



Unabhängige Aufsichtsbehörde
für den Datenschutz

Evangelisch-Lutherische
Kirche in Norddeutschland

Bericht des Beauftragten für den Datenschutz
der Evangelisch-Lutherischen Kirche
in Norddeutschland
an die Landessynode und die Kirchenleitung
im September 2019

Herausgeber

Unabhängige Aufsichtsbehörde für den Datenschutz
der Evangelisch-Lutherischen Kirche in Norddeutschland

Peter von Loeper

Münzstr. 8-10

19055 Schwerin

03998 2598478

peter.loeper@dsb.nordkirche.de

www.datenschutz-nordkirche.de



Inhaltsverzeichnis

1. Einführung	3
2. Novelle des Datenschutzgesetzes der EKD	6
3. Zusammenarbeit	9
3.2. Kooperation Beauftragten für den Datenschutz EKD	9
3.2. Zusammenarbeit römisch-katholischem Datenschutz	11
3.3. Landesdatenschutzbeauftragte HH, M-V u. S-H	11
3.4. Krankenhausprojekt UPDK	12
4. Anforderungen an die Datenschutzaufsicht	13
5. Örtliche Datenschutzbeauftragte	17
6. Information der kirchlichen Öffentlichkeit	19
7. Facebook	19
7.1. Verfahren	19
7.2. Kartellverfahren	21
7.3. Politische Situation	21
8. Messengerdienste	23
9. Microsoft	25
10. Datenpannen	27
11. Auftragsverarbeiter	29
12. Beschwerden/Betroffenen Anfragen	29
13. Fundraising	30
14. Schulung	30



Verehrtes Präsidium, hohe Synode, sehr geehrte Kirchenleitung!

Heute übergebe ich Ihnen meinen Bericht über die Situation des Datenschutzes in der Nordkirche und meine Tätigkeit. Ursprünglich war es vorgesehen, den Bericht auf der Tagung der Landessynode am 02.03.2019 vorzustellen. Das ist dann auf die nächste, heutige Synodentagung vertagt worden.

In meinem Bericht werde ich die Novelle des DSGVO-EKD, deren Hintergründe und Auswirkungen für unsere Kirche ansprechen und neue Kooperationen innerhalb der Kirche und mit staatlichen Stellen vorstellen. Ein weiterer Schwerpunkt wird die Nutzung von Facebook, WhatsApp, und Co. sein. Die Firma Microsoft bietet hervorragende Clouddienste an, die von unserer Kirche gut genutzt werden könnten. Im Anschluss gibt es eine Aufstellung der wesentlichen aufgetretenen Fallkategorien.

Der Bericht wird auf www.datenschutz-nordkirche.de veröffentlicht.

September 2019

Peter Loeper
Beauftragter für den Datenschutz
der Nordkirche



1. Einführung

Datenschutz ist kompliziert, ist teuer und führt nicht zu praktischen Ergebnissen. Datenschutz hält von der eigentlichen Arbeit ab und nervt. Datenschutz beschränkt uns in der schönen, schnellen, digitalen Welt. Wir fühlen uns gefangen in einem komplizierten bürokratischen Netz aus Vorschriftenen.

Ich zitiere aus der Einführung des DSGVO-EKD 2002 durch den Rat der EKD: *„Datenschutz ist Persönlichkeitsschutz. Unsere Persönlichkeit macht aus, was wir denken, meinen, fühlen, tun, unterlassen, erfahren und erinnern. Von all dem teilen wir anderen immer nur so viel mit, wie es uns gerade zweckmäßig und sinnvoll erscheint. Beim Datenschutz geht es also nicht um Geheimniskrämerei, sondern ... um die Freiheit des Einzelnen, zu entscheiden, was er aus seinem Leben und aus seiner Lebenssituation mitteilt, und was er gestattet, was andere aus diesem Wissen machen.“*

In seinem Volkszählungsurteil hat das Bundesverfassungsgericht schon 1983 das Recht auf informationelle Selbstbestimmung als Grundrecht aus dem Recht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) und der Würde des Menschen (Art. 1 Abs. 1 GG) abgeleitet. Jeder Einzelne hat die Befugnis *„grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“*

Aber wir haben gerade in den zwei letzten Jahren gelernt, dass Datenschutz nicht nur dem Schutz der Privatheit des Einzelnen dient. Man denke an den Einsatz von Social Bots im Wahlkampf, die Verbreitung von Fake News oder alternativen Fak-



ten, den Cambridge Analytica Skandal¹ oder den begründeten Verdacht der Wahlbeeinflussung in den USA und Großbritannien. Menschen, Wähler verschwinden in sog. Filterblasen². Dann ist Datenschutz auch eine Voraussetzung für das Funktionieren einer modernen, offenen Demokratie.

Datenschutzrecht seinerseits reagiert auf strukturelle Konflikte. Zwischen mächtigen Organisationen einerseits und dem Einzelnen andererseits bestehen häufig asymmetrische Machtbeziehungen, die durch das Recht eingehegt werden müssen. Mächtige Organisationen sind in diesem Zusammenhang nicht nur Staaten oder Google, sondern auch z.B. Versicherungen, Krankenhäuser, Beratungsstellen oder Kindergärten, denen ich mich als Individuum anvertraue oder anvertrauen muss.

Pointiert gesagt hat Datenschutz nur vordergründig den Schutz von persönlichen Daten zur Aufgabe, vor allem schützt er die Grundrechte, die Freiheit und die Würde des Menschen und damit auch unsere freiheitlich demokratische Grundordnung.

¹ Cambridge-Analytica-Skandal: Vor rund fünf Jahren gaben Entwickler einer Umfrage-App Informationen von Tutzenden Millionen Facebook-Nutzern an die Datenanalyse-Firma Cambridge Analytica weiter.

