Datenschutzbeauftragter der Bayerischen (Erz-)Diözesen

Kapellenstr. 4, 80333 München
Telefon 089 2137 1796
Telefax 089 2137 27 1796
Email: jjoachimski@eomuc.de
München, den 31.3.2018

Bericht des Diözesandatenschutzbeauftragten
Berichtszeitraum 1.4.2017 bis 31.3.2018

Nach § 18 Abs. 3 der Kirchlichen Datenschutzordnung habe ich jährlich einen Bericht zu erstellen, der auch der Öffentlichkeit zugänglich gemacht wird.

1. Entwicklung des europäischen Datenschutzrechts

Die Endfassung der Europäischen Datenschutz-Grundverordnung vom 5.Mai 2016 wird am 25.Mai 2018 in den Mitgliedsstaaten wirksam. Sie ersetzt weitgehend nationale Bestimmungen (BDSG) und Landesvorschriften (Bay. Landesdatenschutzgesetz).

2. Entwicklung des staatlichen Datenschutzrechts in Deutschland

Die EU-Datenschutz-Grundverordnung enthält zahlreiche Öffnungsklauseln und lässt den Mitgliedstaaten Raum für Ausführungsbestimmungen. Die Ausfüllung dieser bewussten Lücken ist in der Bundesrepublik dem Bundesdatenschutzgesetz (neu) und in den Bundesländern deren Landesdatenschutzgesetzen überlassen. Der Bundestag verabschiedete das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU). Es tritt zum 25. Mai 2018 in Kraft. Ein neues bayerisches Landesdatenschutzgesetz ist m. W. n. noch nicht beschlossen.

Eine gute Fundstelle sowohl für das Bundesdatenschutzgesetz wie auch für die EU-DS-GVO ist https://dsgvo-gesetz.de/bdsg-neu/. Dort können die EU-Verordnung und das neue, ab 25.5.2018 geltende Bundesdatenschutzgesetz parallel eingesehen werden.

3. Entwicklung des kirchlichen Datenschutzrechts

Nach jahrelanger Entwicklungsarbeit in der Arbeitsgruppe „Datenschutz und Melderecht“ sowie in ihrer Unterarbeitsgruppe „KDO-Entwicklung“ liegt ein bundeseinheitlicher Entwurf für ein neues kirchliches Datenschutzgesetz seit 20. November 2017 vor. Dieser Entwurf ist inzwischen in den

meisten deutschen Diözesen in Kraft gesetzt und z. T. auch in den Amtsblättern veröffentlicht worden. Es tritt am 24.5.2018 in Kraft.

Klarstellungen: Jede Gesetzesnovelle bemüht sich mit mehr oder weniger Erfolg, Regelungen, die im Vorgängergesetz als unklar empfunden wurden, durch bessere zu ersetzen. Das KDG hat hier vielfach die Diktion der Grundverordnung übernommen, dieschon deswegen, weil sie in allen EU-Staaten gelten soll, kasuistischer sein muss als ein Gesetz für nur einen Staat. Man kann sich eben nicht darauf verlassen, dass die Gerichte aller Mitgliedsstaaten unbestimmte Rechtsbegriffe durchgängig gleich auslegen. Deswegen wird auch gelegentlich schon bei der Grundverordnung der Vorwurf erhoben, es würden Einzelfälle zu wenig abstrakt geregelt.

Erweiterte Informationspflichten: Im Zuge des Bemühens, beim Betroffenen mehr Transparenz im Hinblick auf die über ihn gespeicherten personenbezogenen Daten zu schaffen, wurden die Vorschriften über die Pflicht zur Benachrichtigung des Betroffenen hinsichtlich der Speicherung seiner Daten deutlich verschärft. Geblieben ist allerdings die Ausnahme, dass der Betroffene dann nicht von der Datenspeicherung in Kenntnis gesetzt werden muss, wenn diese mit seinem Willen erfolgte.

Auch in einem anderen Bereich wurde die Benachrichtigungspflicht, die es bisher schon im Bundesdatenschutzgesetz gab, in das KDG übernommen: Stellt der Verantwortliche eine Datenschutzverletzung fest, so ist der Betroffene unverzüglich davon zu informieren, wenn ihm daraus ein Schaden erwachsen kann. Die Datenschutzaufsicht ist auf jeden Fall nach § 33 KDG von einer solchen Datenschutzverletzung in Kenntnis zu setzen.

Erweiterte Löschungsvoraussetzungen: Die KDO legte bisher fest, dass Daten zu löschen sind, wenn sie nicht mehr benötigt werden. Im Gegensatz dazu geht das KDG viel weiter: Es bestimmt, dass der Betroffene ein ausdrückliches Recht hat, die Löschung der Daten zu verlangen. Entsprechendes gilt, wenn eine (widerrufbare) Einwilligung zur Verarbeitung der Daten mit Wirkung für die Zukunft widerrufen wird. § 18 KDG bestimmt darüber hinaus, dass der Betroffene die Einschränkung der Verarbeitung seiner Daten verlangen kann, wenn ihre Richtigkeit nur in Frage steht - bewiesen sein muss die Unrichtigkeit noch nicht.

Einschränkung der Verarbeitung von Daten für Zwecke der Beurteilung eines Menschen: Was bisher nur ein (ungeschriebener) Teil des Arbeitnehmer-Datenschutzrechts war, wird in § 24 KDG ausdrücklich im Gesetz gesagt: Ein Betroffener - nicht notwendig ein Arbeitnehmer - darf nicht ausschließlich auf der Basis automatisierter Entscheidungen beurteilt werden. Das gilt also zum Beispiel auch für Schüler. Für die gesteigerte Form dieser Beurteilung, das sogenannte Profiling, gibt es künftig sogar eine Definition in § 3 Ziffer 6 KDG: „Profiling“ ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten.

Datenschutz-Folgeabschätzung: Es gab sie bisher schon unter dem Begriff „Vorabkontrolle“ nach § 3 Abs. 5 KDO, nun § 35 KDG. Neu sind eine frühzeitige Einbindung der Datenschutzaufsicht und die Regelung, dass von einer Folgeabschätzung abgesehen werden kann, wenn von einer staatlichen oder kirchlichen Aufsichtsbehörde bereits eine solche vorgenommen worden ist. Fühlt sich der Verantwortliche auch bei Unterstützung durch seinen betrieblichen Datenschutzbeauftragten mit der Folgenabschätzung überfordert, so kann er von Anfang an die Datenschutzaufsicht in die Prüfung mit einbeziehen. Dies erleichtert in vielen Fällen die Einführung neuer Programme in den Dienststellen und entbindet diese von der Verpflichtung, in jedem Fall das Rad neu zu erfinden. Die Aufsichtsbehörden haben auch ihrerseits durch die Führung von entsprechenden Listen und die Zusammenarbeit mit den staatlichen Aufsichtsstellen den Überblick darüber, welche Programme bereits den Weg

durch die Prüfung genommen haben. Was auf den ersten Blick als zusätzliche Belastung der Aufsichtsbehörden wirken mag, sollte in der Praxis eine erhebliche Arbeitserleichterung mit sich bringen.

