IT-Sicherheit durchgeführt. Nach einer Einführung in das DSG-EKD mit besonderer Berücksichtigung des Beschäftigtendatenschutzes wurde anhand praktischer Fälle die Umsetzung von technischen und organisatorischen Maßnahmen geschult.

Vikariatsausbildung
Im Rahmen der Vikariatsausbildung der EKBO wurde am 01. März 2016 eine Kurzeinführung zum Thema Datenschutz gegeben. Neben allgemeinen Fragen zum Thema Einwilligung und Zweckbindung wurden insbesondere Fragen zum Thema datenschutzkonforme Nutzung sozialer Netzwerke diskutiert.

Beratungsstelle
Am 13. April 2016 wurde eine zweistündige Schulung zum Thema Datenschutz bei der landeskirchlichen Beratungsstelle Arbeitssicherheit und Gesundheitsschutz der EKBO durchgeführt.

Erfahrungsaustauschkreise
Um die Vernetzung zwischen den Betriebsbeauftragten und den örtlich Beauftragten für den Datenschutz in der Datenschutzregion Ost zu unterstützen, führte die Außenstelle am 19. November 2015 und am 08. März 2016 Erfahrungsaustauschkreise durch. Es wurden alle der Außenstelle bekannten Datenschutzbeauftragten der Datenschutzregion Ost dazu eingeladen, konkrete Fragestellungen und aktuelle Themen in den Bereichen Datenschutz und Datensicherheit zu diskutieren. Ein Schwerpunkt liegt im Austausch über Ausgestaltung der konkreten Datenschutzorganisation in der jeweiligen Einrichtung.

Datenschutzregion Süd

Die Mitarbeitenden der Außenstelle Ulm haben im Berichtszeitraum insbesondere folgende individuelle Weiterbildungen durchgeführt:

Schulungen von Pfarramtssekretärinnen
Die einwöchigen Schulungen zur Pfarramtssekretärin in der Landeskirche Württemberg enthalten regelmäßig (zuletzt am 23. Februar 2016) einen Nachmittag, in dem den angehenden Sekretärinnen das Wichtigste zum Thema Datenschutz erläutert wird.

Viele Aspekte gemeindlichen Handelns laufen bei den Pfarramtssekretärinnen zusammen. Deshalb ist es von großer Wichtigkeit, dass diese mit den Bestimmungen des kirchlichen Datenschutzgesetzes möglichst gut vertraut sind und damit ein Umgang mit personenbezogenen Daten, der das Persönlichkeitsrecht der Betroffenen verletzten könnte, von vornherein erkannt wird.

Beschäftigtendatenschutz und IT-Sicherheit

Bei kirchlichen Mitarbeitenden ist ein stark wachsendes Interesse an Datenschutzfragen zu erkennen. Der Beschäftigtendatenschutz wird auch hier Thema. Um genauer zu sehen, wo die Fragen und Probleme liegen, wurden bei Mitarbeiterversammlungen am 09. November 2015, am 20. und 23. November 2015 und am 25. Februar 2016 Vorträge mit anschließender Diskussion gehalten.

Im Kern ging es darum, dass auf der einen Seite kirchliche Stellen immer komplexere Verfahren einsetzen, um ihren Anforderungen genügen zu können, und auf der anderen Seite Anwendertätigkeiten einer immer weiter gehenden Protokollierung unterliegen. Die Anforderungen des Datenschutzes müssen damit auf intelligente Weise in Einklang gebracht werden. Dies zu leisten, ist eine hohe Anforderung auch an Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz.

Erfahrungsaustauschkreise

Die Tätigkeit der Betriebsbeauftragten und örtlich Beauftragten für den Datenschutz ist nicht einfach und bedarf der ständigen Fortbildung, auch wenn sich diese bei schwierigen Fragen an die Außenstelle Ulm wenden können. Aber die Verhältnisse vor Ort kennen die Betriebsbeauftragten und örtlich Beauftragten am besten.