² Die Filterblase (englisch *filter bubble*) oder Informationsblase ist ein Begriff der Medienwissenschaft, der vom Internetaktivisten Eli Pariser in seinem gleichnamigen Buch von 2011 verwendet wird. Laut Pariser entstehe die Filterblase, weil Webseiten versuchen, algorithmisch vorauszusagen, welche Informationen der Benutzer auffinden möchte – dies basierend auf den verfügbaren Informationen über den Benutzer (beispielsweise Standort des Benutzers, Suchhistorie und Klickverhalten). Daraus resultiere eine Isolation gegenüber Informationen, die nicht dem Standpunkt des Benutzers entsprechen. (Wikipedia)



Das Spannungsverhältnis zwischen freier Entfaltung der digitalen Anwendungsmöglichkeiten und dem Schutz der Rechte der Einzelnen ist zutiefst konfliktrichtig. Nicht weiter hilft es uns die alten Schlachten mit fundamentalen Positionen zu führen. Auch nach dem Datenschutzrecht muss der freie Informationsfluss gewährleistet sein (Art. 1 Nr. 3 EU-DSGVO). Andererseits kann es auch nicht nach dem Grundsatz „digital first“ gehen, sondern das technisch Mögliche muss menschlich gestaltet werden. In der Gesellschaft wird diese Thematik immer intensiver diskutiert. Mit Freude habe ich wahrgenommen, dass sich die Landessynode mit ihrem Digitalisierungsausschuss auch dieser Debatte zuwenden will. Die vielen Aspekte, die bei der Vorstellung der Mitglieder auf der letzten Synodentagung zur Sprache kamen lassen mich auf einen tiefgründigen Austausch und interessante Ergebnisse hoffen.

Aus Sicht des Datenschutzes sind Schwerpunkte basierend auf Risikoanalysen zu setzen. Cloud, big-data, soziale Netzwerke, Smartphones machen vor allem die IT-Sicherheit immer wichtiger.

Es ist daher sehr bedauerlich, dass in unserer Kirche der Verpflichtung zur Erstellung von IT-Sicherheitskonzepten durch die kirchlichen Stellen bisher kaum nachgekommen wurde. Nach § 1 Abs. 2 IT-Sicherheitsverordnung (IT-SVO) hat jede kirchliche Stelle ein IT-Sicherheitskonzept zu erstellen und fortzuschreiben. Die Übergangsfrist nach § 7 IT-SVO dafür ist seit dem 31.12.2017 abgelaufen. Auch von der Möglichkeit IT-Sicherheitsbeauftragte zu bestellen, wurde selbst in großen Einrichtungen wenig Gebrauch gemacht.



Der Datenschutzbeauftragte ist eine unabhängige Aufsichtsbehörde. Gleichwohl verstehe ich mein Amt als eine Dienstleistung für die Einrichtungen unserer Kirche. Mein Auftrag ist es den Einrichtungen dabei zu helfen, die Rechte der anvertrauten Menschen zu respektieren und zu schützen.

2. Novelle des Datenschutzgesetzes der EKD

2016 wurde die EU-Datenschutzgrundverordnung (EU-DSVGO) beschlossen. Eine Verordnung unterscheidet sich von den im Europarecht üblichen Richtlinien dadurch, dass sie in den Mitgliedstaaten unmittelbar geltendes Recht wird, es also keiner Überführung in nationalstaatliches Recht bedarf. Nach einer Übergangsfrist von 2 Jahren ist die EU-DSGVO am 25.05.2018 in Kraft getreten.

In Art. 91 der EU-DSGVO ist den Kirchen das Recht eingeräumt, eigene Datenschutzregeln anzuwenden und auch eine eigene Datenschutzaufsichtsbehörde zu unterhalten. Damit hat auf EU-Ebene der Sonderstatus und das Selbstorganisationsrecht der Kirchen Anerkennung gefunden. Eine Arbeitsgruppe der EKD hat eine umfassende Novellierung des kirchlichen Datenschutzgesetzes vorbereitet. Dieser Arbeitsgruppe sowie der späteren Redaktionsgruppe durfte ich angehören. Das neue DSG-EKD wurde im Herbst 2017 von der EKD-Synode und dem Rat beschlossen. Es ist am 24.05.2018 also einen Tag vor der EU-DSGVO in Kraft getreten.

Wie das vorherige DSG-EKD gilt das novellierte für alle kirchlichen Stellen innerhalb der EKD. Dazu gehören die Landeskirche, Kirchenkreise und Kirchengemeinden, sowie die ihnen zuge-



ordneten kirchlichen und diakonischen Dienste, Einrichtungen und Werke ohne Rücksicht auf deren Rechtsform. Die EU-DSGVO findet mithin auf kirchliche Stellen keine Anwendung.

Die Anpassung des nordkirchlichen Datenschutzrecht an das neue EKD-Datenschutzgesetz ist abgeschlossen. Es gibt seit Mitte letzten Jahres ein neues Datenschutzdurchführungsgesetz und eine neue Datenschutzdurchführungsverordnung (DSDVO). Durch die Aufsichtsbehörde sind eine Vielzahl an Handreichungen, Mustern und Merkblättern erarbeitet und werden den kirchlichen Stellen über das Internet zur Verfügung gestellt.

Die gute Nachricht ist, dass sich inhaltlich nichts Grundsätzliches geändert hat. Das deutsche Datenschutzrecht war quasi die Blaupause für das europäische. Datenschutz in den Einrichtungen muss nicht neu gestaltet werden.

Datenschutzrecht ist Querschnittsrecht, das alle Bereiche kirchlicher Arbeit durchzieht. Auch wenn es mit teilweise sehr detailliert ausgearbeiteten Regelungen komplex erscheint, ist es auf seine Grundsätze zurückgeführt relativ einfach zu handhaben. Zunächst gilt das Verbot mit Erlaubnisvorbehalt. Personenbezogene Daten dürfen nicht verarbeitet werden, wenn ich dafür nicht einen Erlaubnistatbestand habe. Und es gilt der Grundsatz der Datenminimierung (früher Datensparsamkeit). Es dürfen nur diejenigen Daten erhoben und verarbeitet werden, die für die Erfüllung des kirchlichen Auftrags erforderlich sind. Mit diesen beiden Grundsätzen kann in den allermeisten Verfahren jeder entscheiden, ob eine Verarbeitung zulässig ist. Wenn das



der Fall ist, müssen die technisch organisatorischen Maßnahmen (TOMs) getroffen werden, die zum Schutz der Daten erforderlich sind. Die Strenge des Schutzes ist abhängig vom Risiko für die Betroffenen. Das ist das ganze datenschutzrechtliche System. Das DSGVO-EKD hilft dann mit einer Vielzahl von Einzelregeln bei den notwendigen Bewertungen.

Auch nicht geändert hat sich im neuen DSGVO-EKD die Verantwortlichkeit der Leitungen der Einrichtungen für die Einhaltung des Datenschutzes. Dabei werden sie von bestellten örtlichen Datenschutzbeauftragten unterstützt. Weiter bleibt die Verpflichtung zur Erstellung eines IT-Sicherheitskonzeptes unberührt.

