Kath. Datenschutzzentrum Frankfurt/M.

Tätigkeitsbericht 2019

2020

2021

2022

2023

2024

2025

Kath. Datenschutzzentrum
Frankfurt/M.

Tätigkeitsbericht 2019

Herausgegeben von der
Diözesandatenschutzbeauftragten für die (Erz-)Bistümer Freiburg, Fulda,
Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier

Kath. Datenschutzzentrum Frankfurt/M. KdöR
Domplatz 3
Haus am Dom
D-60311 Frankfurt/M.
Tel. 069/800 8718 800
Fax 069/ 800 8718 815
E-Mail: info@kdsz-ffm.de
www.kdsz-ffm.de

Hinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für beiderlei Geschlecht.
Titelmotiv: iStock

Inhaltsverzeichnis

Aufbau macht Fortschritte

Ein Tisch, ein Stuhl, eine Diözesandatenschutzbeauftragte, diese im ersten Bericht des Katholischen Datenschutzzentrums Frankfurt/M. für das Jahr 2018 beschriebene Situation hat sich im Jahr 2019 grundlegend geändert.

Im Jahr 2019 konnten die ersten eigenen Mitarbeiter für das Kath. Datenschutzzentrum Frankfurt/M. gewonnen werden und ihre Arbeit aufnehmen. Dies führte dazu, dass die zahlreichen Anfragen, Beschwerden, eingegangenen Meldungen von Datenschutzverletzungen in einer deutlich verbesserten Zeit beantwortet werden konnten. Die eingeleitete Veränderung der internen IT-Strukturen führte zu einer auch technischen Selbstständigkeit, die weitere Möglichkeiten eröffnete. Die Gespräche zur Gründung des Kath. Datenschutzzentrums Frankfurt/M. als Körperschaft des öffentlichen Rechts nahmen Fahrt auf, sodass auch die organisatorische Unabhängigkeit näher rückte.

Mit der am 1. März 2019 in allen im Zuständigkeitsbereich belegenen (Erz-)Bistümern in Kraft getretenen Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz wurde insbesondere der Bereich der technischen und organisatorischen Maßnahmen weiter gestärkt.

Im Jahr 2019 war zu konstatieren, dass die kirchliche Datenschutzgerichtsbarkeit ihre Arbeit aufgenommen hatte und offensichtlich von den betroffenen Personen auch in Anspruch genommen wurde.

Ursula Becker-Rathmair

Diözesandatenschutzbeauftragte und Leiterin des
Kath. Datenschutzzentrums Frankfurt/M.

1 Aus der Datenschutzaufsicht

Der Aufbau des Kath. Datenschutzzentrums Frankfurt/M., zuständig für die (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier, geht weiter mit großen Schritten voran. Im Berichtsjahr 2019 konnten zwei weitere Juristen an Bord begrüßt werden, zudem begann gleich Anfang des Jahres eine erfahrene Fachkraft das Sekretariat zu organisieren, um die Diözesandatenschutzbeauftragte und Leiterin der gemeinsamen Datenschutzstelle Frau Becker-Rathmair tatkräftig zu unterstützen. Mit dem zusätzlichen Beistand konnten nunmehr auch die ersten Prüfungen durchgeführt werden. Außerdem wurden die Bemühungen intensiviert, das Datenschutzzentrum als Körperschaft des öffentlichen Rechts (KdöR) zu errichten, um es mit einer eigenen öffentlich-rechtlichen Rechtspersönlichkeit auszustatten und die Unabhängigkeit des Datenschutzzentrums sicherzustellen.

2 Entwicklung des Datenschutzes

2.1 Datenschutzbewusstsein hat sich erhöht

Die Europäische Datenschutzgrundverordnung hat sich trotz aller Bedenken und Befürchtungen zu Beginn ihres Wirkens etabliert. Die Abkürzung „DSGVO“ ist zu einem gängigen Kürzel geworden und das nicht nur in Datenschutzkreisen. Sie hat dem neuen Datenschutz ihren Stempel aufgedrückt. Die Belastungen durch die EU-Verordnung hielten sich dann doch in Grenzen und sie hat in kurzer Zeit viel für den praktischen Datenschutz getan. Die datenschutzrechtlichen Belange sind deutlich in den Fokus der Öffentlichkeit gerückt. Die Sensibilisierung für den Schutz der eigenen Daten hat an Fahrt aufgenommen. Die vor allem von der Wirtschaft befürchtete Abmahn- und Bußgeldwelle ist dagegen weitgehend ausgeblieben.

2.2 Erste Änderungen am neuen Datenschutz

Die DSGVO lässt den EU-Mitgliedsstaaten durch Öffnungsklauseln Spielräume für nationale Datenschutzvorschriften. Davon hat die Bundesrepublik Deutschland unter anderem durch die Verabschiedung eines neuen Bundesdatenschutzgesetzes (BDSG) Gebrauch gemacht. Dieses ist zeitgleich mit der DSGVO in Kraft getreten. Erste Änderungen am BDSG gab es im Berichtszeitraum ebenfalls schon.

So wurde das Quorum des § 38 Abs. 1 BDSG für die Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten von bislang 10 auf 20 Personen heraufgesetzt:

§ 38 Abs. 1 Satz 1 BDSG:
„Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen."

Die Erhöhung der Benennungsgrenze war nicht unumstritten. Sie sollte kleineren Betrieben entgegenkommen. Ob diese Änderung allerdings das Handling für den Verantwortlichen wirklich leichter macht, wenn er sich ohne die Unterstützung eines betrieblichen Datenschützers um die komplexen Belange des Datenschutzes kümmern muss, darf bezweifelt werden.

Eine weitere Änderung betrifft § 26 BDSG. Die Einwilligung von Beschäftigten in die Verarbeitung ihrer personenbezogenen Daten kann nunmehr schriftlich oder elektronisch erfolgen:

§ 26 Abs. 2 Satz 3 BDSG:
„Die Einwilligung hat schriftlich oder elektronisch zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist."

Nach bisherigem Recht war für die Einwilligung die Schriftform nötig. Mitarbeitende können mit der Neuregelung jetzt also auch eine Einwilligung per E-Mail erklären.

2.3 E-Privacy-Verordnung rückt in weite Ferne

Eigentlich sollte die E-Privacy-Verordnung mit der DSGVO in Kraft treten, die Regelungen zur elektronischen Kommunikation konkretisieren und die Privatsphäre von Internet-Usern stärken. Doch aus dem EU-Gesetzgebungsvorhaben wird es wohl auf absehbare Zeit nichts. Zu weit scheinen die widerstreitenden Interessen dabei auseinander zu liegen. Die Mitgliedsstaaten stemmten sich unter anderem gegen die geplante Regelung zum Tracking auf Internetseiten über Cookies und das Erstellen von Nutzerprofilen durch website-übergreifende Datensammlungen. Ende 2019 sollte ein ganz neuer Anlauf genommen werden. Dass die neuen Entwürfe der EU ebenso datenschutzfreundlich ausfallen, darf bezweifelt werden. Vor allem die Digitalwirtschaft sieht durch die geplanten Regelungen in der E-Privacy-Verordnung ihre bestehenden Geschäftsmodelle in Gefahr.

2.4 KDG-DVO in Kraft

Die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) ist zum 1. März 2019 in Kraft getreten. Die neue Regelung wurde durch die Vollversammlung des Verbandes der Diözesen Deutschlands (VDD) am 19. November 2018 beschlossen. Sie ersetzt die bis dahin fortgeltende KDO-DVO.