Deshalb wurden am 19. November 2015 und am 14. Juli 2016 Erfa-Kreise in der Datenschutzregion Süd in der Form durchgeführt, dass am Vormittag ein Referent ein praxisbezogenes Referat gehalten hat und am Nachmittag, moderiert vom Regionalverantwortlichen, Austausch untereinander und Networking betrieben wurde. Der nächste Erfa-Kreis ist für den 01. Dezember 2016 geplant.

Datenschutzregion Mitte-West

Die Mitarbeitenden der Außenstelle Dortmund haben im Berichtszeitraum insbesondere folgende individuelle Weiterbildungen durchgeführt:

Datenschutz in medizinischen Einrichtungen

Einen Schwerpunkt der Arbeit stellt der Datenschutz in diakonischen Einrichtungen dar. Der Datenschutz hat im Gesundheitssektor oberste Priorität. Gerade dort, wo mit besonderen Arten personenbezogener Daten wie Gesundheitsdaten gearbeitet wird, muss der Schutz dieser Daten von allen Beteiligten gelebt und umgesetzt werden. Da im Gesundheitsbereich darüber hinaus immer wieder neue komplexe IT-Lösungen in den Workflow integriert werden, die eine datenschutzrechtliche Vorabkontrolle sowie eine professionelle Betreuung im operativen Betrieb benötigen, versuchen die Mitarbeitenden der Außenstelle Dortmund den Kontakt mit den Betriebsbeauftragten der Einrichtungen stetig zu intensivieren und so gemeinsam den Herausforderungen begegnen zu können. Gerade das Zusammentreffen von Datenschutz und den der ärztlichen Schweigepflicht unterfallenden Gesundheitsdaten erfordert auch wegen der Zusammenarbeit mit externen Dienstleistern juristisch klar formulierte Vorgaben und regelmäßige Fortbildung.

Daher referieren Mitarbeitende der Außenstelle Dortmund im Rahmen von verschiedenen Veranstaltungen von diakonischen Einrichtungen regelmäßig zu diesem Thema.

Sensibilisierung Gremien und Mitarbeitende

Um für das Thema Datenschutz zu sensibilisieren, referieren Mitarbeitende der Außenstelle ebenso regelmäßig vor verschiedenen Gremien der Gliedkirchen in der Datenschutzregion Mitte-West.

Da das Thema mittlerweile auch Einzug in das Bewusstsein der Mitarbeitenden gefunden hat, haben die Mitarbeitenden der Außenstelle Dortmund auch bereits vor unterschiedlichen Beschäftigtengruppen individuelle Schulungen gehalten. Insbesondere im Bereich der Gemeindesekretärinnen, der Ehrenamtlichen und bei den Mitarbeitervertretungen freuen sich die Mitarbeitenden der Außenstelle regelmäßig über Einladungen und das weiterhin wachsenden Interesse.

Erfahrungsaustauschkreise

Der Austausch und die Vernetzung sind auch unter den Betriebsbeauftragten und örtlich Beauftragten für den Datenschutz wichtig. Aus diesem Grund waren Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz aus der Datenschutzregion Mitte-West am 02. Februar 2016 erstmalig zum Erfahrungsaustauschkreis (Erfa-Kreis) ins Reinoldinum nach Dortmund eingeladen. Mit über 80 Teilnehmenden wurde der Auftakt für ein neues Format gemacht. Am 17. und 18. Oktober 2016 haben erstmalig getrennte Erfa-Kreise für den Bereich der sog. Verfassten Kirche und der Diakonie stattgefunden.

Um über die grundsätzliche Schulung im Rahmen von Seminaren hinaus praxisnahe Probleme besprechen und einfache Lösungen finden zu können, sind die Erfa-Kreise initiiert worden. Die Erfa-Kreise sollen dazu dienen, aktuelle und konkrete Themen des Datenschutzes zu besprechen, das Netzwerk zu stärken und den internen Austausch untereinander anzuregen. Daher wird den Teilnehmern die Gelegenheit gegeben, eigene Themen anzusprechen und Themenwünsche vorab einzureichen. Insofern wurde im Rahmen der Veranstaltung sowohl juristisch als auch technisch über Lösungen zu den aufgeworfenen Fragestellungen referiert und anschließend ein offener Austausch zu aktuellen Themen angeregt. Gerade auch das Networking und der Austausch untereinander sorgen für Synergieeffekte und Motivation.