Geändert haben sich die Begrifflichkeiten im neuen DSGVO-EKD, die aus der EU-Datenschutz-Grundverordnung vollständig übernommen worden sind. Dadurch wird unter anderem die Anwendung durch externe Auftragsverarbeiter³, aber auch die Kommunikation mit staatlichen Stellen zu Datenschutzfragen erleichtert.

An weiteren Neuerungen sind beispielhaft zu nennen die Verpflichtung zur Erstellung von Verzeichnissen von Verarbeitungstätigkeiten⁴ nach § 31 DSGVO-EKD, die Datenschutzfolgenabschätzung nach § 34 DSGVO-EKD, sowie Meldepflichten bei Datenpan-

³ Immer wenn nicht die kirchliche Stelle selber sondern für sie ein anderer, eine andere kirchliche Stelle oder ein öffentlicher oder privater Dritte die Daten verarbeitet spricht man von einer Auftragsverarbeitung.

⁴ Unter Verarbeitung werden nach dem neuen Recht alle Bearbeitungsvorgänge vom Erfassen, speichern, weiterleiten bis zum Löschen verstanden



nen nach § 32 DSGVO. Insgesamt sind die Rechte der Betroffenen an verschiedenen Stellen deutlich gestärkt worden.

Wichtig ist die nun geltende umfassende Rechenschaftspflicht nach § 5 Abs. 2 DSGVO, die das gesamte Datenschutzrecht durchzieht und die deutlich erweiterte Haftung der kirchlichen Stellen nach § 48 DSGVO bei materiellen und immateriellen Schäden aus Datenschutzverstößen.

Obwohl inhaltlich keine große Veränderung eingetreten ist, hat sich ein hohes Maß an Verunsicherung breit gemacht, die von aufgeregter Presse noch befördert wurde. Allerdings ist diese Verunsicherung auch darauf zurück zu führen, dass in vielen Einrichtungen bisher der Datenschutz eher zurückhaltend behandelt wurde. Vor dem Hintergrund von Abmahnvereinen und den gestärkten Mitteln der Aufsichtsbehörde vor allem aber aufgrund von Nachfragen von Betroffenen wurde ein erheblicher Handlungsbedarf sichtbar. Dabei musste ich feststellen, dass selbst das Bewusstsein eines eigenständigen kirchlichen Datenschutzrechtes nicht sehr ausgeprägt war.

3. Zusammenarbeit

3.2. Kooperation mit Beauftragten für den Datenschutz der EKD

Im letzten Jahr konnte in Abstimmung mit dem Vorsitzenden der Kirchenleitung eine vertiefte Kooperation mit dem Beauftragten für den Datenschutz der EKD vereinbart werden. In diesem Zusammenhang wurde ich selber zum stellvertretenden Datenschutzbeauftragten der EKD bestellt.



Der Beauftragte für den Datenschutz der EKD hat ein ausgefeiltes Schulungsprogramm aufgesetzt. Es besteht aus jeweils dreitägigen Grund- und Aufbau Seminaren und führt dann zu einem Zertifikat. Die Aufbau Seminare sind unterschieden nach verfasster Kirche und Diakonie. Diese Seminare sind ab diesem Jahr auch für Teilnehmer aus dem Bereich der Nordkirche offen. Die Kostenbeiträge unserer Teilnehmer sind gleich hoch wie die der anderen. Die Gebühren decken im wesentlichen Unterkunft, Verpflegung und Organisation. Wir halten dieses Jahr zwei solcher Seminare nach dem selben Muster auf dem Gebiet der Nordkirche in Hamburg und Ratzeburg ab. Damit wird ein einheitliches Niveau der Ausbildung der örtlichen Datenschutzbeauftragten in der EKD erreicht. Unsere Schulungsformate bleiben daneben zunächst bestehen.

Zu den Aufgaben der Beauftragten für den Datenschutz gehört es, die kirchliche Öffentlichkeit zu informieren. In einer der EKD-Arbeitsgruppe (AG Muster) erarbeiten wir gemeinsam einheitliche Muster und Merkblätter, die veröffentlicht und den kirchlichen Stellen zur Verfügung gestellt werden.

Mit dem Beauftragten für den Datenschutz der EKD führen wir unsere Internetauftritte soweit zusammen wie das aufgrund unterschiedlicher Gesetzgebung möglich ist.

Druckvorlagen des Beauftragten für den Datenschutz z.B. eine Handreichung für den Gemeindebrief werden uns zur Verfügung gestellt.



In verschiedenen Verfahren wie z.B. Facebook und Microsoft Clouddienste arbeiten wir eng zusammen und kommen zu gemeinsamen Bewertungen.

3.2. Zusammenarbeit mit römisch-katholischem Datenschutz

Im Rahmen der oben beschriebenen Novellierung des kirchlichen Datenschutzrechtes hat sich eine enge Zusammenarbeit mit den römisch-katholischen Datenschützern entwickelt. Wir standen weitestgehend vor den selben Herausforderungen und haben zwar kein gleichlautendes aber ein deutlich aufeinander bezogenes Recht erarbeitet. Dabei ist die Idee entstanden einen gemeinsamen ökumenischen Datenschutztag zu veranstalten. Der wurde bisher schon drei mal durchgeführt. Wir wollen z. B. ein gemeinsames kirchliches Standarddatenschutzmodell erarbeiten. Das Standarddatenschutzmodell ist ein von der Datenschutzkonferenz des Bundes und der Länder begründetes sehr hilfreiches Instrumentarium zur Datenschutzberatung und –prüfung anhand von Gewährleistungszielen. Wir wollen es gemeinsam auf die kirchlichen Belange anpassen.

3.3. Landesdatenschutzbeauftragte Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein

Mit allen drei Landesdatenschutzbeauftragten auf dem Gebiet der Nordkirche gibt es eine enge Zusammenarbeit, die sich nicht nur in regelmäßigem Austausch äußert, sondern auch bei der Bearbeitung von Fällen hilfreich ist. Zum Beispiel versuchen etwa Zuwendungsbehörden diakonische Einrichtungen zu zwingen unter Verstoß gegen kirchliches und staatliches Datenschutzrecht personenbezogene Daten zu übermitteln. Dabei



werden auch erhebliche Zwangsgelder angedroht. Von Seiten der Landesdatenschutzbeauftragten wird Unterstützung auf der staatliche Seite geleistet. Im eklatantesten Fall musste der Klageweg beschritten werden.