Betriebliche Datenschutzbeauftragte: Sie waren nach § 20 KDO immer dann zu bestellen, wenn in einer Dienststelle mehr als zehn Personen mit der Eingabe von Daten befasst waren. Dies galt gleichermaßen für die verfasste Kirche wie für Verbände oder Ordensgemeinschaften. Das KDG bringt eine Umgestaltung und Differenzierung der Voraussetzungen für die Bestellung eines betrieblichen Datenschutzbeauftragten mit sich:

- Für die verfasste Kirche entfällt die Mindestzahl der mit der Dateneingabe befassten Beschäftigten. Jede Dienststelle in diesem Bereich muss einen betrieblichen Datenschutzbeauftragten haben.
- Die Mindestzahl bleibt jedoch erhalten für Verbände wie zum Beispiel die Caritas und Ordensgemeinschaften. Hat also eine Ordensgemeinschaft einen derart geringen Umfang von Datenbewegungen, dass weniger als elf Personen damit befasst sind, so kann auf die Benennung eines betrieblichen Datenschutzbeauftragten verzichtet werden. Aber Vorsicht: Für die Dateneingabe ist nicht nur kein bestimmter Standard an Geräten erforderlich. Es genügt wie bisher eine elektrische Schreibmaschine oder ein Smartphone. Noch weitergehend: Nach der Fassung des KDG genügt es aber auch schon, wenn die personenbezogenen Daten manuell eingegeben werden.
- Das Mindestzahlerfordernis entfällt auch dann, wenn aus anderen Gründen die Benennung eines betrieblichen Datenschutzbeauftragten angezeigt ist. § 36 Abs. 2 nennt dazu zwei Alternativen: Wie bisher schon muss ein betrieblicher Datenschutzbeauftragter benannt werden, wenn in großem Umfang sogenannte besondere personenbezogene Daten verarbeitet werden. Die gab es bisher schon in § 2 Abs. 10 KDO; jetzt befasst sich eine ganze Vorschrift – § 11 KDG – mit den daraus resultierenden Problemen.
  Unabhängig von der Zahl der Beschäftigten ist auch dann ein betrieblicher Datenschutzbeauftragter zu benennen, wenn der Umfang der Datenverarbeitung eine ständige Überwachung erfordert.

An der Stellung des betrieblichen Datenschutzbeauftragten hat das KDG nichts Erhebliches geändert. Er bleibt weisungsfrei in der Ausübung seiner Fachkunde und wird, sofern er Mitarbeiter der Dienststelle ist, in seinem Dienstverhältnis so geschützt wie ein Mitglied der Mitarbeitervertretung. Wie bisher schon kann der betriebliche Datenschutzbeauftragte für mehrere Einrichtungen tätig werden.

Stellung der Datenschutzaufsicht: Besonders in der verfassten Kirche hatte es sich in den letzten Jahrzehnten eingebürgert, im Diözesandatenschutzbeauftragten die Person zu sehen, die den Datenschutz organisiert. Das kann so für die Zukunft nicht stehen bleiben: Die Datenschutzaufsicht hat das Funktionieren der Datenschutzorganisation zu prüfen und zu bewerten. Ist sie selbst in diese Organisation eingebunden, so fehlt ihr die für die Aufgabe notwendige Objektivität. Gerade die Objektivität der Datenschutzaufsicht ist es aber, was einen erheblichen Anteil der Voraussetzungen für die Selbstständigkeit des kirchlichen Datenschutzes ausmacht. Es muss deshalb darauf gedrungen werden, dass – zumindest nach einem Einführungszeitraum – typische Aufgaben der Datenschutzorganisation nicht der Datenschutzaufsicht obliegen. Dazu zählen unter anderem Schulungsmaßnahmen, aber auch die Bereitstellung einer ausreichenden Anzahl von betrieblichen Datenschutzbeauftragten.

Meldungen von Datenschutzverletzungen: Das KDG sieht in § 33 KDG vor, dass binnen 72 Stunden nach Bekanntwerden eines datenschutz-rechtlichen Vorfalls, der eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt, der zuständigen Datenschutzaufsicht eine Meldung zu machen ist. Die Regelung lehnt sich an § 42a BDSG in der bis 24.5.2018 gültigen Fassung an. Diese Vorschrift wurde in den bayerischen Diözesen während meiner Amtszeit stets entsprechend angewendet.

Schadensersatz: Schon bisher verpflichtete die Verursachung einer Datenschutzverletzung eine Dienststelle der Kirche nach § 823 BGB zum Schadenersatz. Voraussetzung dafür war allerdings der Nachweis des Verschuldens eines unmittelbar Handelnden. Hierdurch unterschied sich der Rechtslage nach der KDO von derjenigen nach dem Bundesdatenschutzgesetz wie vom Datenschutzgesetz der evangelischen Kirche Deutschlands. Nach beiden gesetzlichen Regelungen wurde das Verschulden der Dienststelle dann vermutet, wenn tatsächlich eine Datenschutzverletzung vorlag. Es musste also nicht der Geschädigte beweisen, dass ein Verschulden vorlag, vielmehr war es Sache der Dienststelle, nachzuweisen, dass ein Verschulden fehlte.

Prinzipiell kann man die Verknüpfung von Schadensverursachung und Verschulden auf dreierlei Weise konstruieren:

- Bei der sogenannten reinen Gefährdungshaftung wird ohne Rücksicht auf Verschulden gehaftet. Der Rechtsgrund dafür ist die Erhöhung der Gefahr für die Allgemeinheit durch eine gefahrgeneigte Tätigkeit.
- Die eingeschränkte Gefährdungshaftung, auch Haftung für vermutetes Verschulden genannt, erlaubt dem Verursacher dann eine Exkulpation, wenn ihn kein Verschulden trifft. Den Nachweis dafür hat er selbst zu führen.
- Nach den §§ 823 ff. BGB hat prinzipiell der Geschädigte die Beweislast dafür, dass ein Verschulden beim Verursacher vorlag.

Die EU-Datenschutz-Grundverordnung hat sich für das Modell der reinen Gefährdungshaftung entschieden. Wäre das KDG von dieser Regelung abgewichen, so hätte man sicher der kirchlichen Gesetzgebung den Vorwurf machen können, dass keine gleichartige Regelung wie in der EU-Verordnung geschaffen wurde. Das hätte mit Sicherheit die kirchliche Selbstverwaltung im Datenschutz aufs Spiel gesetzt. Wie in Art. 82 EU-DS-GVO ist die Haftung der handelnden Person selbst in § 59 Abs. 3 KDO ausgeschlossen, wenn sie nachweist, dass sie kein Verschulden trifft.