In der neuen Regelung wurden insbesondere Anpassungen im Hinblick auf die Ausgestaltung der technischen und organisatorischen Maßnahmen gemäß § 26 KDG vorgenommen. Die Formulierung der Sicherheitsmaßnahmen zur Verarbeitung von Meldedaten in kirchlichen Rechenzentren sowie zu Schutzbedarf- und Risikoanalysen orientiert sich explizit an den Vorgaben des IT-Grundschutzkatalogs des Bundesamts für Sicherheit in der Informationstechnik (BSI) und den Schutzstandards der ISO 27001.

Die Klassifizierung personenbezogener Daten in drei Datenschutzklassen, die für diese Regulierungsinstanzen als Standard gilt, wurde zum Beispiel in den §§ 11, 12 und 13 KDG-DVO übernommen. Nach § 10 Abs. 1 KDG-DVO dient die Einordnung personenbezogener Daten in eine Datenschutzklasse der Feststellung des erforderlichen Schutzniveaus. Die Anforderungen zum Schutz personenbezogener Daten der Datenschutzklasse II (etwa Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten) wurden in der Durchführungsverordnung zum KDG erhöht. Gemäß § 12 Abs. 2 lit. e KDG-DVO hat die Übermittlung dieser Daten außerhalb eines geschlossenen und gesicherten Netzwerks grundsätzlich verschlüsselt zu erfolgen.

2.5 Wichtige Gerichtsentscheidungen

2.5.1 Setzen von Cookies erfordert aktive Einwilligung des Users

Der Europäische Gerichtshof (EuGH) hat am 1. Oktober 2019 (Az.: C-673/17) entschieden, dass die für die Speicherung und den Abruf von Cookies auf dem Gerät des Besuchers einer Website erforderliche Einwilligung durch ein voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, nicht wirksam erteilt wird.

In dem Rechtsstreit hatte sich der deutsche Bundesverband der Verbraucherverbände vor den deutschen Gerichten dagegen gewendet, dass die deutsche Planet49 GmbH bei Online-Gewinnspielen zu Werbezwecken ein Ankreuzkästchen mit einem voreingestellten Häkchen verwendet, mit dem Internetnutzer, die an einem solchen Gewinnspiel teilnehmen möchten, ihre Einwilligung in das Speichern von Cookies erklären. Die Cookies dienten zur Sammlung von Informationen zu Werbezwecken für Produkte der Partner der Planet49 GmbH. Dem Urteil des Gerichtshofs lag ein Ersuchen des Bundesgerichtshofs

(BGH) um die Auslegung des Unionsrechts über den Schutz der Privatsphäre in der elektronischen Kommunikation zugrunde (Az.: I ZR 7/16).

Der europäische Richterspruch stellt aus Datenschutzsicht vor allem klar, dass User in das Setzen von nicht notwendigen Cookies – und das sind die allermeisten – aktiv einwilligen müssen. Ein voreingestelltes Ankreuzkästchen genügt hierfür nicht.

2.5.2 Mitverantwortung für Datenweitergabe durch „Like-Button“

Ebenfalls im Jahr 2019 hat der EuGH über die datenschutzrechtliche Verantwortung bei Social Plugins entschieden. Konkret ging es um den „Gefällt mir“-Button von Facebook, den der Websitebetreiber „FashionID“ auf seiner Seite eingebunden hat und über den personenbezogene Daten der Besucher ohne deren Einwilligung und ohne Information an Facebook Ireland übermittelt wurden (Az.: C-40/17).

In diesem Fall hat der Gerichtshof geurteilt, dass der Betreiber einer Website, in der dieser Facebook-Button enthalten ist, für das Erheben und das Übermitteln der personenbezogenen Daten der Besucher seiner Website gemeinsam mit Facebook verantwortlich sein kann. Denn es kann nach Überzeugung des EuGH davon ausgegangen werden, dass der Shopbetreiber und Facebook Ireland gemeinsam über die Zwecke und Mittel entscheiden. Der Betreiber soll aber grundsätzlich nicht für die spätere Verarbeitung dieser Daten allein durch Facebook verantwortlich sein.

Vorsicht ist also beim Einbinden von Inhalten Dritter auf Internetseiten geboten.

2.5.3 Datenschutz bei der Arbeitszeiterfassung

Nach einer weiteren wichtigen Entscheidung des EuGH vom 14. Mai 2019 (Az.: C-55/18) müssen die Mitgliedsstaaten die Arbeitgeber verpflichten, ein System einzurichten, mit dem die tägliche Arbeitszeit der Beschäftigten gemessen werden kann. Da es sich dabei um personenbezogene Daten handelt, ist bei der Einführung von Zeiterfassungssystemen besonders auf den Datenschutz zu achten.

2.5.4 Facebook Fanpages besser abschalten

Das Bundesverwaltungsgericht (BVerwG) hat am 11. September 2019 (Az.: 6 C 15.18) entschieden, dass der Betreiber eines im sozialen Netzwerk Facebook unterhaltenen Unternehmensauftritts (Fanpage) verpflichtet werden kann, seine Fanpage abzuschalten, falls die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist. Gegenstand des Revisionsverfahrens war eine Anordnung der schleswig-holsteinischen Datenschutzaufsicht, mit der die Klägerin, eine

in Kiel ansässige Bildungseinrichtung, unter der Geltung der Datenschutzrichtlinie (Richtlinie 95/46/EG) verpflichtet worden war, die von ihr bei Facebook betriebene Fanpage zu deaktivieren. Zuvor hatte der EuGH auf Vorlage des BVerwG (Az.: 1 C 28.14) mit Urteil vom 5. Juni 2018 (Az.: C-210/16) entschieden, dass der Betreiber einer Fanpage für die durch Facebook erfolgende Datenverarbeitung mitverantwortlich ist.

> „Die Konferenz der Diözesandatenschutzbeauftragten spricht erneut die Empfehlung aus, auf das Betreiben einer Facebook-Fanpage zu verzichten, da eine datenschutzrechtliche Haftung des Betreibers einer Fanpage nicht wirksam ausgeschlossen werden kann."

Denn, so der EuGH, er ermöglicht durch den Betrieb der Fanpage Facebook den Zugriff auf die Daten der Fanpage-Besucher.

Bereits nach dem Urteil des EuGH hat die Konferenz der Diözesandatenschutzbeauftragten kirchlichen Einrichtungen empfohlen, auf das Betreiben einer Facebook-Fanpage zu verzichten, da eine datenschutzrechtliche Haftung des Betreibers einer Fanpage nicht wirksam ausgeschlossen werden kann. Der Beschluss vom 10. Oktober 2018 ist auf der Homepage des Datenschutzzentrums veröffentlicht und lautet:

„Die Konferenz der Diözesandatenschutzbeauftragten spricht erneut die Empfehlung aus, auf das Betreiben einer Facebook-Fanpage zu verzichten, da eine datenschutzrechtliche Haftung des Betreibers einer Fanpage nicht wirksam ausgeschlossen werden kann."

2.5.5. Strenge Anforderungen bei Videoüberwachung

Das höchste deutsche Verwaltungsgericht hat sich 2019 auch eingehend mit der Videoüberwachung beschäftigt (Az.: 6 C 2.18). In dem zugrunde liegenden Fall hatte eine Zahnärztin in ihrer Praxis eine Videokamera oberhalb des Empfangstresens angebracht, weil dieser nicht besetzt war und die Räumlichkeiten durch die Eingangstür ungehindert betreten werden konnten. Das BVerwG verneinte eine datenschutzrechtliche Erforderlichkeit.

Dem Urteil lag zwar noch die alte Gesetzeslage zugrunde. Die Richter trafen aber auch Aussagen zur Zulässigkeit der Videoüberwachung unter der seit 25. Mai 2018 geltenden DSGVO. Danach ist die Zulässigkeit von Videoüberwachungen zu privaten Zwecken nunmehr nach einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO zu beurteilen. Privaten Stellen stünde von vornherein keine Befugnis zur Verarbeitung personenbezogener Daten auf Grundlage von Art. 6 Abs. 1 lit. e DSGVO zu, soweit diesen keine Wahrnehmung hoheitlicher Aufgaben zukomme.