Mittlerweile ist zumindest im Land Mecklenburg-Vorpommern eine Klärung für die Diakonischen Einrichtungen erfolgt, welche Daten übermittelt werden müssen, ob die Offenlegung durch Übergabe oder Einsichtnahme vor Ort zu erfolgen hat und welche Daten eben nicht weitergegeben werden dürfen. Das Sozialministerium konnte bewegt werden eine entsprechende datenschutzkonforme Rundverfügung zu erlassen.

3.4. Krankenhausprojekt UPDK

Besonders hervorheben will ich die Kooperation mit dem Landesdatenschutzbeauftragten Mecklenburg-Vorpommern hinsichtlich eines Projektes zur Erhebung des Standes des Datenschutzes in unseren Krankenhäusern, genannt "Umgang mit Patientendaten in Krankenhäusern - UPDK"⁵. Es handelt sich nicht um eine Prüfung im eigentlichen Sinn, sondern es sollen die Probleme der Krankenhäuser im Rahmen von semi-strukturierten Interviews erkannt und gemeinsam nach praktikablen Lösungen (z.B. best practice) gesucht werden. Die Teilnahme ist freiwillig. In Mecklenburg-Vorpommern gibt es 31 staatliche und 4 diakonische Krankenhäuser. Die Erkenntnisse werden selbst innerhalb der Behörde nur anonymisiert weitergegeben. Wir erhalten Einsicht in alle anonymisierten Daten.

⁵ <https://www.datenschutz-mv.de/datenschutz/Projekte/UPDK/>



Da ich selber als Aufsicht nicht in die Datenerhebung eingebunden sein kann, werden wir von einem Mitarbeiter des BfD-EKD unterstützt, der die Anonymität gewährleisten kann.

Bei den staatlichen Krankenhäusern herrscht mittlerweile eine hohe Bereitschaft mitzumachen, da erkannt wurde, dass das Projekt die tatsächlichen Probleme aufnimmt und nach umsetzbaren Lösungen gesucht wird. Ich halte das für ein sehr richtungsweisendes Projekt, aus dem wir viel für die Praxis in unseren diakonischen Krankenhäusern lernen können. Am 28.10.2019 werden die Ergebnisse in einer Fachtagung vorgestellt und diskutiert.

4. Anforderungen an die Datenschutzaufsicht

Im Mai 2018 sind die EU-Datenschutzgrundverordnung (EU-DSGVO) und das novellierte Datenschutzgesetz der EKD (DSG-EKD) in Kraft getreten. Vor allem wegen eines damit einhergehenden gestärkten Datenschutzbewusstseins sowohl im staatlichen als auch im kirchlichen Bereich sind die Anforderungen an die Datenschutzaufsicht erheblich gestiegen. Auch weil sich der IT-Bereich sehr schnell entwickelt, verändern sich auch die Anforderungen an den Datenschutz, seine Problemstellungen und Lösungsansätze laufend und in ebenso schnellem Tempo.

Die Fallzahlen des Datenschutzbeauftragten der EKD zeigen, dass mit der Novelle des Datenschutzrechtes im Jahr 2018 die Anforderungen an die Datenschutzaufsicht signifikant gestiegen sind (siehe unten Statistiken Fallzahlen 2017 – 2018), sie haben sich mehr als verdoppelt, wobei das neue Gesetz erst im Mai in Kraft



getreten ist. . Es gibt ein Vielfaches an Anfragen, Beschwerden und Meldungen. Die Nachfrage nach Schulungsveranstaltungen ist massiv gestiegen, es gibt monatelange Wartelisten. Gerade aus der Diakonie wird nach einer intensiveren und vor allem spezifischeren Betreuung gefragt.

	Aufsicht	Beratung	Weiterbildung	Gesamt
Hauptsitz	12	49	6	67
AS Hannover	26	129	8	163
AS Berlin	21	84	5	110
AS Ulm	19	212	14	245
AS Dortmund	26	162	8	196
Summe	104	636	41	781

Bericht BFD-EKD 2019: Statistik über die Anzahl der Tätigkeiten 2017

	Aufsicht	Beratung	Weiterbildung	Gesamt
Hauptsitz	16	71	12	99
AS Hannover	30	230	9	269
AS Berlin	27	166	15	208
AS Ulm	27	472	21	520
AS Dortmund	67	486	25	578
Summe	167	1425	82	1674

Bericht BFD-EKD 2019: Statistik über die Anzahl der Tätigkeiten 2018

Eine entsprechende Statistik können wir in unserer Behörde aus Kapazitätsgründen ohne Assistenz nicht aufstellen. Für den Da-



tenschutzbeauftragten der Nordkirche stellt es sich aber genauso dar.

Eine gewissenhafte Aufgabenerfüllung ist mit der derzeitigen Personalausstattung nicht gewährleistet. Gerade im Bereich der Diakonie kann die Datenschutzaufsicht ihren Beratungs- und Schulungsaufgaben ohne eine Stellenaufstockung nicht mehr gerecht werden. Sie müsste nach meiner Einschätzung zwingend um mindestens eine volle Referenten- und eine teilweise Assistenzstelle aufgestockt werden.

Mit ähnlichem Kostenaufwand wäre es aber auch möglich, die Aufsicht über die Diakonie nach § 39 Abs. 3 Satz 1 DSGVO auf den Beauftragten für den Datenschutz der EKD zu übertragen. Die Gliedkirchen können nach § 39 Abs. 3 Satz 2 DSGVO bestimmen, dass die Diakonie gesondert beaufsichtigt wird. Eine Übertragung auf den Beauftragten für den Datenschutz der EKD hätte den Vorteil, dass nicht ein einzelner Mitarbeiter der Datenschutzaufsicht der Nordkirche die Diakonie mit ihren vielfältigen Aktivitäten von der kleinen Beratungsstelle bis zum Großkrankenhaus zu betreuen und zu beraten hätte, sondern die breite Expertise mit Spezialisierung und Vergleichsmöglichkeiten des Beauftragten für den Datenschutz der EKD zur Verfügung stünde.