Ohne jeden Zweifel bedeutet dies eine Verschärfung der Haftung für Datenschutzverletzungen. Man sollte jedoch die Auswirkungen nicht überschätzen: Die EKD, welche bisher schon seit 1993 eine ähnliche Verschuldensregelung wie die zukünftig im KDG gebrauchte hatte, wurde nicht wirklich von Schadensersatzforderungen überzogen. Ganz im Gegenteil: Seit 1993 erfolgte keine Zahlung aus diesem Rechtsgrund. Die Begründung hierfür liegt auf der Hand: Auch wenn der Geschädigte das Verschulden des unmittelbar Handelnden nicht nachweisen muss, obliegt ihm die Verpflichtung zum Nachweis der Schadenshöhe. Gerade die aus Datenschutzverletzungen resultierenden Schäden sind aber schwer quantifizierbar. Im Ergebnis ist es daher nicht veranlasst, sich wegen der neuen Schadensersatzregelung große Sorgen zu machen.

Geldbußen: Empfiehlt es sich schon beim Schadenersatz, die praktischen Auswirkungen ohne übertriebene Vorsicht oder gar Panik abzuwarten, so gilt dies erst recht für die künftig bestehende Möglichkeit, dass die Datenschutzaufsicht Geldbußen gegen einen handelnden Verantwortlichen – nicht gegen die Dienststelle als solche – verhängen kann. Eine derartige Möglichkeit ist in der EU-Verordnung vorgegeben; das KDG konnte gar nicht anders, als diese Regelung zu übernehmen. Es hätte sonst an der grundlegenden Gleichwertigkeit der kirchlichen Regelung gefehlt und dem Argument wäre Tür und Tor geöffnet, das KDG könne mit der EU-Verordnung nicht in Einklang gebracht werden.

§ 51 KDG bestimmt, dass die Aufsichtsbehörde bei schuldhaften Datenschutzverletzungen „Geldbußen bis zu 500.000 € verhängen kann." § 51 Abs. 3 KDG nennt die Kriterien, nach denen die Geldbuße

zu bemessen ist, wenn sie denn wirklich verhängt wird. Die Vorschrift ist außerdem im Kontext mit § 47 Abs. 4 KDG zu lesen, der bestimmt:

> *Die Datenschutzaufsicht kann von einer Beanstandung absehen oder auf eine Stellungnahme der die Aufsicht führenden Stelle verzichten, wenn es sich um unerhebliche Mängel handelt, deren Behebung mittlerweile erfolgt ist.*

Die Konferenz der Diözesandatenschutzbeauftragten hat bereits eine Arbeitsgruppe eingesetzt, welche Richtlinien zur Bemessung der Geldbuße festlegen soll. Angestrebt wird eine bundeseinheitliche Lösung, die zwar die Anforderungen der Verordnung erfüllt, auf der anderen Seite jedoch Augenmaß bewahrt.

Rechtsweg in Datenschutzsachen: § 49 KDG legt in Übereinstimmung mit der EU-Datenschutz-Grundverordnung fest, dass es gegen die Entscheidungen der Datenschutzaufsicht einen Rechtsweg geben muss. Dies kann nicht der zu den staatlichen Verwaltungsgerichten sein, weil sonst entgegen Art. 137 der Weimarer Reichsverfassung ein staatliches Gericht über Interna der katholischen Kirche entscheiden würde. Damit wäre das Selbstverwaltungsrecht der Religionsgemeinschaften nicht mehr das Papier wert, auf dem es geschrieben ist.

Da es ein entsprechendes Gericht noch nicht gibt, musste es mitsamt der dazugehörigen Verfahrensordnung erst geschaffen werden. Die Vorgaben für den Entwurf waren:

- bescheidener Umfang des gesamten Gesetzes;
- weitestgehende Vermeidung zusätzlicher Formalerfordernisse;
- keine drastische Ausweitung personeller Ressourcen.

Natürlich hätte es sich angeboten, einfach die staatliche Verwaltungsgerichtsordnung zu übernehmen. Dies hätte allerdings die gestellten Anforderungen in ihr logisches Gegenteil verkehrt.

Zunächst bedurfte es eines Trägers für eine Gerichtsbarkeit; in der Bundesrepublik sind das der Bund und Länder. Hier zeigen sich schon die ersten Schwierigkeiten: Es gibt keine einheitliche katholische Kirche in Deutschland. Die deutsche katholische Kirche ist in Diözesen und - um es noch etwas komplizierter zu machen - in Ordensgemeinschaften päpstlichen Rechts gegliedert. Diese Ordensgemeinschaften stehen den Bistümern auch in der Gesetzgebungsbefugnis gleich.

Da es keine institutionelle und hergebrachte überörtliche gemeinsame Institution der katholischen Kirche in Deutschland gibt, musste auf den Verband der Diözesen Deutschlands (VDD) als Träger zurückgegriffen werden. Der Verband hat seinen Sitz in Bonn und dort wird auch, wenn alle Pläne realisiert werden sollten, der erste Sitz des höheren kirchlichen Datenschutzgerichtes sein, die erste Instanz im nahegelegenen Köln. Natürlich muss dieses Datenschutzgericht alle Anforderungen erfüllen, die in einem Rechtsstaat an es gestellt werden. Das bedeutet

- einfacher Zugang für jeden Betroffenen ohne unnötige formale Hürden
- klare Zuständigkeitsregelungen
- Verankerung des rechtlichen Gehörs
- rechtsstaatliches Verfahren
- Außenwirkung der Entscheidung
- Möglichkeit eines Rechtsbehelfs gegen erstinstanzliche Entscheidungen.

Von vorneherein erschien es ausreichend, für das Datenschutzverfahren zwei Instanzen vorzusehen.

Sie bieten ausreichend Gelegenheit, ein Vorbringen auf seine Stichhaltigkeit zu prüfen. Auch im internationalen Vergleich sind zwei Instanzen ein guter Mittelwert; wir müssen nicht in allen Fällen für Beschwerden eine Tatsachen- und eine gesonderte Rechtsinstanz vorsehen. Zumindest in den ersten zehn Jahren wird sich die Belastung des Gerichts wohl in Grenzen halten. Als Spruchkörper sind zwei Kammern vorgesehen: Die Datenschutzkammer des Interdiözesangerichts, besetzt mit dessen Präsidenten als Vorsitzendem- und zwei weiteren Richtern, bildet die erste Instanz; die Kammer des Beschwerdegerichts, besetzt mit dem Präsidenten und vier weiteren Richtern, bildet die Beschwerdeinstanz.

In der Praxis wird es nun wohl regelmäßig um Rechtsfragen gehen, die sich auch ohne die leibliche Präsenz des Betroffenen bzw. seines Vertreters in angemessener Weise entscheiden lassen. Deswegen sieht das Verfahren eine freigestellte mündliche Verhandlung vor, was bedeutet, dass der Vorsitzende eine Verhandlung immer nur dann ansetzt, wenn er die Verletzung des rechtlichen Gehörs des Betroffenen befürchtet.