Über die Dienststelle des BfD EKD

IV

Doch auch sonst gibt es allerhand Wissenswertes und Interessantes aus der Dienststelle des BfD EKD zu berichten! Darüber informiert das vierte Kapitel des Tätigkeitsberichts.

Infrastruktur

Im Rahmen der grundlegenden organisatorischen Festlegungen im Organigramm wurden in der Dienststelle zwischenzeitlich die Funktion der örtlich Beauftragten für den Datenschutz und der IT-Sicherheitsbeauftragten implementiert. In Ausgestaltung dieser grundlegengenden Festlegungen konnten zwischenzeitlich im Bereich der rechtlichen Infrastruktur folgende konkreten Festlegungen getroffen werden:

- Geschäftsverteilungsplan
- Aktenplan
- Dienstvereinbarungen (z.B. zur privaten Nutzung von Internet und E-Mail etc.)
- Diverse Hausverfügungen (z.B. zu Vertretungsregelungen, Zeichnungsbefugnissen etc.)
- Diverse Prozessbeschreibungen (zur Etablierung eines Qualitätsmanagementsystems)
- Leitlinien zur Informationssicherheit und zum Datenschutz

Diese konkreten Festlegungen dienen der weiteren Implementierung einer unabhängigen Behörde und werden ständig auf dem aktuellen Stand gehalten.

Im Bereich der technischen Infrastruktur wurde das im Sachstandsbericht von September 2014 beschriebene eigenständige IT-Konzept des BfD EKD erfolgreich umgesetzt. Somit sind nunmehr alle Standorte des BfD EKD sicher miteinander vernetzt, und eine zentrale Terminalserverlösung konnte etabliert werden. Diese zentrale Struktur ermöglichte dem BfD EKD auch die Einführung eines (digitalen) Aktenplans, in dem nicht nur analoge, sondern auch digitale Informationen zentral abgelegt und durch ein Rollenkonzept gesichert werden.

Zur Absicherung der digitalen Kommunikation hat der BfD EKD verschiedene Möglichkeiten der Ende-zu-Ende-Verschlüsselung eingeführt. 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 unserer Webseite Ende-zu-Ende verschlüsselt mit uns zu kommunizieren. Hierbei werden die entstehenden Metadaten zusätzlich durch eine Transportverschlüsselung gesichert. Sollten Gesprächspartner keine Möglichkeit der Ende-zu-Ende-Verschlüsselung mittels PGP besitzen, so können diese auf die alternative Submit Box ausweichen, welche eine Ende-zu-Ende verschlüsselte Kommunikation mit dem BfD EKD ermöglicht.

Im Rahmen des Aufbaus und der Professionalisierung der technischen Infrastruktur der Dienststelle arbeitet der BfD EKD auch an der Erstellung und Umsetzung eines eigenen – von der IT-Sicherheitsverordnung EKD geforderten – IT-Sicherheitskonzeptes nach dem Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). So konnten bereits viele technische und organisatorische Maßnahmen umgesetzt werden. In diesem Zusammenhang hat der BfD EKD auch eigene Regeln für die Klassifizierung von Informationen erarbeitet und eine IT-Sicherheitsbeauftragte benannt.