Die Behörde des Beauftragten für den Datenschutz der EKD wurde seit ihrer Errichtung zum 1. Januar 2014 strukturell und personell sukzessive aufgebaut. Dieser Aufbau orientiert sich an dem von der EKD, den gliedkirchlichen Zusammenschlüssen, dem Evangelischen Werk für Diakonie und Entwicklung, sowie den Landeskirchen und den diakonischen Landesver-



bänden zur Verfügung gestellten finanziellen Mitteln, die im Rahmen der Übertragung der Datenschutzaufsicht zu entrichten sind. In den letzten fünf Jahren haben 16 Landeskirchen und sieben diakonische Landesverbände einschließlich ihrer Mitgliedseinrichtungen die Datenschutzaufsicht auf die Behörde übertragen. Die Dienststelle des Beauftragten für den Datenschutz ist eine unselbstständige Einrichtung der EKD mit Hauptsitz in Hannover. Zur regionalen Gliederung der vertraglich auf die EKD übertragenen Datenschutzaufsicht in den Landeskirchen und Diakonischen Werken sind vier Datenschutzregionen gebildet worden. In jeder Datenschutzregion ist eine Außenstelle errichtet.⁶

Gute Voraussetzungen für die Teilübertragung sind durch die vertiefte Kooperation mit dem Beauftragten für den Datenschutz der EKD (s.o.) geschaffen. Im Landeskirchenamt wurden bereits die notwendigen Änderungsregelungen erarbeitet. Allerdings hat der Haushaltsbeauftragte des Kollegiums wie folgt Stellung genommen: „Durch die Gesetzesinitiative wird eine weitere auf Dauer angelegte Ausgabeposition im landeskirchlichen Haushalt eingerichtet. Eine Kompensation der zusätzlichen Ausgaben wird nicht vorgeschlagen. Mit Blick auf die zukünftige Ertragsituation der Nordkirche muss der Haushaltsbeauftragte widersprechen.“

So sehr das Argument des Haushaltsbeauftragten verständlich und nachvollziehbar ist, bleibt doch die Frage offen, wie eine regelgerechte Datenschutzaufsicht in unserer Kirche gewähr-

⁶ vgl. Vorlage an das Kollegium am 09.07.2019



leistet werden soll. Zugegebenermaßen handelt es sich um eine freiwillige Aufgabe. Es wäre auch möglich die Aufsicht durch den Staat durchführen zu lassen. In der EKD hat man sich aber entschieden, die Aufgabe in eigener Verantwortung durchzuführen und wir bekommen vom Staat z.B. die Meldedaten nur, wenn wir einen gleichwertigen Datenschutz gewährleisten. Fehler werden auf die gesamte EKD zurückfallen. Und es sind Fehler passiert (vgl. Datenpannen).

5. Örtliche Datenschutzbeauftragte

Die Leitungen der kirchlichen Stellen sind verantwortlich für die Einhaltung der Datenschutzregeln. Zur Unterstützung werden örtliche Datenschutzbeauftragte bestellt. In bestimmten Fällen ist eine Bestellung zwingend. Um den Aufgaben sinnvoll nachkommen zu können, ist ein Stellenumfang von 20 % das Minimum⁷. Zunächst muss bedacht werden, dass örtliche Datenschutzbeauftragte eine Verpflichtung zur Aus- und Fortbildung haben. Nur dann können sie die Leitung mit der Erstellung von Datenschutzkonzepten, mit Schulungen der Mitarbeitenden, durch Unterstützung bei Risikobewertungen oder der Erarbeitung von Verzeichnissen der Verarbeitungstätigkeiten sowie Datenschutzfolgeabschätzungen kompetent unterstützen.

Dieser Umstand ruft gerade zu nach der ausdrücklich durch § 36 Abs. 2 DSGVO-EKD vorgesehen gemeinsamen Bestellung von örtlichen Beauftragten schon alleine aus ökonomischen Grün-

⁷ Entschließung der EKD-Datenschutzkonferenz zur Bestellung von örtlichen Beauftragten vom 05.05.2017, Nr. 4



den. In der Praxis ist davon noch sehr wenig Gebrauch gemacht worden.

In der verfassten Kirche gibt es darüberhinaus das Gebot zur gemeinsamen Bestellung auf Kirchenkreisebene. Nach § 13 Abs. 3 unserer DSDVO sind die Kirchenkreise gehalten gemeinsame örtliche Datenschutzbeauftragte für ihren Bereich zu bestellen. Das wäre eine große Hilfe für die Kirchengemeinden, die viele ähnlich gelagerte Problemstellungen haben und oft kompetente Unterstützung brauchen. Bisher machen von dieser wertvollen Möglichkeit leider erst drei Kirchenkreise Gebrauch.

Ein Problem bei der Besetzungen von Stellen für örtliche Datenschutzbeauftragte ist an mich heran getragen worden. Es fehlt an einer Ordnung der Eingruppierung. Dadurch sind die Aufstellung von Stellenplänen, Ausschreibungen und Einstellungen erschwert. Die örtlichen Datenschutzbeauftragten müssen die erforderliche Fachkunde und Zuverlässigkeit besitzen (§ 36 Abs. 3 DSGVO-EKD). Hinweise zur Eingruppierung können aus dem sog. Ulmer Urteil⁸ gezogen werden. Danach sind Datenschutzbeauftragte zumindest dem gehobenen Dienst zuzuordnen. Ohne in die Tarifhoheit eingreifen zu wollen, wäre es für die Entwicklung des Datenschutz in unserer Kirche sehr hilfreich, wenn sich die Tarifparteien und Sozialpartner dieses Themas annehmen würden.

⁸ LG Ulm, Beschluss vom 31.10.1990 – 5 T 153/90



6. Information der kirchlichen Öffentlichkeit

Zu den Aufgaben der Aufsichtsbehörde gehört es, die kirchliche Öffentlichkeit zu informieren z.B. durch die Verbreitung von Warnungen, das Bekanntmachen von Stellungnahmen, neuer Handreichungen oder Merkblätter zur Erleichterung der Arbeit in den kirchlichen Stellen. Es ist bedauerlich, dass die Aufsichtsbehörden dafür kein Medium haben. Wir können das nur auf unserer Internetseite zur Verfügung stellen. Wir erwarten natürlich nicht, dass dort regelmäßig geschaut wird, ob es etwas Neues gibt. Zur Zeit können wir die Kirchenkreise und diakonischen Werke nur per E-Mailverteiler auf Neuigkeiten hinweisen. Ob dann die nächste Ebene und dort die verantwortlichen Leitungen und örtlichen Datenschutzbeauftragten informiert werden, können wir nicht überblicken. Aus Nachfragen wissen wir, dass das häufig nicht der Fall ist. Es ist bedauerlich, dass dafür in der Nordkirche kein modernes Medium vorhanden ist. Es gibt z.B. im Internetauftritt der Nordkirche keine Newsletterfunktion. Mit einem solchen Informationstool könnte der Datenschutz, aber nicht nur der sondern der gesamte Informationsfluss in unserer Kirche erheblich effizienter gestaltet werden.