Das Verfahren wird normalerweise durch die Einreichung einer Antragsschrift eingeleitet, in welcher der Antragsteller auch vorbringen muss, in eigenen Rechten betroffen zu sein. Sie kann wahlweise beim Gericht oder bei der Datenschutzaufsicht entweder binnen eines Jahres nach einem für den Betroffenen negativen Bescheid oder binnen drei Monaten der Untätigkeit eingereicht werden. Die Fristen bilden kein Zulässigkeitskriterium; vielmehr wird die Rechtsbehelfsberechtigung bei nutzlosem Verstreichen der Frist verwirkt. Typischerweise richtet sich das Verfahren gegen die Datenschutzaufsicht, doch kann auch direkt der Verantwortliche einer Dienststelle Antragsteller oder -gegner sein.

Nach Eingang der Antragsschrift hört das Gericht die Gegenseite an und bestimmt in den geschilderten Ausnahmefällen einen Termin zur mündlichen Verhandlung. Anlass für eine mündliche Verhandlung kann es aber auch sein, dass das Gericht Beweise erheben will. Es besteht der Amtsermittlungsgrundsatz; Beweise sind die auch in anderen Verfahren üblichen. Mit oder ohne mündliche Verhandlung entscheidet die kleine Kammer durch Beschluss. Sie kann den Antrag als unzulässig verwerfen, ihn zurückweisen oder ihm stattgeben.

Gegen diesen Beschluss hat die unterlegene Partei die Möglichkeit der Beschwerde binnen einer (Verwirkungs-) Frist von drei Monaten. Das Verfahren in der zweiten Instanz entspricht demjenigen der ersten mit der Maßgabe, dass eine mündliche Verhandlung nur ganz ausnahmsweise stattfindet. Mit der Mitteilung des Beschlusses der großen Kammer endet das Verfahren vor dem Datenschutzgericht; eine dritte Instanz ist nicht mehr vorgesehen.

4. Änderung bei den Diözesandatenschutzbeauftragten im Bundesgebiet

Im Zuge der Umorganisation der Datenschutzaufsicht in den deutschen (Erz-) Diözesen wurde zum 1.1.2018 Frau Ursula Becker-Rathmair als neue Diözesandatenschutzbeauftragte Deutschland-Südwest mit Sitz in Frankfurt für die Bistümer Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart und Speyer bestellt.

Die Verringerung der Zahl zuständiger Diözesandatenschutzbeauftragter führte zu einer deutlichen Verbesserung der Kommunikation zwischen ihnen. Mittlerweile liegt ein Beschluss der Diözesandatenschutzbeauftragten-Konferenz vor, jährlich vier bis sechs Mal zu tragen. Dies eröffnet die Möglichkeit, in allen wesentlichen Streitfragen zu einer bundeseinheitlichen Lösung zu kommen und damit die Rechtssicherheit im kirchlichen Datenschutz deutlich zu verbessern. Da an mindestens einer der Konferenzen ein Vertreter des Datenschutzes der EKD teilnimmt und entsprechend Diözesandatenschutzbeauftragte zu den Sitzungen des Datenschutzes der EKD eingeladen werden, ist auch eine ausgezeichnete Kommunikation mit der evangelischen Kirche für diesen Bereich gesichert.

Unter anderem ist eine Veröffentlichung der Beschlüsse der Diözesandatenschutzbeauftragten-Konferenz geplant. Die wichtigsten bisherigen Beschlüsse:

Datum	**Inhalt**
3.5.2017	Die Verwendung eines Messengerdienstes wie What's App auf dienstlichen Endgeräten ist untersagt, soweit eine physikalische Datenspeicherung außerhalb des Gebiets des EWR und der Schweiz stattfindet oder keine Punkt-zu-Punkt-Verschlüsselung genutzt wird.
3.5.2017	Es soll eine einheitliche Schulungssoftware für alle mit der Datenverarbeitung befassten Beschäftigten entwickelt werden.
20.11.2017	Wenn Daten in die Cloud gestellt werden, dann dürfen sie unabhängig von § 203 StGB: • nur verschlüsselt gespeichert und übertragen werden • nur unter Beteiligung des Auftraggebers verarbeitet werden
20.11.2017	Die Konferenz beschließt die Gründung eines technischen Arbeitskreises.
20.11.2017	Die Konferenz beschließt einstimmig, bespielhaft Standardvertragsklauseln zusammenzustellen und auf der Internetseite als Formulierungshilfen zur Verfügung zu stellen.
20.11.2017	Die Konferenz beschließt folgende Punkte für die zukünftige Darstellung nach außen: • Für die Koordination gibt es zukünftig eine feste postalische Anschrift in Dortmund für mögliche Ansprechpartner. Ebenso werden in Dortmund die zukünftigen Sitzungen der Konferenz in Zusammenarbeit mit dem Ausrichtenden koordiniert, dies betrifft insbesondere: • Vorlagen • Protokolle und Beschlüsse
20.11.2017	Die Konferenz ist sich einig, dass Schulungen der DDSB nur auf Multiplikatorenebene (DIAG/DG/Verbänden etc.) stattfinden. Es sollen keine Mitarbeiterschulungen (z.B. MAV) vor Ort angeboten werden.
8.2.2018	Bis zum Auslaufen der Übergangsregelung der KDO-DVO am 30.6.2019 dürfen bei Verwendung von MS Office personenbezogene Daten nicht bei MS ONE-Drive gespeichert werden.
8.2.2018	Die Konferenz stellt die datenschutzrechtliche Unzulässigkeit der Weitergabe von personenbezogenen Daten/ Meldedaten eines (Erz-)Bistums zum Zweck der Werbung für eine Kirchenzeitung an die jeweiligen Verlage fest.
8.2.2018	Die DDSB und deren Mitarbeiter sind nur in Ausnahmefällen an der Gesetzgebung im kirchlichen Datenschutz zu beteiligen.
8.2.1018	Die Konferenz setzt Mindestinhalte für den Erwerb der Fachkunde durch betriebliche Datenschutzbeauftragte fest (vgl. Anhang 1: Curriculum)

Die Internetseiten der Diözesandatenschutzbeauftragten stellen wichtige Informationsquellen dar und enthalten vielfach wichtige Beiträge, Formulierungshilfen oder Erklärungsmuster. Hier die Webadressen:

Deutschland-Ost: https://www.datenschutzbeauftragter-ost.de/

Deutschland -Nord: https://www.datenschutz-kirche.de/

NRW: https://www.katholisches-datenschutzzentrum.de

Deutschland-SW: http://kdsz-ffm.de/ (noch im Aufbau)