2.6 Erste Entscheidungen des Interdiözesanen Datenschutzgerichts

2.6.1 Weitergabe von Daten an das Jugendamt

In seinem ersten Fall hatte sich das Interdiözesane Datenschutzgericht (IDSG) mit der Frage der Weitergabe von personenbezogenen Daten an Sozialeinrichtungen bei einer vermuteten Kindeswohlgefährdung zu befassen (Beschluss vom 15. Mai 2019, Az.: IDSG 01/2018).

In einem katholischen Kindergarten stellten die Erzieherinnen wiederholt bei einem Kind Auffälligkeiten fest. Sie informierten darüber das zuständige Jugendamt, das jedoch bei einem Hausbesuch keine Gefährdung des Kindeswohls feststellen konnte. Die Eltern rügten daraufhin die unbefugte Offenbarung von Sozialdaten. Die Datenschutzaufsicht verneinte das Vorliegen einer Datenschutzverletzung durch den Kindergarten. Die hiergegen gerichtete Klage blieb letztlich ohne Erfolg. Das IDSG sah vorliegend die Information des Jugendamts als gerechtfertigt an.

2.6.2 Weitergabe von Daten an die Staatsanwaltschaft

In einem zweiten Fall vor dem IDSG ging es um die Weitergabe von Opferdaten in Fällen des sexuellen Missbrauchs an die Staatsanwaltschaft (Beschluss vom 23. Oktober 2019, Az.: IDSG 03/2018). Die Parteien stritten unter anderem über die datenschutzrechtliche Zulässigkeit der Weiterleitung eines Schreibens des späteren Klägers an die Staatsanwaltschaft. Darin hat er den Namen eines Priesters genannt, den er des sexuellen Missbrauchs bezichtigte. Er habe jedoch nicht sein Einverständnis in die Weitergabe seines Falles an die Staatsanwaltschaft erteilt. Das Datenschutzgericht sah das Weitergeben dieser Informationen wie schon die zuständige Datenschutzaufsichtsbehörde zuvor als rechtmäßig an. Gegen den Beschluss des IDSG wurde Rechtsmittel eingelegt (Az.: DSG-DBK 01/2019).

Das IDSG veröffentlicht ausgewählte Entscheidungen auf seiner Homepage.

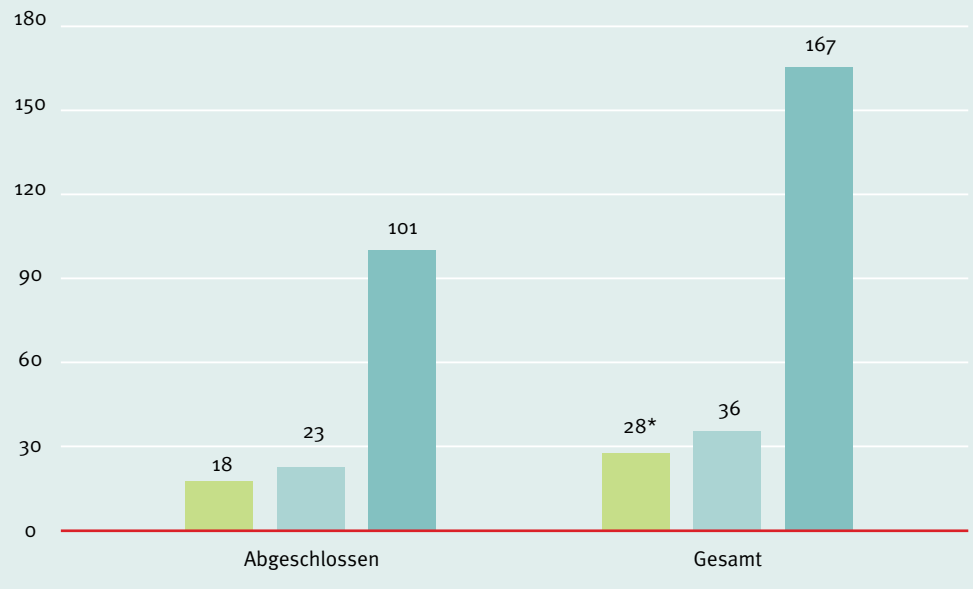
3 Schwerpunkte der Tätigkeiten im Berichtszeitraum

3.1 Meldungen von Datenschutzverletzungen nehmen Fahrt auf

Im Berichtszeitraum wurden insgesamt 167 Datenschutzverletzungen gemeldet. Die Meldungen kamen überwiegend aus den (Erz-)Bistümern Trier, Limburg und Freiburg. Die Datenschutzverletzungen betrafen vor allem die Bereiche Krankenhaus, Kindergarten und Einrichtungen der Caritas. Den gemeldeten Datenschutzverletzungen lagen wieder zahlreiche versendete E-Mails ohne BCC-Funktion, verirrte Arztbriefe und gestohlene Geräte wie beispielsweise Notebooks zugrunde. Neben diesen „Klassikern" gingen mehrere Meldungen zu Hackerangriffen und zu Verschlüsselungstrojanern ein, die ihr Unwesen auf Computern trieben. Bei anderen Meldungen konnte man sich des Eindrucks nicht erwehren, dass der Datenschutz als willkommener Anlass genommen wurde, es aber bei genauerer Betrachtung eigentlich um Diffamierungen, verletzte Eitelkeiten oder etwa schlicht um Rachegelüste ging.

Datenschutzeingaben im Jahr 2019 insgesamt und in diesem Zeitraum abgeschlossene Anfragen, Beschwerden und Meldungen über Datenschutzverletzungen

**Statistik des Kath. Datenschutzzentrums Frankfurt/M.
im Berichtszeitraum 1.1.2019 – 31.12.2019**



Anfragen
Beschwerden
Meldungen über Datenschutzverletzungen

* Keine genaueren Angaben möglich, weil nicht jede Anfrage ein eigenes Aktenzeichen bekommen hat. Vielen Anfragenden wurde direkt am Telefon oder umgehend per E-Mail geholfen.

3.1.1 Kindertagesstätten

Beliebt bei Langfingern sind Kindertagesstätten – vor allem an Wochenenden. Neben zerstörten Fenstern und Türen ist dabei der Verlust von Hardware und der sich darauf befindlichen Daten besonders ärgerlich. Zum Beuteschema gehörten insbesondere höherpreisige Geräte wie zum Beispiel Laptops, PCs, Diensthandys, Digitalkameras und externe Festplatten. USB-Sticks werden dagegen mittlerweile oft am Tatort zurückgelassen. Hieraus lässt sich womöglich ein allgemeiner Trend im Nutzerverhalten weg von betagteren Speichermedien feststellen.

Erschreckend für das Kath. Datenschutzzentrum Frankfurt/M. war, wie mangelhaft geschützt die teils sensiblen Daten auf den Geräten gespeichert sind – und welche Daten sich ab und an darauf befunden haben.

Ein drastischer Fall zeigte sich im Zuge des Diebstahls einer Spiegelreflexkamera in einem katholischen Kindergarten. In dem Fotoapparat befand sich noch die Speicherkarte mit zahlreichen Fotos der Kindergartenkinder – darunter auch einige Aufnahmen, auf denen diese im Rahmen eines Rollenspiels unbekleidet fotografiert wurden. Zweifelsohne ein gravierender Datenschutzverstoß, der weitreichende Konsequenzen – unter anderem die Einschaltung der Präventionsbeauftragten, die Anordnung, keine Fotos von unbekleideten Kindern egal aus welchen Gründen mehr anzufertigen und die Mitarbeiter nochmals eingehend im Datenschutz zu schulen – nach sich gezogen hat.