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 sicherzustellen, dass die Dienststellenleitung einheitliche und verlässliche organisatorische und inhaltliche Absprachen mit den Mitarbeitenden treffen kann. Grundsätzlich einmal im Monat treffen sich alle Mitarbeitenden am Hauptsitz in Hannover zu einer hierarchieübergreifenden halbtägigen Dienstbesprechung. Einmal im Jahr findet die Dienstbesprechung rotierend an einem anderen Standort der Dienststelle des BfD EKD statt. Im Frühjahr und im Herbst finden jeweils zweitägige Dienstbesprechungen als Klausurtagungen statt. Die Dienstbesprechungen werden vom Dienststellenleiter oder dessen Vertreter geleitet. Zur Ergebnissicherung werden über die Dienstbesprechungen interne Protokolle erstellt. Am Ende des Jahres 2017 soll überprüft werden, ob weiterhin regelmäßige Dienstbesprechungen mit persönlicher Anwesenheit am

Hauptsitz in Hannover stattfinden oder durch regelmäßige Videokonferenzen ersetzt werden. Zum fachlichen Austausch finden zwischen den Dienstbesprechungen regelmäßig Telefonkonferenzen unter den Mitarbeitenden mit der gleichen Funktion innerhalb der Dienststelle (Regionalverantwortliche, IT-Sachbearbeitende und Teamassistenz) statt. Davon unabhängig organisieren sich in den Außenstellen der Dienststelle die Mitarbeitenden eigenständig zum weiteren fachlichen und organisatorischen Austausch.

Die Außenstellen und der Hauptsitz sind bereits seit Ende 2014 im Rahmen der sachlichen Infrastruktur mit den erforderlichen Büromöbeln, technischen Endgeräten (Telefonie, Rechner, Multifunktionsgeräte etc.) sowie sonstigem Inventar ausgestattet. Im Rahmen des geplanten Ausbaus der Außenstelle Hannover wurde zwischenzeitlich am Standort Böttcherstraße in Hannover eine weitere Etage angemietet. Die Außenstelle in Berlin wurde vom Gebäude des Evangelischen Werkes für Diakonie und Entwicklung (EWDE) verlegt in ein in der Nähe des bisherigen Standorts liegendes anderes Geschäftshaus (Vermieter: Verband diakonischer Dienstgeber Deutschlands).

Finanzen

Die Personal- und Sachkosten des BfD EKD werden durch Finanzumlage derjenigen finanziert, die die Datenschutzaufsicht auf vertraglicher oder gesetzlicher Grundlage auf die EKD übertragen haben. Der Finanzbeirat der EKD hat im März 2016 den mittelfristigen Finanzbedarf der Dienststelle für Personal- und Sachkosten festgelegt mit der Maßgabe, dass alle Gliedkirchen und diakonischen Landesverbände die Datenschutzaufsicht auf die EKD übertragen. Dabei werden diese Kosten in Höhe von zwei Drittel 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 zur einen Hälfte auf der Grundlage des Schlüssels Gemeindegliederzahlen und zur anderen Hälfte auf der Grundlage des Schlüssels Beschäftigtenzahlen. Im Bereich der Diakonie werden die Umlagen nur auf der Grundlage des Schlüssels Beschäftigtenzahlen ermittelt. Diese mathematisch nach unterschiedlichen Schlüsseln errechnete Umlage muss erst nach der tatsächlichen Übertragung der Datenschutzaufsicht auf die EKD erbracht werden. Einzelheiten sind den Haushaltsplänen und Haushaltsabschlüssen der EKD zu entnehmen.

Die Finanz- und Budgethoheit liegt beim BfD EKD. In allen Finanz- und Haushaltsangelegenheiten wird der BfD EKD von der Abteilung Finanzen im Kirchenamt der EKD unterstützt. Die praktische Umsetzung und Abwicklung erfolgt überwiegend unmittelbar durch die Dienststelle des BfD EKD.

Personal

Nachdem der personelle Aufbau am Hauptsitz bereits im Jahre 2014 abgeschlossen war, ist nunmehr auch der personelle Aufbau in den Außenstellen grundsätzlich abgeschlossen. Alle vier Außenstellen sind mit einer oder einem Regionalverantwortlichen (juristische Kompetenz), einer IT-Sachbearbeitung und einer Teamassistenz besetzt. Somit arbeiten zum 01. Januar 2017 insgesamt 16 Mitarbeitende beim BfD EKD. Es ist anzumerken, dass die Besetzung der IT-Sachbearbeitungsstellen vor dem Hintergrund der Rahmenbedingungen langwierig und schwierig gewesen ist. Im Sinne einer kontinuierlichen Personalentwicklung haben alle Mitarbeitenden an mehrtägigen Weiterbildungsmaßnahmen teilgenommen.