Eine weitere wichtige Webseite mit entsprechendem Inhalt:

Datenschutz-Notizen: https://www.datenschutz-notizen.de/category/kirchlicher-datenschutz/

5. Datenschutzaufsicht bei der Evangelischen Kirche

Zur Wahrnehmung der originären sowie der vertraglich übertragenen Aufgaben der Datenschutzaufsicht ist seit Anfang 2014 die Dienststelle „Beauftragter für den Datenschutz EKD“ organisatorisch und strukturell als unselbstständige Einrichtung der EKD mit Hauptsitz in Hannover aufgebaut. Ihr gehören der Datenschutzbeauftragte und drei Mitarbeiter an. 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 je eine Außenstelle errichtet, die mit einem Leiter – vielfach Jurist/in – und zwei bis drei Mitarbeitern besetzt sind:

- Nord Hannover
- Ost-Berlin
- Süd Ulm
- Mitte-Nordwest Dortmund

Der Bericht des Datenschutzbeauftragten der EKD ist im Internet unter https://datenschutz.ekd.de/ueber-uns/unsere-taetigkeitsberichte/ abrufbar.

Mit den im Datenschutz tätigen Mitarbeitern der EKD besteht eine sehr enge Zusammenarbeit. Regelmäßig nimmt ein Kollege der EKD an den Sitzungen der Arbeitsgruppe „Datenschutz und Melderecht“ teil. Umgekehrt sind die Mitglieder der Arbeitsgruppe stets bei der EKD eingeladen. Auch auf der Ebene der Diözesandatenschutzbeauftragten gibt es mehrere Treffen jährlich. Als Besonderheit ist für den 12. April 2018 ein ökumenischer Datenschutztag in Erfurt vorgesehen. Bei der Ausarbeitung der Gesetzestexte zur Anpassung des kirchlichen Datenschutzrechts an die EU-Datenschutz-Grundverordnung wurde darauf geachtet, möglichst keine großen Unterschiede zwischen EKD und katholischer Kirche entstehen zu lassen.

6. Kirchliche Datenschutzorganisation in Bayern

a. Datenschutzaufsicht

Die gemeinsame Datenschutzstelle der bayerischen (Erz-) Diözesen besteht weiterhin aus meinen zwei Mitarbeitern im Aufsichtsdienst und mir; eine Vergrößerung dieser Gruppe um zwei weitere Aufsichtspersonen und eine Schreibkraft halte ich weiterhin für sinnvoll.

Meine beiden in der Datenschutzaufsichtsgruppe zusammengefassten Mitarbeiter haben im Berichtszeitraum insgesamt folgende Dienststellen geprüft:

- 67 Kirchenstiftungen
- 38 Kindertageseinrichtungen
- 6 Verbände/Orden bischöflichen Rechts

Beide Mitarbeiter sind im Berichtszeitraum auch ganz erheblich in Fortbildungen eingesetzt worden. Es besteht zwar ein entgegengesetzter Beschluss der Konferenz der Diözesandatenschutzbeauftragten, demzufolge Schulungen nicht durch die Datenschutzaufsicht durchgeführt werden sollten. Ich sah mich jedoch außerstande, diesem Beschluss zu folgen, weil sonst in einem Teil der Diözesen eine ausreichende Fortbildung der Mitarbeiter nicht gewährleistet gewesen wäre. Auch die Vorbereitung auf die Einführung des neuen Rechts zum 25. Mai 2018 habe ich durch die Ansetzung verschiedener Fortbildungstermine für Juristen bzw. betriebliche Datenschutzbeauftragte gefördert, ohne dass ein entsprechender Auftrag vorlag. Es war sonst in großen Bereichen keinerlei andere Vorbereitung erkennbar, die bis zum Inkrafttreten des neuen Rechts greifen würde.

Es sollte dabei allerdings nicht übersehen werden, dass auch die normalen mit der Dateneingabe befassten Mitarbeiter und die Dienststellenleiter einer Schulung im Hinblick auf das neu einzuführende KDG bedürfen. Die erstgenannte Schulung muss sicher nicht den Umfang haben, wie er bei betrieblichen Datenschutzbeauftragten notwendig ist. Es liegt das Angebot einer Onlineschulung vor, die den Zweck in jeder Hinsicht erfüllt. Ich würde raten, dieses Angebot anzunehmen, soweit noch nicht geschehen. Für die Dienststellenleiter ist ein höherer Aufwand vorzusehen.

Neben Prüfungen und Fortbildungen haben sich meine beiden Mitarbeiter inzwischen jeweils auf besondere Aspekte ihrer gesamten Tätigkeit spezialisiert: Frau Mayinger obliegt neben meiner Vertretung und der Mitarbeit in rechtlichen Fragen die Verwaltung des Dienst-PKWs und des gesamten Materials. Herr Gleißner arbeitet bei der Vorabkontrolle von Verfahren mit und hält die Verbindung zu den Gliederungen der Caritas.

Die Freisinger Bischofskonferenz beschloss im Rahmen ihrer Herbstkonferenz 2017, den kirchlichen Datenschutz in Bayern im Sinne einer zentralen Datenschutzaufsicht mit voraussichtlichem Sitz in Nürnberg zu organisieren. Dabei soll der Bereich „Datenschutzmanagement“ nicht bei der zentralen Datenschutzaufsicht angesiedelt werden. Die Verantwortlichkeit für das Datenschutzmanagement verbleibt vielmehr bei der jeweiligen (Erz)Diözese.

Die zentrale Datenschutzstelle (Datenschutzaufsicht) soll als Körperschaft des öffentlichen Rechts errichtet werden.

Das Katholische Büro Bayern wurde beauftragt, gemeinsam mit dem Finanzdirektor des Erzbischöflichen Ordinariats München, einen Finanzierungsplan für die zentrale Datenschutzaufsicht zu entwerfen. In die Aufstellung des Finanzierungsplans war ich nicht eingebunden. Die Abstimmung hierüber wurde in der Frühjahrsvollversammlung 2018 getroffen.

Eine – allerdings nicht besonders gewichtige – Unsicherheit besteht noch bei der künftigen Gestaltung der Datenschutzaufsicht. Während die überwiegende Meinung Art. 91 Abs. 2 EU-DS-GVO (*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.*) dahingehend versteht, dass die „unabhängigen Aufsichtsbehörden“ zumindest auch solche der Kirchen sein können[1], vertreten einige Kommentatoren die Auffassung, die Aufsichtsbehörde müsse eine staatliche sein[2]. Landesgesetzliche Regelungen hierzu gibt es nicht.