Die exemplarisch aufgeführten Datenschutzverletzungen zeigen, dass nach wie vor noch viel Aufklärungsarbeit nötig ist. Das Kath. Datenschutzzentrum Frankfurt/M. weist in diesen Fällen regelmäßig darauf hin, dass sich auf der Hardware möglichst keine personenbezogenen Daten befinden sollten und es sich speziell bei Kameras empfiehlt, den Speicherchip nach der Nutzung herauszunehmen und anderweitig zu lagern. Mit diesen einfachen Mitteln wäre bei Einbruchsdiebstählen zumindest nur der Verlust der Geräte zu beklagen.

3.1.2 Pflegeeinrichtungen

Dass bei Einbrüchen eigentlich unscheinbare Gegenstände durchaus das Interesse von Kriminellen wecken können, wenn diese nur ansprechend dargeboten werden, zeigt ein Vorfall in einer Pflegeeinrichtung. Dort befand sich ein Schlüsselbord mit Wohnungsschlüsseln und die dazugehörige Liste mit Adressen von „Essen auf Rädern“-Kunden gleich in der Nähe auf einem Schreibtisch. Die Kunden bekamen daraufhin bald Besuch und mussten Abschied von Schmuck und Bargeld nehmen. Eine Verknüpfung von Daten mit bösen Folgen. Hier waren größere vom Kath. Datenschutzzentrum Frankfurt/M. angeordnete Nachbesserungen bei den technischen und organisatorischen Maßnahmen nötig.

3.1.3 Bildungsbereich

Auch um Leben und Tod kann es bei einer unbedarften Weitergabe von Adressdaten ab und an gehen. Das zeigte ein weiterer Fall aus dem Berichtsjahr 2019. Eine Frau meldete sich bei einem Seminar an mit dem ausdrücklichen Hinweis, dass ihre Adresse nicht weitergegeben werden darf. Diese ist aus Sicherheitsgründen gesperrt. Aufgrund von Morddrohungen ihres Ex-Mannes musste sie bereits auf Anraten der Polizei den Wohnort wechseln.

Nichtsdestotrotz versandte der Seminaranbieter an sämtliche Teilnehmer eine Adressliste aller Teilnehmer zwecks Bildung von Fahrgemeinschaften. Ein an sich sinnvoller Gedanke. Nicht jedoch in diesem Fall, bei dem der Seminarort ausgerechnet auch noch in der Nähe des Wohnorts des Ex-Mannes lag. Hier war schnelles Handeln gefragt. Die Kursteilnehmer wurden mit „aktualisierten“ andersfarbigen Teilnehmerlisten versorgt mit der Bitte, diese zum Seminar mitzubringen und die alten Listen zu vernichten. Zu Kursbeginn wurde dann kontrolliert, ob nicht jemand möglicherweise eine alte Liste vor sich liegen hatte. Im Anschluss an die Meldung dieser Datenschutzverletzung begannen umfangreiche Arbeiten, um den Seminaranbieter datenschutzgerecht aufzustellen.

3.2 Beschwerdemöglichkeiten über Datenschutzverstöße werden genutzt

Insgesamt 36 Beschwerden sind im Berichtszeitraum über tatsächliche oder vorgebliche Datenschutzverletzungen im Kath. Datenschutzzentrum Frankfurt/M. eingegangen – eine deutliche Zunahme gegenüber 2018.

3.2.1 Fundraisingmaßnahmen

Einige Beschwerden richteten sich gegen die Verwendung von Meldedaten zur Durchführung von Spendenaktionen kirchlicher Einrichtungen. Hier gestaltete sich das Finden von Rechtsgrundlagen für Fundraisingmaßnahmen bisweilen für die betrieblichen Datenschutzbeauftragten vor Ort beschwerlich.

3.2.2 Krankenpost

Weitere Beschwerden betrafen Datenpannen im Krankenhausbereich. Die Petenten teilten beispielsweise mit, dass sie Rechnungen von anderen Patienten oder falsche Entlassbriefe übersandt bekamen. Ein Krankenhaus formatierte seine Schreiben so, dass bei einem Verrutschen des Schreibens der Betreff im Sichtfenster des Umschlags zu sehen war („2. Mahnung“). Hier konnte durch eine IT-seitige Änderung der Formatvorlage schnell Abhilfe geschaffen werden. Generell ist der Krankenhausbereich, in dem viele besondere Kategorien personenbezogener Daten gemäß § 4 Zi. 2 KDG verarbeitet

werden, ein sehr beratungsintensiver Bereich. Betrachtet man sich die zahlreichen Meldungen und Beschwerden zu Datenschutzverletzungen in Hospitälern genauer, lässt sich erkennen, dass die ganz überwiegende Zahl an Datenpannen im Trubel des Alltagsgeschäfts geschehen. Hieran zeigt sich die Wichtigkeit regelmäßiger Schulungen der Mitarbeiter durch die betrieblichen Datenschützer, um die Belegschaften immer wieder für den Datenschutz zu sensibilisieren.

> „Insgesamt 36 Beschwerden sind im Berichtszeitraum über Datenschutzverletzungen im Kath. Datenschutzzentrum Frankfurt/M. eingegangen – eine deutliche Zunahme gegenüber 2018."

3.2.3 Seniorenresidenz

Eine weitere Beschwerde, die ebenfalls zu einer Beanstandung führte, lag folgender Sachverhalt zugrunde. Der Bewohner eines Pflegeheims tätigte seine Bankgeschäfte auf einem Rechner in der Bibliothek, der zur Nutzung durch die Bewohner bereitstand. Auf diesem PC sollte kein Ausdrucken möglich sein. Dennoch kamen auf einem Drucker in der Verwaltung der Einrichtung gleich mehrfach Unterlagen zu den durchgeführten Bankvorgängen heraus. Die Ursache für dieses Phänomen an dem Bibliothekscomputer blieb letztlich unklar. Der Beschwerde wurde abgeholfen und der Verantwortliche aufgefordert, entsprechende technische und organisatorische Maßnahmen zu treffen, um solche unerwünschten Ausdrucke künftig zu unterbinden.

3.3 Anfragen weiter auf hohem Niveau

Das Kath. Datenschutzzentrum Frankfurt/M. erreichten auch wieder zahlreiche Anfragen – überwiegend von betrieblichen Datenschutzbeauftragten – in schriftlicher, elektronischer und telefonischer Form zu ganz unterschiedlichen Themen. Diese beschäftigten sich beispielsweise mit Fragen zum Datenaustausch im Konzern, zum Abschluss von Auftragsverarbeitungsverträgen, zum Umfang von Auskunftsansprüchen oder zur Zuständigkeit. Da vielen Anfragen direkt am Telefon oder umgehend per E-Mail abgeholfen werden konnte, bekam nicht jede Anfrage ein eigenes Aktenzeichen. Daher liegen hierzu im Gegensatz zu Datenschutzverletzungen und Beschwerden keine genaueren Zahlen vor.

3.3.1 Ökumenischer Energieversorger

Es war unter anderem die Frage zu klären, welchem Datenschutzrecht – weltlich oder kirchlich und wenn kirchlich, evangelisch oder katholisch – eine lokale Energieversorgungsgesellschaft unterfällt, die paritätisch von der katholischen und der evangelischen Kirche getragen wird. Letztlich kam das Kath. Datenschutzzentrum Frankfurt/M. nach umfangreichen Recherchearbeiten zu dem Ergebnis, dass die Gesellschaft dem welt-

lichen Recht zuzuordnen ist, mit der Folge, dass die DSGVO und nicht das KDG oder das DSGE-KD zur Anwendung kommt. Ausschlaggebend war, dass der Energieversorger zwar im weiteren Sinne kirchlich ist, jedoch keine kirchliche Einrichtung im Sinne des § 3 Abs. 1 KDG darstellt. Hierzu müsste sie vielmehr der kirchlichen Aufsicht unterliegen, was vorliegend nicht gegeben war. Die Frage, ob evangelisches oder katholisches Datenschutzrecht anwendbar und damit, welche Datenschutzaufsicht bei strikt paritätisch verteilten Gesellschaftsanteilen zuständig ist, stellte sich am Ende dann nicht mehr.