7. Facebook

7.1. Verfahren

Es ist seit dem Facebookurteil des Europäischen Gerichtshof (EuGH) vom 05.06.2018 vermehrt zu Anfragen aus dem Raum der Kirche zur Zulässigkeit eines Facebookauftritts, einer sog. Fanpage, gekommen. Der EuGH hat festgestellt, dass der Be-



treiber einer Facebook-Fanpage mitverantwortlich für die Datenverarbeitung ist. Es ist deshalb mit Facebook darüber eine Vereinbarung zu schließen wie die Betroffenenrechte wahrgenommen werden. Die Konferenz der Datenschutzbeauftragten der Bundesrepublik Deutschland hat dazu Kriterien entwickelt. Facebook bietet mittlerweile zwar eine Vereinbarung an. Nach Meinung der Konferenz der Datenschutzbeauftragten genügt diese Vereinbarung jedoch nicht den rechtlichen Erfordernissen. Am 11.09.2019 hat das BVerwG diese Rechtsprechung in nationales Recht übernommen und festgestellt, dass die Datenschutzaufsicht aus Praktikabilitätsabwägungen auch den Betreiber einer Fanpage in Anspruch nehmen kann.

Ich habe deshalb ein Musterverfahren bei einer Facebook-Fanpage in unserer Landeskirche angestrengt. Mit dem Seitenbetreiber wurde Einverständnis über ein gemeinsames Vorgehen erreicht. Der Kirchenleitung wurde berichtet. Demnach wird der Seitenbetreiber Facebook auffordern, eine Vereinbarung i.S. der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorzulegen, notwendigenfalls auch unter Ausnutzung von Rechtsmitteln (Klage). Nach dem Urteil des BVerwG am 11.09.2019 wurde am 12.09.2019 der entsprechende abgestimmte Bescheid durch mich erlassen.

Hinsichtlich der Nutzung von Facebook muss ich warnen, dass nach dem neuesten Urteil des BVerwG vermehrt mit Verfahren zu rechnen ist. Betroffene oder spezialisierte Rechtsanwälte könnten sich wegen eines Datenschutzverstößes an die Betreiber mit gebührenpflichtigen Abmahnungen oder an die Aufsichtsbehörden mit Beschwerden wenden.



7.2. Kartellverfahren

Auch das Bundeskartellamt geht gegen Facebook vor. Am 03.03.2016 wurde ein Verfahren gegen Facebook eröffnet das vor ca. drei Wochen, am 07.02.2019, zu einer Anordnung gegen Facebook geführt hat. Facebook wird es untersagt ohne freiwillige Einwilligung der Nutzer Daten von WhatsApp mit den Facebookprofilen zu verknüpfen. Voraussetzung für diese Anordnung ist es, dass das Bundeskartellamt eine marktbeherrschende Position von und einen sog. „Ausbeutungsmissbrauch“ durch Facebook festgestellt hat. Mit dieser Anordnung wird eine Anordnung des Landesdatenschutzbeauftragten von Hamburg, Herrn Prof. Caspar, wieder in Kraft gesetzt. Mit Einführung der EU-DSGVO ist die zentrale datenschutzrechtliche Zuständigkeit für Facebook zum Datenschutzbeauftragten von Irland gewandert. Dort ist der Hauptsitz von Facebook in Europa. Dieser hat die Anordnung nicht aufrechterhalten.

7.3. Politische Situation

Am 22.02.2019 veröffentlichte das Wall Street Journal⁹, dass nach seiner Recherche Facebook aus vielen Apps Daten erhält. Dazu gehören auch Gesundheitsdaten. Auch verschiedene sog. Zyklusapps zur Kontrolle der Periode von Frauen mit allen Details einschließlich z.B. des Kinderwunsches würden an Facebook übermittelt. Der Gouverneur von New York hat Ermittlungen angeordnet. Einige der Apps haben nach Veröffentlichung

⁹ <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636>, aufgerufen am 15.09.2019



des Artikels bekannt gegeben, dass sie die Datenübermittlung an Facebook eingestellt haben.

Am 18.02.2019 veröffentlichte das britische Parlament seinen Bericht über den Cambridge-Analytica-Skandal¹⁰, in dem es Facebook auffordert, sich nicht wie ein „digitaler Ganster“ zu verhalten. Nach Auffassung des britischen Parlamentes hat Facebook „vorsätzlich und wissentlich“ gegen Datenschutz- und Wettbewerbsrecht verstoßen. Die Ermittlungen seien von Facebook absichtlich behindert worden. Zudem kommt der Bericht zu dem Ergebnis, dass durch Facebook und andere Soziale Medien die Demokratie gefährdet sei. Die Regierung wird aufgefordert, Untersuchungen über die Rolle der Sozialen Medien beim schottischen Unabhängigkeitsreferendum 2014, dem EU-Referendum 2016 und den Parlamentswahlen 2017 einzuleiten.

Auch das Europaparlament hat sich mit Facebook befasst. Am 05.07.2018 hat es eine Resolution zum Privacy-Shield-Abkommens mit 2/3-Mehrheit beschlossen. Bei dem Privacy-Shield handelt es sich um ein Abkommen zwischen der EU und den USA wonach ein Transfer von personenbezogenen Daten in die USA zulässig ist. Die Facebookdaten werden unter dieser Regelung übermittelt. Unter dem Eindruck insbesondere des Cambridge-Analytica-Skandal und des US-CLOUD-Act vom

¹⁰ Cambridge-Analytica-Skandal: Vor rund fünf Jahren gaben Entwickler einer Umfrage-App Informationen von Dutzenden Millionen Facebook-Nutzern an die Datenanalyse-Firma Cambridge Analytica weiter.



20.03.2018 hat das Europaparlament die Kommission aufgefordert das Privacy-Shield-Abkommen entweder nachzubessern oder ab dem 01.09.2018 auszusetzen. Jedenfalls sollte nach Auffassung der Parlamentarier Facebook die Zertifizierung entzogen werden.

Die Entscheidung des EU-Parlamentes ist zwar rechtlich für die EU-Kommission nicht bindend, aber mit deutlicher Mehrheit EU-weit demokratisch legitimiert. Wenn sich das EU-Parlament wegen der festgestellten Wahlbeeinflussung und der damit einhergehenden Gefährdung für unsere Demokratie so positioniert, könnte das vielleicht auch einen Einfluss auf die grundsätzliche Stellung der Kirche zu Facebook haben.