[1] vgl. Paal/Pauly, EU-DS-GVO, 2.Auflage 2018, RN 20 zu Art. 91; BeckOK Datenschutz RN 21
[2] Schantz/Wollff, Das neue Datenschutzrecht, 2017, RN 1372 unter Bezugnahme auf

b. Betriebliche Datenschutzbeauftragte

Der Diözesandatenschutzbeauftragte und seine Mitarbeiter bilden lediglich die in der EU-Datenschutz-Grundverordnung künftig auch so bezeichnete Aufsichtsbehörde; sie hat die Einhaltung des Datenschutzes in den kirchlichen Einrichtungen zu kontrollieren. Organisiert werden muss der Datenschutz dagegen auf der Ebene der Dienststellen, in erster Linie durch den sogenannten betrieblichen Datenschutzbeauftragten

Das kirchliche Datenschutzgesetz sieht dazu in § 36 Folgendes vor:

§ 36 Benennung von betrieblichen Datenschutzbeauftragten

(1) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. a) benennen schriftlich einen betrieblichen Datenschutzbeauftragten.

(2) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. b) und c) benennen schriftlich einen betrieblichen Datenschutzbeauftragten, wenn

a) sich bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen,

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 besteht.

Unter Abs. 1 fallen die Dienststellen der verfassten Kirche. Die Caritas und ihre Untergliederungen fallen unter Abs. 2.ebenso wie z. B. die Orden bischöflichen Rechts oder kirchliche Vereine. Es müssen also für alle Dienststellen der verfassten Kirche zum 25. Mai 2018 betriebliche Datenschutzbeauftragte benannt werden. Ich habe die Kirchenstiftungen bereits davon in Kenntnis setzen lassen, dass die Datenschutzaufsichten aller deutschen (Erz-) Diözesen ein spezielles Programm beschaffen, welches die Benennung über einen Internet- Kontakt übermittelt. Deswegen sollten tunlichst nicht vor dem 25. Mai Meldungen abgegeben werden, es sei denn sie werden vom Ordinariat gesammelt übermittelt.

In den bayrischen Diözesen ist die Ausstattung der Kirchenstiftungen mit betrieblichen Datenschutzbeauftragten sehr unterschiedlich: Während in einer Diözese betriebliche Datenschutzbeauftragte jeweils für ein Dekanat und nahezu flächendeckend bestellt sind, ist in zwei anderen Diözesen für alle Kirchenstiftungen jeweils ein betrieblicher Datenschutzbeauftragter bestellt, der keine sonstigen Aufgaben hat. In den restlichen Diözesen werden die Aufgaben der betrieblichen Datenschutzbeauftragten durch die Diözesanjuristen, die auch als Datenschutzreferenten fungieren, z. T. unter Assistenz eines weiteren Mitarbeiters wahrgenommen. Die Ausstattung der Ordinariate selbst mit betrieblichen Datenschutzbeauftragten ist angesichts der Vielzahl von Aufgaben auch noch nicht durchwegs befriedigend, wird aber laufend verbessert.

Sehr unterschiedlich ist auch die Lage bei den Verbänden. Allerdings hat in den letzten beiden Jahren wenigstens ein Großteil der Caritas-Verbände auf Bezirks- bzw. Kreisebene betriebliche Datenschutzbeauftragte bestellt.

Was aber auf jeden Fall bisher fehlt, ist eine zentrale Organisation des betrieblichen Datenschutzes je (Erz) Diözese, die Ansprechpartner für alle kirchlichen Dienststellen im Hinblick auf Schulung und Fortbildung sein kann. Die Konferenz der Diözesandatenschutzbeauftragten hat ein Curriculum für die Aus- und Fortbildung der betrieblichen Datenschutzbeauftragten entwickelt und Ziele

Damman, ZD 2016, 307/311, der das aber nicht so erklärt.

dafür definiert. Es könnte bei der Ausbildung der betrieblichen Datenschutzbeauftragten hilfreich sein. Wichtig wäre es aber auch für die Tätigkeit der Datenschutzaufsicht, in jeder (Erz-) Diözese einen kompetenten betrieblichen Datenschutzbeauftragten als Ansprechpartner zu haben. Er sollte auch entsprechend dem Beschluss der Bischofskonferenz vom Herbst 2017 das Datenschutzmanagement für seinen Bereich leiten. Nur dann kann das Zusammenarbeitsgebot des § 38e KDG in der täglichen Arbeit verwirklicht werden.

Insgesamt erscheint die Ausstattung mit betrieblichen Datenschutzbeauftragten noch verbesserungswürdig. Nach Ansicht der Bundesdatenschutzbeauftragten, welcher der Landesdatenschutzbeauftragte ausdrücklich folgt, ist bei einer Gesamtzahl von je 1000 Beschäftigten eine volle Stelle einzuplanen; dieses Ziel wird bisher kaum in einer Diözese erreicht. Natürlich sind in die Zahl der betrieblichen Datenschutzbeauftragten auch diejenigen einzurechnen, die u. a. darauf hinwirken sollen, dass insgesamt eine genügende Anzahl von betrieblichen Datenschutzbeauftragten zur Verfügung steht.

Die Konferenz der Diözesandatenschutzbeauftragten hat einen Arbeitskreis gebildet, der sich ausschließlich mit der notwendigen Zahl von betrieblichen Datenschutzbeauftragten pro mit der Datenverarbeitung befasster Mitarbeiter beschäftigt. Der Bericht des Arbeitskreises ist für den 17./18. 4.2018 (Tagung in Würzburg) angekündigt und soll die Grundlage eines Beschlusses bilden; ich werde die Ergebnisse dieser Tagung allen Diözesen umgehend zur Kenntnis bringen.

Die betrieblichen Datenschutzbeauftragten werden von mir mit einer inzwischen sehr umfangreichen Materialsammlung in einer geschützten Seite des Internets und einem dort auch eingerichteten Datenschutzforum unterstützt. Ab Ende April sollten die vorhandenen Skripten an das neue Recht angepasst sein. Einmal im Jahr findet ein Erfahrungsaustausch der betrieblichen Datenschutzbeauftragten statt, in dessen Verlauf meine Mitarbeiter und ich Referate zu aktuellen Themen halten; 2017 lag der Schwerpunkt naturgemäß auf der Vorstellung der EU-Datenschutz-Grundverordnung und der durch sie bedingten Änderungen im kirchlichen Datenschutz; für den 10.4.2018 ist ein Erfahrungsaustausch mit einem komprimierten Update zur Gesetzessituation angesetzt.

Es ist mir ein Anliegen, hier den betrieblichen Datenschutzbeauftragten aller bayerischen (Erz-) Diözesen für die verantwortungsbewusste Wahrnehmung ihrer Aufgaben zu danken.