3.3.2 Weltliche und kirchliche Jugendhilfeeinrichtungen

Das örtliche Jugendamt einer Stadt wollte eine Befragung der Mandanten von Jugendhilfeeinrichtungen durchführen. Diese Einrichtungen befinden sich in städtischer als auch in evangelischer und katholischer Trägerschaft. Ein Datenschutzkonzept wurde zu dem Vorhaben ausgearbeitet, das auf der DSGVO beruhte. Die Nachfrage, an welche Datenschutzaufsicht sich Betroffene in den jeweiligen Einrichtungen bei Datenschutzfragen konkret wenden können, löste rege Betriebsamkeit aus.

3.4 Gerichtsverfahren

Erste Klagen vor dem Interdiözesanen Datenschutzgericht ließen im Berichtszeitraum ebenfalls nicht lange auf sich warten. Eine Klage gegen eine Entscheidung des Kath. Datenschutzzentrums Frankfurt/M. schaffte es 2019 bereits in die zweite Instanz.

3.4.1 Klage wegen angeblicher Untätigkeit

In einem Fall (Az.: IDSG 04/2019) wurde das Kath. Datenschutzzentrum Frankfurt/M. wegen Untätigkeit verklagt. Dem Ganzen zugrunde lag eine Beschwerde über versendete Weihnachtsgrüße eines Caritasverbands verbunden mit einer Einladung an sogenannte Wunschgroßeltern und Familien mit offenem E-Mail-Verteiler – statt über die BCC-Funktion. Das Datenschutzzentrum sah vorliegend jedoch keine weitergehende Datenschutzverletzung als das bereits gegenüber dem Verantwortlichen beschiedene nicht datenschutzkonforme Versenden der besagten E-Mail. Eine Entscheidung des Interdiözesanen Datenschutzgerichts wird für 2020 erwartet.

3.4.2 Vorwurf der Untätigkeit in zweiter Instanz

Eine weitere Klage wegen angeblicher Untätigkeit des Kath. Datenschutzzentrums Frankfurt/M. ist mittlerweile in zweiter Instanz beim Datenschutzgericht der Deutschen Bischofskonferenz anhängig (Az.: DSG-DBK 01/2019). Die Richter des Interdiözesanen Datenschutzgerichts konnten in erster Instanz keine Untätigkeit seitens der Datenschutzaufsicht erkennen. Der Kläger machte im vorliegenden Fall gegenüber einem im Zustän-

digkeitsbereich des Datenschutzzentrums Frankfurt/M. liegenden Bistum unter anderem geltend, Opfer sexuellen Missbrauchs durch einen Priester geworden zu sein. Er habe aber Stillschweigen über den Missbrauchsvorwurf vereinbart. Doch entgegen dieser Absprache habe das Bistum seine Akte an die Staatsanwaltschaft weitergegeben. Über die Entscheidung – die erste überhaupt – der zweiten Instanz wird gegebenenfalls im Tätigkeitsbericht für das Jahr 2020 zu lesen sein.

3.5 Umfangreiche Websiteprüfungen begonnen

Das Kath. Datenschutzzentrum Frankfurt/M. hat im Berichtszeitraum in größerem Umfang begonnen, die Websites von kirchlichen Einrichtungen in seinem Zuständigkeitsbereich auf Datenschutzkonformität zu prüfen. Schließlich ist die Website einer kirchlichen Einrichtung so etwas wie eine Visitenkarte, die von den Nutzern oft auch als Erstkontakt in Anspruch genommen wird. Umso wichtiger ist es, dass sich die User sicher sein können, dass auch beim elektronischen Kontakt mit ihren personenbezogenen Daten ein datenschutzsicherer und -gerechter Umgang seitens der Betreiber einer Website gewährleistet wird.

Begonnen wurde mit den Websites der sieben (Erz-)Diözesen im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M.

Im Mittelpunkt der Prüfung standen die Datenschutzerklärungen und Impressen der Internetauftritte. Darüber hinaus wurden die SSL-Verschlüsselung der Website, der Server-Standort und die rechtmäßige Verwendung von Cookie-Bannern geprüft.

> „Von den geprüften Websites katholischer Einrichtungen blieb keine ohne Beanstandung."

Im Rahmen der Prüfungen wurde unter anderem geschaut, ob die Betreiber ihren Informationspflichten gemäß dem KDG nachkommen und ob die Datenschutzerklärung auch die technischen Gegebenheiten tatsächlich abbildet. Hierzu waren im Vorfeld umfangreichere technische Prüfungen nötig, um die eingesetzten Tools wie zum Beispiel Cookies und Analyse-Werkzeuge oder die Einbindung von Social Media-Plattformen oder Kartendiensten auf der Website zu identifizieren. An dieser Stelle zeigte sich schnell, dass Softwareprogramme eingesetzt wurden, die in der Datenschutzerklärung nicht beschrieben wurden – aber auch umgekehrt, dass Tools aufgeführt wurden, obwohl diese auf der Website gar nicht verwendet wurden. Von den geprüften Websites katholischer Einrichtungen blieb keine ohne Beanstandung. Die Betreiber wurden über die Prüfergebnisse in Kenntnis gesetzt und zur Behebung der Mängel aufgefordert. Beanstandet wurden unter anderem Bezugnahmen auf die nicht einschlägige DSGVO, einzelne Rechtsgrundlagen der verschiedenen Datenverarbeitungen, das Setzen von Cookies ohne Einwilligung oder der Hinweis auf die aktivierte Anonymisierungsfunktion bei Google

Analytics in der Datenschutzerklärung, obwohl dies im Rahmen der technischen Prüfung nicht festgestellt werden konnte.

In der Folge waren bereits kurze Zeit nach den diesseitigen Schreiben konkrete Verbesserungen in den Datenschutzerklärungen auch hinsichtlich Transparenz und Verständlichkeit sichtbar. Technische Anpassungen wurden von den Verantwortlichen ebenfalls in enger Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten vor Ort und der Datenschutzaufsicht vorgenommen.

Im Anschluss an die Prüfungen der Internetauftritte der (Erz-)Bistümer Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier wurde mit den Website-Prüfungen der verschiedenen Caritasverbände und -zentren begonnen.

Weitere Prüfungen sind in Planung. Angesichts der unzähligen kirchlichen Einrichtungen zwischen Bodensee und Kassel können diese aber natürlich nur nach und nach erfolgen.

4 Veranstaltungen und Öffentlichkeitsarbeit

Auch im Jahr 2019 wurden wieder zahlreiche Dienstreisen unternommen, die Schulungszwecken und Fortbildungsmaßnahmen dienten, zum Beispiel nach Stuttgart zum zweiten Austauschforum Datenschutz des Diözesancaritasverbandes Rottenburg-Stuttgart, zum Treffen der Offizialate der Oberrheinischen Kirchenprovinz nach Mainz oder nach Schmerlenbach zur Qualifizierung von DiAG-MAV-Vorständen. Außerdem lud das Kath. Datenschutzzentrum Frankfurt/M. unter anderem die betrieblichen Datenschutzbeauftragten der Caritasverbände in den mittel- und südwestdeutschen (Erz-)Bistümern in den Erbacher Hof nach Mainz ein, um aktuelle datenschutzrechtliche Themen zu erörtern und Fragen im Zuge von Fundraisingmaßnahmen zu beantworten. Bei einem Treffen der betrieblichen Datenschutzbeauftragten des Erzbistums Freiburg und der Bistümer Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier im Haus am Dom in Frankfurt/M. informierte das Datenschutzzentrum unter anderem über die laufenden Websiteprüfungen und zeigte anhand von Fallbeispielen die Anwendung der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz auf.