Es ist beabsichtigt im Rahmen der fortschreitenden Übertragung der Datenschutzaufsicht der diakonischen Landesverbände in den Außenstellen drei weitere Regionalverantwortliche einzustellen. Auch zukünftig werden Mitarbeitende potenzial- und genderorientiert ausgewählt.

Die Teams der Außenstellen organisieren sich bei der Aufgabenerledigung unter Berücksichtigung des Geschäftsverteilungsplanes selbständig, ohne dass ein Mitarbeitender vor Ort Leitungsverantwortung hat. Somit unterstehen alle Mitarbeitenden der Fach- und Dienstaufsicht des Beauftragten für den Datenschutz der EKD. In diesem Zusammenhang werden mit allen Mitarbeitenden regelmäßig strukturierte Mitarbeitendengespräche geführt.

Im Bereich der Personalverwaltung wird der BfD EKD von der Personalabteilung im Kirchenamt der EKD unterstützt.

Vertretung in Gremien, Konferenzen und Arbeitsgruppen der EKD

Der Beauftragte für den Datenschutz der EKD bzw. sein Vertreter sind persönlich in mehreren Gremien, Konferenzen und (temporären) Arbeitsgruppen der EKD (als Gast) vertreten.

- Gremien (Organ der EKD)
  - Synode der EKD (mit Gaststatus)
- Konferenzen
  - Sitzung der Leitenden Juristinnen und Juristen in den zentralen Verwaltungen der Gliedkirchen der EKD
  - Referentenkonferenzen der EKD
    - Referentenkonferenz für Datenschutz, Meldewesen und Kirchenmitgliedschaftsrecht
    - IT-Referentenkonferenz der EKD
- Arbeitsgruppen (AG)
  - AG Bring Your Own Device
  - AG Novellierung DSG-EKD
  - AG Personalverwaltungsprogramm
  - AG Praxisleitfaden Softwareprüfung und -freigabe
  - AG Social Media
  - AG IT-Sicherheitskonzept (AG nach Aufgabenerledigung eingestellt)

Unabhängig davon trägt der Beauftragte für den Datenschutz der EKD seine Angelegenheiten eigenständig dem Rat der EKD, gegebenenfalls auch der Kirchenkonferenz und dem Finanzbeirat der EKD vor.

Vernetzung

Um den BfD EKD in kirchlichen und staatlichen Strukturen nachhaltig zu etablieren, baut der BfD EKD ein umfangreiches Netzwerk auf. Hierfür sind in den letzten zwei Jahren vielfältige Kontakte geknüpft worden, die auch zukünftig weiter ausgebaut und gepflegt werden.

In der evangelischen Kirche

Der BfD EKD tauscht sich einmal im Jahr im persönlichen Gespräch mit dem Ratsvorsitzenden der EKD, der Dienstvorgesetzter des BfD EKD ist, 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.

Der BfD EKD und sein Vertreter stehen in regelmäßigem Kontakt zur Leitungsebene (insbesondere leitende Juristinnen und Juristen sowie Vorstände) und zur operativen Ebene (insbesondere Datenschutzreferenten und ITler) der Landeskirchen und diakonischen Landesverbänden, die die Datenschutzaufsicht auf die EKD übertragen haben. Neben diesen Kontakten werden landeskirchliche Vertreter auch in die eigenen Arbeitsgruppen des BfD EKD eingebunden. Darüber hinaus hat der BfD EKD im Jahr 2016 zwei Vernetzungstreffen für IT-Verantwortliche in den Gliedkirchen und diakonischen Landesverbänden organisiert. Im Jahr 2017 soll erstmalig ein Vernetzungstreffen auch für die Leitungen der Rechnungsprüfungseinrichtungen innerhalb der EKD organisiert werden.