7. Meine Aufgabenschwerpunkte 2017

a. Tätigkeit in der Arbeitsgruppe „Datenschutz und Melderecht“ und in der Unterarbeitsgruppe „KDO-Entwicklung“

Mehr als in allen Jahren zuvor stand im Vordergrund meiner Tätigkeit die Mitarbeit an der Rechtsentwicklung im Gefolge der Anpassung der KDO an das Datenschutzrecht der EU-Datenschutz-Grundverordnung. Jeder, der daran beteiligt war, kam nicht umhin, in diese Aufgabe einen sehr großen Teil seiner Arbeitszeit zu investieren.

b. Beschwerden wegen Datenschutzverletzungen

Die statistische Gesamtbelastung hat sich gegenüber dem Vorjahreszeitraum fast nicht verändert. Auch der positive Trend der vergangenen Jahre, in denen die Beschwerden einen sehr geringen Anteil an meiner Tätigkeit ausmachten, hat sich fortgesetzt. 2017 wurden mit sechs nur relativ wenige Beschwerden erhoben; in zwei Fällen davon stellte ich – relativ geringfügige – Datenschutzverletzungen fest. Da die betroffene kirchliche Dienststelle jeweils bereits Abhilfe geschaffen hatte, erübrigte sich eine Anweisung neben der erhobenen Beanstandung.

c. Beratung

Sie nahm einen sehr großen Teil meiner Tätigkeit ein und erscheint hinsichtlich der meisten telefonischen oder mündlichen Anfragen auch gar nicht in der Statistik. Natürlich sind die in meinem Vorjahresbericht erwähnten Beratungsschwerpunkte auch im jetzigen Berichtszeitraum noch aktuell gewesen. Zur Vermeidung von Wiederholungen nehme ich jedoch insoweit auf meinen Vorjahresbericht Bezug.

Neue Beratungsschwerpunkte waren im Berichtszeitraum:

- **Bevorstehende Rechtsänderung:** Zahlreiche Dienststellen sind durch Einwirkungen von außen, insbesondere die Werbemaßnahmen der Kanzleien externer Datenschutzbeauftragter, erheblich verunsichert, was die künftige Rechtsentwicklung betrifft. In allen Bereichen wurde spürbar, dass Informationen gewünscht sind. Einzelne Dienststellen baten um persönliche Beratung, andere wiederum suchten Hinweise auf Informationsmaterial.

  Alle Diözesandatenschutzbeauftragten erstellten seit September 2017 Material zur Rechtsänderung. Mittlerweile sind 18 Einzeldokumente verfügbar, die auf den Webseiten der Mitglieder eingestellt wurden. Ich habe darüber hinaus meine beiden grundlegenden Skripten „Einführung in das kirchliche Datenschutzrecht“ und „Einführungshilfe für den betrieblichen Datenschutzbeauftragten“ überarbeitet. Beide Skripten werden mit der ab 25. Mai 2018 gültigen Rechtslage zum 1.4.2018 veröffentlicht. Auch das übrige Informationsmaterial wurde und wird an die neue Rechtslage angepasst; Entsprechendes gilt für die Muster von Erklärungen und Anordnungen. Bis 25. Mai 2018 sollte durchgehend der neueste Stand erreicht sein.

  In ihrer Sitzung vom 8.2.2018 hat die Konferenz der Diözesandatenschutzbeauftragten beschlossen, künftig Formulierungshilfen für immer wieder vorkommende Verträge zu erstellen und zu veröffentlichen. Sie sollen nicht als „Standard Vertragsklauseln“ veröffentlicht werden, weil dies unter Umständen ein Kohärenzverfahren auslösen könnte. Die Klauseln beziehen sich in erster Linie auf die Verträge zur Auftragsdatenverarbeitung und sollen auch zum Zeitpunkt der Rechtsänderung zur Verfügung stehen.

- **Office 365**: Microsoft hat durch eine relativ aggressive Preispolitik in den letzten zwei Jahren versucht, sein Produkt „Office 365“ in Schulen und Hochschulen unterzubringen. Die Besonderheit dieses Produktes ist es, dass es eine Datenspeicherung in der Cloud erlaubt und dass auch schon bei der Installation des Programms die Vorgabe einer entsprechenden Datenspeicherung eingestellt wird, was dazu führt, dass in aller Regel dies auch bei der endgültigen Installation so bleibt. Der physikalische Datenspeicher dieser Cloud befindet sich in den Vereinigten Staaten von Amerika, also außerhalb des europäischen Wirtschaftsraumes und damit in einem Drittland gemäß § 39 KDG. Ein Angemessenheitsbeschluss der europäischen Kommission liegt nicht vor, sodass die Datenübertragung in die USA unter Umständen eine Datenschutzverletzung darstellt. Um dies zu umgehen, hat Microsoft mittlerweile zwei verschiedene Modelle vorgestellt:

  - Beim sogenannten „Treuhandmodell“ wird die Verfügung über die gespeicherten Daten einem deutschen Unternehmen (Telekom AG) übertragen. Nur dieses Unternehmen soll befugt sein, eine Einsicht in die gespeicherten Daten anzuordnen.
  - Daneben gibt es das Modell, in welchem deutsche Unternehmen Auftragsverarbeiter von Microsoft werden und eine Datenspeicherung im Inland stattfindet. In diesem Modell verzichtet Microsoft völlig auf eine Auswertung der Daten.

  Im Treuhandmodell besteht nach den Erhebungen der Diözesandatenschutzbeauftragten die

Möglichkeit, dass durch eine Gesetzesänderung in den USA doch ein Zugriff auf die gespeicherten Daten – und zwar rückwirkend – zulässig wird. Wegen der erheblich geringeren Sicherheit hat die Konferenz der Diözesandatenschutzbeauftragten dieses Modell für die Dienststellen der Kirche nicht freigegeben. Keine Bedenken bestehen dagegen gegen das letzte bezeichnete Modell, in welchem eine ausschließliche Datenspeicherung im Inland stattfindet. Allerdings ist dieses Modell mehr als dreimal so teuer als das ursprüngliche mit physikalischer Datenspeicherung in den USA.

- Die **weitere dienstliche Kommunikation** kirchlicher Dienststellen findet nicht nur über den Postweg, das Telefon oder E-Mails statt. Vielfach besteht das Bedürfnis, daneben Messenger zu benutzen. Dies führt deswegen zu Problemen, weil die meistverbreitete Software „What's App" eine nicht datenschutzgerechte Anbindung an Facebook hat und die Speicherung der Verbindungsdaten außerhalb des Bereichs des europäischen Wirtschaftsraumes stattfindet. Facebook wiederum steht insbesondere nach dem im März 2018 bekannt gewordenen Datenskandal mit „Cambridge Analytics" im Verdacht, die von seinen Nutzern übermittelten Daten in einer Weise zu vermarkten, wie sie von den Nutzern nicht gewünscht wird. Die sicheren What's App-Alternativen „Threema" bzw. „Signal" sind nicht (vollständig) kostenlos – „Threema" kostet z.B. einmalig 2,99 € pro Nutzer - und weniger verbreitet.