Die Diözesandatenschutzbeauftragte ihrerseits nahm unter anderem Anfang 2019 am 13. Europäischen Datenschutztag in Berlin teil, im Mai am Daten-Tag „1 Jahr DSGVO“ der Stiftung Datenschutz und am Symposium „1 Jahr KDG – Rückblick und Ausblick“ in Siegburg, das vom Katholischen Datenschutzzentrum, zuständig für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster, veranstaltet wurde.

Die Information der Öffentlichkeit und der kirchlichen Stellen zum Umgang mit personenbezogenen Daten ist ein zentraler Bestandteil aufsichtlicher Tätigkeit. Die Aufgaben sind in § 44 Abs. 3 KDG klar benannt. Auch um diesen nachzukommen, hat sich das Kath. Datenschutzzentrum Frankfurt/M. im Internet neu aufgestellt und seine Website https://www.kdsz-ffm.de im Jahr 2019 komplett neu gestaltet. Zahlreiche Informationen und Materialien stehen Interessierten nunmehr dort zur Verfügung. Diese reichen von Gesetzestexten, Anordnungen und Verordnungen für die (Erz-)Bistümer, die zum Zuständigkeitsbereich des Datenschutzzentrums gehören, über Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten und praktischen Arbeitshilfen bis hin zu aktuellen Datenschutznachrichten im News-Ticker.

Selbstverständlich können weiterhin Datenschutzverletzungen über die Homepage gemeldet und betriebliche Datenschutzbeauftragte über die bekannten Formulare benannt werden. Neu integriert wurde die Möglichkeit, Beschwerden einfach per E-Mail zu übermitteln.

Die neu gestaltete Website enthält nunmehr auch die Möglichkeit für Betroffene, Beschwerden einfach per E-Mail zu übermitteln.

5 Meldungen von betrieblichen Datenschutzbeauftragten noch schleppend

Kirchliche Stellen haben als Verantwortliche die Benennung eines betrieblichen Datenschutzbeauftragten gemäß § 36 Abs. 2 KDG anzuzeigen. Für die Meldung von Datenschutzbeauftragten hat das Kath. Datenschutzzentrum Frankfurt/M. ein Formular auf seiner Homepage zur Verfügung gestellt. Bei Betrachtung der Meldezahlen ist jedoch auch für den Berichtszeitraum 2019 teilweise wieder nur eine schleppende Teilnahme zu verzeichnen. Die Neumeldungen hielten sich stark in Grenzen.

Eine Ausnahme bildet das Bistum Trier. Dies sei an dieser Stelle ausdrücklich erwähnt. Aus der westlichsten Diözese im Zuständigkeitsgebiet sind im letzten Jahr insgesamt 692 Meldungen eingegangen. Kirchliche Stellen im Erzbistum Freiburg nahmen immerhin nach 280 im Jahr 2018 noch 112 Meldungen vor und aus dem Bistum Rottenburg-Stuttgart wurden 19 Datenschutzbeauftragte gemeldet. Die Meldungen aus den restlichen Bistümern bewegten sich im einstelligen Bereich. Hier erhofft sich das Kath. Datenschutzzentrum eine regere Beteiligung. Sind doch die gemeldeten betrieblichen Datenschützer oft die ersten Ansprechpartner in Datenschutzangelegenheiten vor Ort und über das elektronische Melderegister schnell herauszufinden.

Gemeldete betriebliche Datenschutzbeauftragte aus den sieben Bistümern im Jahresvergleich

Bistümer	2018	2019
Freiburg	280	112
Fulda	9	6
Limburg	14	9
Mainz	42	3
Rottenburg-Stuttgart	21	19
Speyer	95	0
Trier	63	692
Gesamt	**524**	**841**

6 Vernetzung mit anderen Datenschutzaufsichten

Um zu einer möglichst einheitlichen Anwendung der Datenschutzregelungen beizutragen, sind die jeweiligen Datenschutzaufsichten nach § 46 KDG angehalten, auf eine enge Zusammenarbeit mit anderen Datenschutzaufsichten sowie staatlichen und sonstigen kirchlichen Aufsichtsbehörden hinzuwirken.

So haben sich die fünf Diözesandatenschutzbeauftragten auch im Jahr 2019 wieder mehrfach getroffen, um über aktuelle Themen zu beraten und ein einheitliches Handeln in der Datenschutzpraxis weiter voranzubringen. Diese Konferenz der Diözesandatenschutzbeauftragten beschäftigte sich beispielsweise in ihren Sitzungen Ende Januar in Frankfurt/M. und Ende März in Dortmund eingehend mit den möglichen Auswirkungen des Brexit und mit dem Thema Videoüberwachung.

Anfang April 2019 fand ein gemeinsames Treffen in Georgsmarienhütte mit Kollegen aus dem evangelischen Datenschutzbereich statt. Beim Treffen der Konferenz in Freising im Juli stand unter anderem der Entwurf zu dem geplanten Gesetz zum Schutz von Patientendaten in katholischen Einrichtungen des Gesundheitswesens auf der Tagesordnung. Weitere Treffen fanden Mitte September in Dortmund und im November in Berlin statt. Dabei ging es auch um die Evaluierung des KDG.

Neben einem regen regelmäßigen Austausch untereinander organisierte die katholische Datenschutzaufsicht in Dortmund einen gemeinsamen zweitägigen Workshop „Datenschutzrechtliche Prüfungen durch die kirchlichen Aufsichten“ Mitte Dezember 2019 im Haus Marienhof in Königswinter. Dieses Datenschutzauditorentraining in winterlicher Idylle bot reichlich Möglichkeiten zur Vernetzung unter den katholischen Datenschutzaufsichtsbehörden.

7 Beschlüsse aus der Konferenz der Diözesandatenschutzbeauftragten

Die Konferenz der Diözesandatenschutzbeauftragten erörtert aktuelle Themen und gemeinsame Anliegen aus dem Bereich des kirchlichen Datenschutzes. Sie erarbeitet gemeinsame Empfehlungen zur einheitlichen Handhabung der gesetzlichen Vorschriften und gibt diese in Form von Beschlüssen bekannt. Auch im Jahr 2019 hat sie einige zu wichtigen Themen gefasst. Die Beschlüsse im Wortlaut:

7.1 Beschluss über den Umgang mit Bildern von Kindern und Jugendlichen vom 4. April 2019

Umgang mit Bildern von Kindern und Jugendlichen

Mit Beschluss vom 4. April 2019 ist der Beschluss der Konferenz der Diözesandatenschutzkonferenz vom 18. April 2018 („Veröffentlichung von Fotos von Kindern und Jugendlichen unter 16 Jahren“) aufgehoben worden. Folgende Beschlüsse sollen den aufgehobenen Beschluss ersetzen:

1. Erhebung und Speicherung von Bildern

Für die Rechtmäßigkeit der Erhebung und Speicherung von Bildern von Kindern und Jugendlichen ist es nicht zwingend erforderlich, dass eine Einwilligung der Sorgeberechtigten vorliegen muss. Rechtsgrundlage für die Erhebung und Speicherung von Bildern kann auch – nach erfolgter Abwägung – das berechtigte Interesse nach § 6 Abs. 1 lit. g) KDG sein.