Der BfD EKD und sein Vertreter stehen auch in Erfüllung des gesetzlichen Auftrags zur Zusammenarbeit in regelmäßigem Kontakt zu den anderen Beauftragten für den Datenschutz innerhalb der EKD. Einmal im Jahr wird zu Fragen des kirchlichen Datenschutzes die Tagung der Konferenz der Beauftragten für den Datenschutz in der EKD unter Vorsitz des BfD EKD durchgeführt. Organisiert wird die Tagung jährlich wechselnd von einer Landeskirche bzw. einem diakonischen Landesverband und dem BfD EKD. Im Jahr 2015 hat die Konferenz in Dessau (Veranstalter: Evangelische Landeskirche Anhalts) und im Jahr 2016 in Köln (Veranstalter: BfD EKD) stattgefunden. Im Jahr 2017 wird die Tagung in Hamburg (Veranstalter: Evangelisch-Lutherische Kirche in Norddeutschland) stattfinden. An den Tagungen nimmt regelmäßig der Sprecher der Datenschutzbeauftragten in der römisch-katholischen Kirche teil. Im Rahmen der Zusammenarbeit ist im Berichtszeitraum die Entschließung der Konferenz der Datenschutzbeauftragten in der Evangelischen Kirche in Deutschland zum Thema Cloud Computing erarbeitet und am 01. Juli 2015 verabschiedet und veröffentlicht worden.

Zur römisch-katholischen Kirche

Der BfD EKD und sein Vertreter stehen in regelmäßigem Kontakt zu den Datenschutzbeauftragten in der römisch-katholischen Kirche. Neben Kontakten in persönlichen Gesprächen nimmt der BfD EKD regelmäßig als Gast an den Tagungen der Konferenz der Beauftragten für den Datenschutz in der römisch-katholischen Kirche teil (im Jahr 2015 in Köln).

Im April 2016 haben beide Konferenzen erstmalig einen ökumenischen Datenschutztag in Köln organisiert. Referenten waren der Vizepräsident der Bundesamtes für Sicherheit in der Informationstechnik (BSI) Andreas Könen sowie der Referatsleiter für Datenschutz im Bundesministerium des Inneren, Dr. Jost Onstein und der Referatsleiter Compliance in der Bundesanstalt für Finanzdienstleistungsaufsicht, Dr. Martin Eßer.

Zu Bund und Ländern

Der BfD EKD und sein Vertreter stehen in regelmäßigem Kontakt zur Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie den Landesbeauftragten für Datenschutz und Informationsfreiheit. Im Berichtszeitraum konnte sich der BfD EKD im Rahmen von Antrittsbesuchen mit allen Landesbeauftragten (auf dem Gebiet der Gliedkirchen und diakonischen Landesverbände, die die Datenschutzaufsicht auf die EKD übertragen haben) und der Bundesbeauftragten über die gemeinsamen Aspekte des staatlichen und kirchlichen Datenschutzes austauschen. In allen Gesprächen wurde bekräftigt, auch zukünftig intensiv zu kooperieren. Zudem ist vor dem Hintergrund der Regelungen in der EU-Datenschutz-Grundverordnung beabsichtigt, dass zukünftig eine Beteiligung der Kirchen im Rahmen des sog. Kohärenzprinzips erfolgt, sofern Belange des kirchlichen Datenschutzes betroffen sind.

Zu den öffentlich-rechtlichen Rundfunk- und Fernsehanstalten

Auch zur eigenständigen Datenschutzaufsicht im Bereich der öffentlich-rechtlichen Rundfunk- und Fernsehanstalten werden regelmäßige Kontakte gepflegt.