  Ein besonderer Bedarf für den Messenger scheint insbesondere dort zu bestehen, wo Ehrenamtliche zum Einsatz kommen. In der Praxis zeigt es sich insbesondere bei Firm- oder sonstigen Jugendgruppen, dass die elektronische Kommunikation weitgehend unverzichtbar ist. Das Problem taucht allerdings auch beim E-Mail-Verkehr auf, lässt sich dort aber leichter lösen: Es ist anzustreben, dass zumindest alle hauptamtlichen und ein Teil der nebenamtlichen Mitarbeiter E-Mail-Adressen bekommen, die dem jeweiligen Ordinariat zugeordnet sind. Damit wird vermieden, dass dienstliche E-Mails von privaten Providern eingesehen werden können.

  Da sich die Einsicht durchgesetzt hat, dass ein bloßes Ankämpfen gegen diesen Messenger wenig Sinn machen würde, muss versucht werden, Schaden zu verhüten. Deswegen wird der Einsatz von What's App zur Übermittlung personenbezogener dienstlicher Daten untersagt; eine entsprechende Willensbildung der deutschen Diözesandatenschutzbeauftragten fand in mehreren Konferenzen 2017 statt. Soweit der Messenger zu privaten Zwecken eingesetzt wird, soll durch Anleitungen in der Downloadseite versucht werden, die Nutzer zu einer datenschutzgerechten Einstellung zu bewegen, die weiteren Schaden verhindert. Es kann zwar nicht übersehen werden, dass hierdurch das Verbot der dienstlichen Nutzung teilweise konterkariert wird, doch lässt eine Güterabwägung dies als hinnehmbar erscheinen.

- **Webauftritte:** Mittlerweile hat nahezu jede Kirchenstiftung und jeder Verband der Kirche einen Internetauftritt. Mit diesem hängen zahlreiche rechtliche Fragen zusammen, die sowohl das Impressum als auch die Notwendigkeit einer Datenschutzerklärung betreffen können. Für letztere gibt es mittlerweile Muster in der Downloadseite; die mit dem Internetauftritt zusammenhängenden Fragen bilden einen wichtigen Bestandteil meiner Beratungstätigkeit.

c. Vorabkontrollen

Vorabkontrollen waren bisher nach § 3 Abs. 5 KDO immer dann erforderlich, wenn die Einführung eines neuen Verfahrens erhöhte Risiken für den Schutz personenbezogener Daten mit sich bringen kann. Die Vorschrift der noch gültigen KDO lautet:

> *Eine Vorabkontrolle ist insbesondere durchzuführen, wenn*
> *1. besondere Arten personenbezogener Daten (§ 2 Abs. 10) verarbeitet werden oder*

2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,…

Zuständig war grundsätzlich der betriebliche Datenschutzbeauftragte, wenn es einen solchen gibt, sonst der diözesane (§ 3 Abs. 6 KDO). An die Stelle der Vorabkontrolle tritt mit dem Inkrafttreten des KDG ab 25.5.2018 die sogenannte „Folgenabschätzung“:

§ 35 Datenschutz-Folgenabschätzung und vorherige Konsultation

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Der elementare Unterschied zum bisherigen Recht besteht darin, dass künftig die Datenschutzaufsicht schon sehr früh in das Freigabeverfahren eingebunden werden kann:

(3) Ist der Verantwortliche nach Anhörung des betrieblichen Datenschutzbeauftragten der Ansicht, dass ohne Hinzuziehung der Datenschutzaufsicht eine Datenschutz-Folgenabschätzung nicht möglich ist, kann er der Datenschutzaufsicht den Sachverhalt zur Stellungnahme vorlegen.

Liegt nun eine solche Stellungnahme der Datenschutzaufsicht vor und enthält sie eine Freigabe, so bietet es sich an, dies auch in künftigen Verfahren zu berücksichtigen:

(5) Die Datenschutzaufsicht soll eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine Datenschutz-Folgenabschätzung gemäß Absatz 1 durchzuführen ist. Sie kann ferner eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

(6) Die Listen der Datenschutzaufsicht sollen sich an den Listen der Aufsichtsbehörden des Bundes und der Länder orientieren. Gegebenenfalls ist der Austausch mit staatlichen Aufsichtsbehörden zu suchen.

Dies entspricht recht weitgehend der bisher von mir bereits im Vorgriff auf das KDG so praktizierten Handhabung. Die frühzeitige Einbindung der Datenschutzaufsicht soll auch nach Ansicht der Konferenz der Diözesandatenschutzbeauftragten dazu führen, dass mehr Freigaben durch die Datenschutzaufsicht selbst erfolgen und diese Freigaben dann eine Doppelarbeit in anderen Bereichen vermeiden helfen.

Schließlich kann nur dann die mehrfache Durchführung der Vorabkontrolle hinsichtlich desselben Verfahrens vermieden werden, wenn diese Verfahren nicht nur zentral erfasst, sondern auch durch mit besondere Autorität versehene Personen freigegeben wurden. Deswegen hatte sich die Konferenz der Diözesandatenschutzbeauftragten schon bei den Vorberatungen zum KDG dazu entschlossen, bei der Neuformulierung im Hinblick auf die EU-Datenschutz-Grundverordnung die frühzeitige Einbindung des Diözesandatenschutzbeauftragten vorzuschlagen.

Folgende Verfahren wurden von mir im Berichtszeitraum im Rahmen einer möglichen Vorabkontrolle geprüft:

- VIS5 Aktensystem (Freigabe unter Auflagen)
- Microsoft One (Freigabe abgelehnt)
- Desknet (Kein Anlass für Vorabkontrolle)

- Euregon (Rückgabe an betrieblichen DSB; von diesem freigegeben)
- Altruja (Rückgabe an betrieblichen DSB; von diesem freigegeben)
- Siltot (Kein Anlass für Vorabkontrolle)
- Little Bird (keine Vorabkontrolle wegen vorangegangener Freigabe durch die EKD)
- inQS (Abgabe an bDSB der Caritas Köln)
- Easy Business Package (Vorabkontrolle nicht veranlasst)

d. Kontakte mit anderen Datenschutz-Aufsichtsstellen

Mit dem **bayerischen Landesbeauftragten für den Datenschutz** und seinen Mitarbeitern sowie dem Landesamt für Datenschutzaufsicht hatte ich regelmäßig persönlich und telefonisch Kontakt, zuletzt am 7.3.2018. Bei diesem Treffen ging es neben den mit der Einführung des neuen Rechts einhergehenden Fragen vor allem um folgende Probleme:

- Elektronische Kommunikation über E-Mail und What‘s App.
- Erforderliche Anzahl betrieblicher Datenschutzbeauftragter.

Die kommenden Monate werden im Hinblick auf den Datenschutz eine besonders kritische Zeit, die von allen damit Befassten ein Optimum an Leistungen verlangen wird. Ich wünsche uns bei der Bewältigung dieser Aufgaben Geduld, Weitblick und Gottes Segen.

J. Joachimski
Diözesandatenschutzbeauftragter