Grundsätzlich kann nicht ausgeschlossen werden, dass Bilder von Kindern und Jugendlichen auch im Rahmen des berechtigten Interesses nach § 6 Abs. 1 lit. g) KDG erhoben und gespeichert werden können. Das berechtigte Interesse nach § 6 Abs. 1 lit. g) KDG erfordert in jedem Fall eine Interessenabwägung zwischen dem berechtigten Interesse des Verantwortlichen oder eines Dritten an der Erhebung und Speicherung der Bilder und dem Interesse bzw. den Grundrechten und Grundfreiheiten der betroffenen Personen. Sofern das Interesse des Verantwortlichen oder des Dritten an der Erhebung und Speicherung der Bilder überwiegt, ist die Datenverarbeitung auch zulässig. Die Interessenabwägung ist vor der Erhebung und Speicherung von Bildern durchzuführen und unterliegt der vollständigen aufsichtsbehördlichen Kontrolle. Da es sich um Bilder von Kindern und Jugendlichen handelt, sind deren Interessen besonderes zu werten und zu berücksichtigen. Relevant können hier insbesondere Merkmale wie z.B. das Alter des betroffenen Kindes, der Zweck der Verarbeitung oder die Gruppengröße, aber auch die Eingriffsintensität sowie die Wahrscheinlichkeit des Eintritts eines Schadens sein. Die durch den Verantwortlichen durchgeführte Interessenabwägung unter besonderer Berücksichtigung der Interessen der Minderjährigen ist auf Anforderung der Datenschutzaufsichtsbehörde nachzuweisen. ▶

2. Verarbeitung durch Übermittlung/Verbreitung

Für den Fall, dass die Bilder durch eine Übermittlung/Verbreitung verarbeitet werden sollen, ist es in der Regel erforderlich, dass die Sorgeberechtigten einwilligen. Ausnahmen können sich dann ergeben, wenn ein berechtigtes Interesse nach § 6 Abs. 1 lit. g) KDG vorliegt. Im Rahmen der durchzuführenden Interessenabwägung können die Grundsätze des § 23 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie herangezogen werden.

a) Einwilligung

Die Verarbeitung durch Übermittlung/Verbreitung von personenbezogenen Daten (hier konkret die Bilder von Kindern und Jugendlichen) ist in der Regel nur mit einer Einwilligung der Sorgeberechtigten zulässig. Die Verarbeitung durch Übermittlung/Verbreitung umfasst jeden Vorgang, durch den andere Personen, Stellen, Behörden oder Einrichtungen Kenntnis von den personenbezogenen Daten erlangen oder erlangen können. Konkret bedeutet dies, dass jede Herausgabe von personenbezogenen Daten aus der jeweiligen Einrichtung an bspw. Eltern, Presse, Internetseite, o.ä. eine Verarbeitung durch Übermittlung/Verbreitung darstellt. Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands sieht es als ausreichend an, wenn die Einwilligung für konkret benannte Veranstaltungen vor bzw. bei Beginn des Schul- oder Kitajahres für das jeweilige Jahr eingeholt wird. Die Einwilligung kann entweder unmittelbar im Anmeldeprozess oder am ersten Schul- oder Kita-Tag eingeholt werden. Das Erfordernis, dass das konkrete Bild im Zeitpunkt der Unterzeichnung der Einwilligungserklärung vorliegen soll, entfällt.

b) Berechtigtes Interesse

Ausnahmen zur Einwilligung können sich dann ergeben, wenn ein berechtigtes Interesse nach § 6 Abs. 1 lit. g) KDG vorliegt. Auch hier ist eine Interessenabwägung zwingend erforderlich (s. Punkt 1). Insbesondere sind aufgrund der spezifischen Gefahren einer Verarbeitung durch Übermittlung/Verbreitung die Interessen der Kinder und Jugendlichen besonders zu berücksichtigen. Je größer der (un-)bekannte Personenkreis ist, der von den Bildern Kenntnis nimmt oder Kenntnis nehmen kann, desto höher und intensiver ist der Eingriff in die Interessen oder die Grundrechte und Grundfreiheiten der Kinder und Jugendlichen. Im Rahmen der Interessenabwägung können die Grundsätze des § 23 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie herangezogen werden. Eine Dokumentation der durchgeführten Interessenabwägung ist auch auf Anforderung der Datenschutzaufsichtsbehörde nachzuweisen.

3. Grundsätzlicher Hinweis

Sofern der jeweilige Verantwortliche beabsichtigt, die Bilder aufgrund einer Einwilligung zu verarbeiten und die betroffene Person die Einwilligung nicht erklärt, ▶

nicht wirksam erklärt oder widerrufen hat, so ist ein Rückgriff auf das berechtigte Interesse oder eine andere Rechtsgrundlage ausgeschlossen.

4. Informations- und Transparenzpflichten

Sowohl bei der Erhebung und Speicherung als auch bei der Verarbeitung durch Übermittlung/Verbreitung von Bildern sind die Informationspflichten nach dem KDG einzuhalten. Während die Informationspflichten bei der Erhebung und Speicherung sowie bei der Verarbeitung durch Übermittlung/Verbreitung aufgrund einer Einwilligung keine Besonderheiten aufweisen, sind bei der Verarbeitung durch Übermittlung/Verbreitung aufgrund des berechtigten Interesses einige Punkte zu beachten. Wenn bei Aufzügen, bei Veranstaltungen oder ähnlichen Ereignissen eine unüberschaubar große Menge von Menschen fotografiert wird, ist es naheliegend, dass die Verarbeitung der Daten derjenigen, die als „Beiwerk" abgelichtet werden, nicht mit deren Kenntnis erfolgt. Die insoweit vorhandene Informationspflicht kann aber nach § 15 Abs. 4 KDG zurücktreten, wenn sich die Erteilung der Information aufgrund der unüberschaubaren Menge der Betroffenen als unmöglich erweist oder einen unverhältnismäßig großen Aufwand erforderlich machen würde. Bei der Beurteilung sind jeweils die Umstände des Einzelfalls maßgeblich. Es gilt also keineswegs generell, dass die Informationspflichten zurücktreten. Abhängig vom tatsächlichen Bild kann es auch beim Fotografieren von Sehenswürdigkeiten oder Veranstaltungen mit einem vertretbaren Aufwand möglich sein, die Informationspflichten nach § 15 KDG bei der Erhebung der personenbezogenen Daten zu erfüllen. Dies hat zur Folge, dass die vorgenannte Ausnahme nicht eintreten kann. Die Informationserteilung muss auch nicht zwangsläufig durch den Fotografen erfolgen. Bei Veranstaltungen ist es beispielsweise möglich, dass der Verantwortliche die Teilnehmer über die Anfertigung und die Verarbeitung durch Übermittlung/Verbreitung von Fotografien informiert. Ist eine solche Information aufgrund der Struktur der Veranstaltung von vorneherein unmöglich, spricht vieles dafür, dass die Erfüllung der Informationspflichteneinen unverhältnismäßig großen Aufwand erfordern würde(vgl. § 15 Abs. 4 KDG). Wenn die Umstände des Einzelfalls so sind, dass aus den genannten Gründen eine Informationspflicht zurücktreten kann, ist es dem Fotografen nicht zumutbar, im Nachhinein die von seinen Aufnahmen erfassten Personen zu identifizieren, um ihnen die nach dem kirchlichen Datenschutzgesetz grundsätzlich zustehenden Informationen zukommen zu lassen. Nach § 13 KDG ist er nicht verpflichtet, zur Einhaltung dieses Gesetzes zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffenen Personen zu informieren. Wird demgegenüber eine überschaubare Menge von Personen fotografiert, ist der Verantwortliche natürlich verpflichtet, seinen Informationspflichten nach §§ 14-16 KDG nachzukommen. Diese Bewertung des Umgangs insbesondere mit der Verarbeitung durch Übermittlung/Verbreitung von Fotos versteht sich als eine Erläuterung, welche ergänzt werden kann.