Zu sonstigen Akteuren

Darüber hinaus stehen der BfD EKD und sein Vertreter zu weiteren „Playern" im Bereich Datenschutz und IT-Sicherheit im Umfeld von Politik, Gesellschaft und Wissenschaft in Kontakt:

- Netzpolitische Sprecher der im Bundestag vertretenen Fraktionen: Im Berichtszeitraum hat es Gespräche mit den netzpolitischen Sprechern der Bundestagsfraktion Bündnis 90/Die Grünen, MdB Dr. Konstantin von Notz, und der Bundestagsfraktion der SPD, MdB Gerold Reichenbach, gegeben. Gespräche mit den netzpolitischen Sprechern der weiteren im Bundestag vertretenen Fraktionen werden im Jahr 2017 stattfinden.
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Im Berichtszeitraum hat es einen Gedankenaustausch mit dem Vizepräsident des BSI, Andreas Könen, gegeben. Darüber hinaus hat der Vertreter des BfD EKD im Mai 2015 am Deutschen IT-Sicherheitskongress in Bonn-Bad Godesberg teilgenommen.
- Stiftung Datenschutz: Im Berichtszeitraum hat es mehrere Gespräche mit dem Vorstand der Stiftung, Frederick Richter, gegeben, der im Jahr 2015 als Referent an einer Klausurtagung des BfD EKD teilgenommen hat.
- Institut für Rechtsinformatik (IRI), Institut der juristischen Fakultät der Gottfried Wilhelm Leibniz Universität Hannover: Im Berichtszeitraum hat es zu mehreren Anlässen Gesprächskontakte zum Leiter des IRI, Prof. Dr. Nikolaus Forgó, und dessen Mitarbeitenden gegeben. Darüber hinaus ist der BfD EKD Mitglied in einem Gesprächskreis des IRI.

Der BfD EKD ist Mitglied in folgenden Interessenvertretungen:

- Virtuelles Datenschutzbüro
- Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
- Gesellschaft für Informatik (GI) e.V.
- Allianz für Cybersicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Öffentlichkeitsarbeit

Unter den bisherigen Mottos „Datenschutz ist Menschenschutz!“ und „Datenschutz beginnt bei mir!“ verfolgt der BfD EKD das Ziel, mit gezielten Aktionen, Produkten und Plattformen das Thema kirchlicher Datenschutz modern, attraktiv und leicht in die kirchliche Öffentlichkeit und an den Menschen zu bringen.

Internetauftritt

Der wichtigste Kommunikationskanal des BfD EKD ist dessen Internetauftritt. Der Internetauftritt ist im Jahr 2015 vom BfD EKD konzeptionell entworfen und operativ umgesetzt worden. Seit dem nutzt der BfD EKD diese Plattform, um aktuelle Informationen, Materialen und Arbeitshilfen zur Verfügung zu stellen. So werden alle datenschutzrechtlich relevanten Regelungen der Gliedkirchen sowie die Struktur und die Dienststelle des BfD EKD dargestellt. Der weitaus größere und wichtigere Teil stellen allerdings aktuelle Artikel zum Thema rechtlicher und technischer Datenschutz dar. Darüber hinaus können alle interessierten Personen in der Infothek Entschließungen, Handreichungen, Kurzinformationen und Muster sowie Materialien zur Sensibilisierung herunterladen.

Interviews

Im Rahmen der EKD Synode 2014 mit dem Schwerpunktthema „Kommunikation des Evangeliums in der digitalen Gesellschaft“ wurde ein Lesebuch vom Gemeinschaftswerk der Evangelischen Publizistik (GEP) im Auftrag der EKD produziert. In diesem Lesebuch ist unter anderem ein Interview unter dem Titel „Menschen schützen, nicht Daten“ mit Michael Jacob und Dr. Sascha Tönnies abgedruckt, welches durch den EPD durchgeführt wurde.