Mir stellt sich die grundsätzliche Frage, ob es in Anbetracht der datenschutzrechtlichen Risiken richtig und zukunftsweisend ist, dass Kirche mit so einem Unternehmen wie Facebook zusammen arbeiten will. Aus dem Digitalisierungsausschuss erhoffe ich dazu Impulse.

8. Messengerdienste

Ohne WhatsApp sei Jugendarbeit nicht mehr möglich, höre ich. Und den datenschutzwidrigen weitverbreiteten Einsatz kann ich bestätigen.

Bei der Installation von WhatsApp werden alle Kontaktdaten aus dem Smartphone an WhatsApp/Facebook übermittelt. Auch diejenigen Kontaktdaten von Menschen, die WhatsApp nicht installiert haben. Das ist ohne Einwilligung der Betroffenen unzulässig, weil damit in deren Recht auf informationelle



Selbstbestimmung eingegriffen wird. Ich erinnere: Datenschutz ist Grundrechtsschutz. Wir müssen uns also klar machen, dass wir mit der Installation die Freiheitsrechte und die Würde anderer Menschen verletzen.

Facebook legt sog. Schattenprofile von Menschen an, die dort nicht aktiv sind mit der Behauptung, man könne sich ja irgendwann dort anmelden und dann seien der Freundeskreis und damit auch Vorlieben oder Hobbys schon gleich bekannt. Genutzt werden die Profile für die Schaltung von zielgenauer Werbung für Produkte aber auch für politische Inhalte.

Ein datenschutzrechtliches Problembewusstsein ist grundsätzlich vorhanden. Die Landeskirche Hannover setzt auf den Messenger „Just Connect“, der von Nutzern unentgeltlich geladen werden kann, allerdings nur in der Androidversion.

Ein guter und vom Leistungsumfang mit WhatsApp vergleichbarer Messenger ist ginlo (ehemals SIMSme) von der deutschen Post. Für die Nutzer ist er unentgeltlich, für Unternehmen kostenpflichtig. Die Wirtschaftsgesellschaft der Kirchen in Deutschland mbH (WGKD) hat einen Rahmenvertrag für kirchliche Stellen mit der Post abgeschlossen, der vergünstigte Bedingungen anbietet.

Mit den römisch-katholischen Datenschutzbeauftragten sind wir im Gespräch eine gemeinsame Messengerempfehlung auszusprechen. Es wäre doch die Mühe wert, wenn Kirche sich insgesamt auf einen datenschutzrechtlich unbedenklichen Messengerdienst einigen könnte.



Aber immer wieder wird mir entgegengehalten, Jugendarbeit sei ohne WhatsApp nicht möglich. Das denke ich nicht. In meinen Augen ist es doch auch eine Chance mit Jugendlichen darüber ins Gespräch zu kommen, ob sie in die Rechte der anderen eingreifen wollen. In den meisten Fällen wird ihnen das gar nicht bewusst sein. Ein großes Thema in der Jugendarbeit ist Respekt. Ich halte es aber für respektlos in die verfassungsmäßig garantierten Rechte anderer einzugreifen. In der Praxis der Konfirmandengruppe kann man doch im Rahmen einer entsprechenden Einheit gemeinsam den z.B. den unentgeltlichen ginlo-Messenger runterladen und den Kindern zeigen, dass es Alternativen gibt. Das wird gemacht und funktioniert.

9. Microsoft

Microsoft bietet hervorragende Clouddienste an, für die Kirche zu sehr vergünstigten Konditionen. In der Nordkirche wurde die Serverstruktur 2012 mit der Fusion der Kirchen entwickelt und aufgesetzt. Es bedarf dringlich einer Erneuerung. Das könnte mit Clouddiensten von Microsoft gut, schnell und kostengünstig gemacht werden. Deshalb sind der Beauftragten für den Datenschutz der EKD und ich im Gespräch mit Microsoft, um die rechtlichen Voraussetzungen zu schaffen.

Die Konferenz der Beauftragten für den Datenschutz in der EKD hat am 04.04.2019 zur Verwendung von Microsoft Clouddiensten wie folgt Stellung genommen:

Eine Verwendung von Microsoft Clouddiensten (Azurecloud) erscheint datenschutzkonform unter den folgenden Voraussetzungen möglich:



- a. *Es wird von Microsoft eine wirksame Zusatzvereinbarung nach § 30 Abs. 5 DSGVO angeboten.*
 - b. *Eine Verschlüsselung der Daten ohne Zugang von Microsoft ist möglich (HYOK = Hold your own Key)*
 - c. *Die Übersendung von Telemetriedaten kann durch entsprechende Einstellungen unterbunden werden.*
- Wir gehen derzeit davon aus, dass vor Einführung entsprechender Systeme eine Datenschutzfolgenabschätzung nach § 34 Abs. 1 DSGVO durchzuführen ist.*

Es bedarf einer sog. Zusatzvereinbarung (§ 30 Abs. 5 Satz 3 DSGVO). Auftragsverarbeiter, die der EU-DSGVO unterliegen, haben sich zusätzlich der kirchlichen Datenschutzaufsicht zu unterwerfen. Dabei ist klar, dass es keine Anordnungen gegenüber dem Auftragsverarbeiter geben kann. Solche Verfügungen könnten sich ggf. immer nur gegen den Auftraggeber richten. Es geht also nur um Kontrollrechte, die Microsoft seinen Kunden in begrenztem Umfang sowieso einräumt.

Die bisherigen Vorschläge von Microsoft für eine Zusatzvereinbarung entsprechen noch nicht den gesetzlichen Anforderungen. Die Datenschutzaufsicht durch die Kirchen hat der staatlichen Datenschutzaufsichtsbehörden zu entsprechen, deren Befugnisse in Art. 58 EU-DSGVO geregelt sind.

Seit knapp einem Jahr bemühen sich die Datenschutzaufsichtsbehörden der EKD gemeinsam um einen abgestimmten Text mit Microsoft, der EKD-weit einschließlich der Diakonie genutzt werden kann. Dabei bin ich der Verhandlungsführer. Eigentlich sind wir kurz vor einem Ergebnis. Microsoft hat aber nun umgeschwenkt und will einzeln mit den Gliedkirchen verhandeln, um



die solidarische Position zu durchbrechen. Wir haben daher auch als Nordkirche die Verhandlungen aufgenommen. Eine Reaktion ist bisher nicht erfolgt. Andererseits haben wir eine Umfrage bei den Gliedkirchen und den Diakonischen Werken mit guter Resonanz gestartet. Ob wir es schaffen eine gemeinsame Position innerhalb der EKD zu halten, wird sich zeigen.