Europäischer Datenschutztag

Der Europäische Datenschutztag ist ein Aktionstag für den Datenschutz und wurde auf Initiative des Europarats ins Leben gerufen. Er wird seit 2007 jährlich am 28. Januar begangen, da 1981 an diesem Tag die Europäische Datenschutzkonvention unterzeichnet wurde. Ziel des Europäischen Datenschutztages ist es, die Bürger Europas für den Datenschutz zu sensibilisieren. Dies soll durch Aktionen aller mit dem Datenschutz betrauten Organisationen erfolgen. Deswegen hat sich seit dem Jahr 2015 auch der BfD EKD an diesem Aktionstag beteiligt. In 2015 hat der BfD EKD hierfür einen Stand im Kirchenamt der EKD in Hannover aufgebaut und Gimmicks verteilt. In netter Atmosphäre bei einer Tasse Kaffee konnten sich außerdem alle Mitarbeitenden des Kirchenamtes über den Datenschutz informieren. In 2016 hat der BfD EKD dieses Konzept dann auf alle Datenschutzregionen ausgeweitet. Am 28. Januar 2016 haben in vier landeskirchlichen Oberbehörden und im Evangelischen Werk für Diakonie und Entwicklung in Berlin entsprechende Veranstaltungen stattgefunden.

Posterkampagne

Im Sommer 2016 hat der BfD EKD eine zwölfwöchige Posterkampagne durchgeführt. Hierfür wurden in der Dienststelle des BfD EKD 12 Poster entwickelt und darin die Themen Vertraulichkeit, Passwortqualität und das Sperren von Bildschirmen aufgegriffen. Jedes dieser Themen umfasste vier Poster, die aufei-

nander aufbauend präsentiert wurden. Die Poster hat der BfD EKD wöchentlich im Internet veröffentlicht und zum Herunterladen angeboten. Parallel dazu fand im Kirchenamt der EKD mit dem Ziel, Mitarbeitende für die Themen zu sensibilisieren, eine Posterausstellung statt. Bereits vor dem Start der Kampagne hatten die Gliedkirchen die Möglichkeit, die Poster direkt beim BfD EKD zu bestellen. Von dieser Möglichkeit haben viele Gliedkirchen und örtlich Beauftragte für den Datenschutz Gebrauch gemacht.

Werbematerial

Um auf verschiedene Art und Weise Menschen für das Thema Datenschutz zu interessieren, haben Mitarbeitende des BfD EKD unterschiedliche Werbematerialen erstellt, die bei diversen Anlässen verwendet werden:

- Webcam Blocker: Hierbei handelt es sich um kleine, selbstklebende und wieder ablösbare Aufkleber, die auf Webcams in Laptops geklebt werden können. Webcam Blocker sollen verhindern, dass fest verbaute Webcams ohne Kenntnis des Benutzers Bilder aufzeichnen können.
- Postkarten: Unter dem Motto „Datenschutz beginnt bei mir!“ hat der BfD EKD Postkarten entwickelt, auf denen einige praktische Tipps zum Umgang mit dem Thema Datenschutz im Alltag abgedruckt sind.
- Passwortkarten: Das sind Karten in der Größe von Visitenkarten, die es einem ermöglichen sollen, sich unterschiedliche Passwörter für unterschiedliche Dienste merken zu können.
- Kugelschreiber: Mit Slogan und Internetadresse des BfD EKD beschriftete Kugelschreiber sowie Blöcke mit vollständigen Kontaktinformationen werden vor allem bei den Weiterbildungsangeboten des BfD EKD verteilt und genutzt.

Printprodukte

Unter dem Sammelbegriff Printprodukte versteht der BfD EKD alle Produkte, die auch in gedruckter Form beim BfD EKD bestellt werden können. Dazu gehören bis jetzt die Kurzinformation „Datenschutz in Kindertagesstätten“, die Handreichung „Datenschutz im Gemeindebrief“ und die Poster der Posterkampagne.

Der Beauftragte für den Datenschutz
der Evangelischen Kirche in Deutschland
Böttcherstraße 7
30419 Hannover

Telefon: +49 (0) 511 768128-0
Telefax: +49 (0) 511 768128-20
E-Mail: info@datenschutz.ekd.de
Internet: https://datenschutz.ekd.de