Die Möglichkeit einer Verschlüsselung HYOK¹¹ hat Microsoft grundsätzlich angeboten.

Bei einer Datenschutzprüfung hat die niederländische Regierung im November letzten Jahres nicht unerhebliche Verstöße gegen die EU-DSGVO in den Clouddiensten von Microsoft festgestellt. Insbesondere werden umfangreich Telemetriedaten an Microsoft gesendet. 25.000 verschiedene Ereignisse werden übermittelt und für bis zu 18 Monate gespeichert. Teilweise werden die Betreffzeilen oder ganze Teile aus E-Mails übermittelt. Eine Möglichkeit, das zu unterbinden, wird fast einem Jahr zugesagt, aber ist noch nicht geliefert. Der Weg zu den Microsoftclouddiensten ist damit auch aus technischer Sicht noch nicht für eine Nutzung frei.

10. Datenpannen

Einen großen Anteil an den gemeldeten Verstößen machen die Meldungen von Datenpannen aus. Die Verpflichtung zur unverzüglichen Meldung von Datenpannen ist neu und die Anzahl der Datenpannenmeldungen war überraschend (s.o.). Datenpan-

¹¹ Hold Your Own Key



nen beginnen bei dem Verlust eines Smartphones mit Zugriffsmöglichkeit auf den Server bis hin zu verlorenen oder gar von Dritten gefundenen Papierakten. Es ist verblüffend, was alles verloren gehen oder abhanden kommen kann. Aber auch schwerwiegendere Fälle z.B. von fehlerhaften Zugriffsmöglichkeiten auf Daten gibt es. In einer Schule gab es auf der Suche nach Klausuren einen Einbruch von Schülern in das Lehrernetzwerk.

Die massivsten Datenpannen waren einmal die Sperrung der gesamten EDV eines großen Diakonischen Trägers durch Ransomware mit Erpressungsversuch. Der Träger war wochenlang ohne Zugang zu seinen Daten – ein immenser Schaden. Der Abfluss von Daten konnte nicht nachgewiesen werden. Gelernt werden konnte daraus, wie wichtig regelgerechte Backups sind und dass es Sinn hat, ein Verfahren für das Einspielen eines Backups im Verfahrensverzeichnis aufzunehmen. Weitere solche Erpressungsversuche sind vorgekommen.

Zum anderen die Offenlegung von Meldedaten in größerem Umfang ohne rechtliche Grundlage. Diese Grundlage konnte nachgeholt werden, so dass es sich eher um einen organisatorischen Mangel handelt. Es wird daran gearbeitet diese aufzudecken und entsprechende Maßnahmen zu ergreifen, die Eingang ins Verfahrensverzeichnis finden.

Insgesamt kann man feststellen, dass ein Großteil der Datenpannen auf organisatorischen Mängeln beruhen. Die Pannen wären vermeidbar, wenn die kirchlichen Stellen umfassende Verfahrensverzeichnisse hätten. Ich kann nur immer wieder



darauf hinweisen, dass diese datenschutzrechtlichen Verfahrensverzeichnisse auf der Organisation und Prozessbeschreibung in der kirchlichen Stelle aufsetzen. <die Erarbeitung eines Verfahrensverzeichnisses kann durchaus hilfreich für die Organisation einer Einrichtung sein.

Letztlich können wir dankbar sein, dass es bis heute zu einem großen Datenverlust noch nicht gekommen ist.

11. Auftragsverarbeiter

Bearbeitung durch Auftragsverarbeiter nehmen ebenfalls einen großen Raum ein. Zum einen gibt es häufig Mängel bei den entsprechenden Verträgen, obwohl das neue Datenschutzrecht da erhebliche Erleichterungen geschaffen hat. Offenkundig wird das dadurch, dass Betroffene sich gegen die Übermittlung von Daten an private Firmen wehren. Nicht ganz nachvollziehbar ist das, da entsprechende Muster zur Verfügung gestellt werden. Diese scheinen oft nicht bekannt zu sein.

12. Beschwerden/Betroffenen Anfragen

Viele Beschwerden sowohl von Mitarbeitenden als auch von Betroffenen gibt es zu organisatorischen Abläufen in Einrichtungen. Sehr häufig fehlt es an einer geordneten Prozessbeschreibung. Das sind grundsätzliche organisatorische Mängel und die Verpflichtungen aus dem Datenschutzrecht können dabei helfen, diese zu überwinden. Es fehlen oft IT-Sicherheits- und Datenschutzkonzepte. Von der EKD AG Muster wurde im Februar ein Muster für ein Verzeichnis von Verarbeitungstätig-



keiten veröffentlicht, das bei der Ordnung der Prozess hilfreich sein kann.

Wenn die Informationsrechte von Betroffenen geltend gemacht werden, trifft man verbreitet auf eine gewisse Hilflosigkeit. Auch dafür gibt es häufig keine geordneten Prozesse.

13. Fundraising

Fundraising wird ein immer breiteres Thema. Obwohl wir in der Nordkirche mit § 42 N DSVO eine gut handhabbare Regelung dafür haben, kommt es zu Datenpannen. Viele diakonische Einrichtungen wollen ihre Daten für Fundraising nutzen, haben aber oft die rechtlichen Voraussetzungen dafür nicht geschaffen.

14. Schulung

Ein weiterer Schwerpunkt der Arbeit im letzten Jahr war neben den neuen Datenpannenmeldungen die Beratung und Schulung. Viele Anfragen richteten sich auf die Auswirkungen des neuen Datenschutzrechtes für die konkrete Arbeit. Da es ja inhaltlich wenig Veränderung gegeben hat war festzustellen, dass in der Vergangenheit viele Mängel vorhanden waren, die jetzt offenkundig wurden. So gab es beispielsweise einen Umgang mit Fotos auch im Internet, der nicht mit dem Datenschutzrecht vereinbar war und ist. Mit Mustern und Merkblättern konnte unseren Einrichtungen geholfen werden. Die vorher sporadischen allgemeinen Schulungen werden nun im regelmäßigen Rhythmus angeboten. Spezielle Schulungen etwa für Schulen oder Kitas werden rege nachgefragt. Zusätzlich haben wir die



Schulungsformate, die wir gemeinsam mit dem BfD-EKD anbieten.