7.2 Beschluss zur Auftragsverarbeitung mit externen Dienstleistern vom 4. April 2019

Verträge zur Auftragsverarbeitung mit externen Unternehmen

Die Konferenz der Diözesandatenschutzbeauftragten weist darauf hin, dass bei Abschluss von Verträgen kirchlicher Einrichtungen mit Stellen, die nicht dem KDG unterliegen, zumindest eine Bezugnahme auf das aktuelle KDG in den Vertragstext aufgenommen werden soll.

Erläuterung zu dem Beschluss:

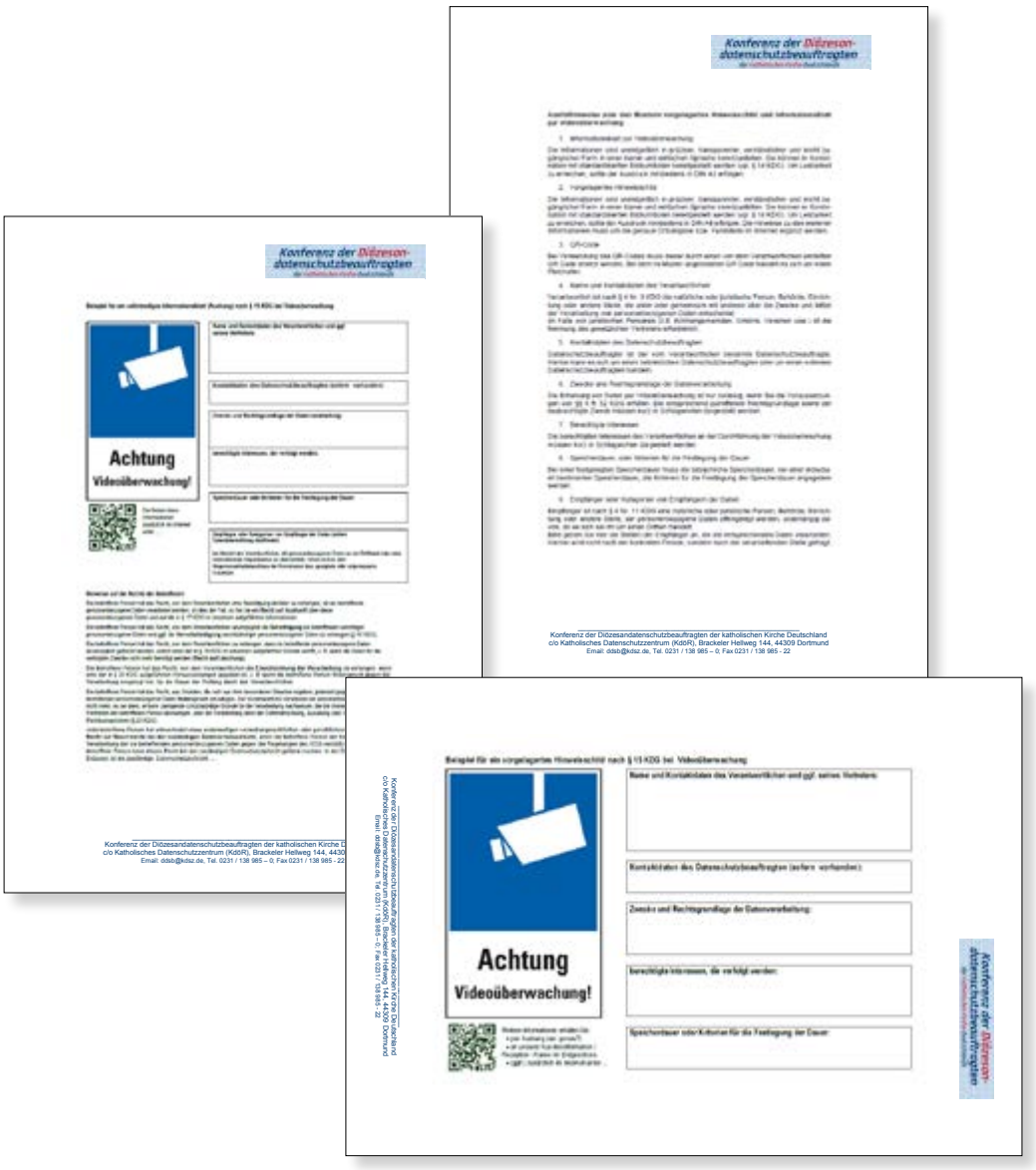
Soweit sich kirchliche Stellen bei der Verarbeitung personenbezogener Daten anderer Stellen bedienen, haben sie – je nach Gegenstand der Vereinbarung – ihre Pflichten nach dem KDG vertraglich abzusichern bzw. auch auf die andere Stelle zu übertragen. Dies wird regelmäßig durch die Bezugnahme auf das KDG im Vertrag geschehen. Hat der Vertragspartner einen Vertrag, der ausreichende Regelungen zu Datenschutz enthält, aber auf die entsprechenden Normen der DSGVO verweist, sollte zumindest ein pauschaler Verweis auf das Kirchliche Datenschutzgesetz in den Vertrag aufgenommen werden. Ist auch dieser pauschale Verweis nicht möglich, sollte in einem Begleitschreiben zum Vertrag auf das Kirchliche Datenschutzrecht (KDG) hingewiesen werden. Auch hier müssen aber ausreichende Regelungen zum Datenschutz im Vertrag vorhanden sein.

7.3 Beschluss und Muster zur Videoüberwachung vom 4. Juli 2019

Muster zur Videoüberwachung

Die Konferenz der Diözesandatenschutzbeauftragten hat in Ihrer Sitzung am 4. Juli 2019 in Freising das beigefügte Muster inkl. Erläuterungen beschlossen. Das Dokument steht auch zum Download auf der Homepage de Datenschutzzentrums.

Beispiel für ein vorgelagertes Hinweisschild nach § 15 bei einer Videoüberwachung



7.4 Beschluss über die Möglichkeit der Einwilligung in schlechtere technische und organisatorische Maßnahmen vom 19. September 2019

Möglichkeit der Einwilligung in schlechtere technische und organisatorische Maßnahmen

In der Praxis kommt es zu Fällen, in denen die betroffene Person eine Einwilligung in Abweichungen von Aspekten der Datensicherheit erteilen soll. Beispielhaft zu nennen ist an dieser Stelle die Einwilligung in unverschlüsselte Kommunikation per Email beim Versand von besonderen Kategorien personenbezogener Daten. Da in diesen Fällen regelmäßig die Einwilligung nach § 6 Absatz 1 lit b) bzw. § 11 Absatz 2 lit a) KDG nicht als eigentliche Rechtsgrundlage für die Verarbeitung dienen soll, sondern hier für eine an sich schon gerechtfertigte Verarbeitung eine negative Abweichung von technischen Schutzmaßnahmen zum Datenschutz legitimiert werden soll, kann die Einwilligung diese Abweichung des durch § 26 KDG gesetzlich geforderten Schutzstandards nicht erreichen.

Die Konferenz der Diözesandatenschutzbeauftragten hat daher folgenden Beschluss gefasst: Die Konferenz der Diözesandatenschutzbeauftragten beschließt für sich folgende Auslegung des KDG in dieser Frage:

1. Die in § 26 KDG normierte Verpflichtung des Verantwortlichen, geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus zu treffen, ist zwingender Natur und steht mithin nicht zur Disposition der an der Datenverarbeitung Beteiligten.

2. Insbesondere darf eine Einwilligung im Sinne des § 6 Absatz 1 lit. b) bzw. § 11 Absatz 2 lit. a) KDG nicht verlangt werden, um nicht ausreichend geeignete technische und organisatorische Maßnahmen durch den Betroffenen zu legitimieren.

Die aufgeführten Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten aus dem Jahr 2019 stehen zum Herunterladen und weiteren Gebrauch auf der Website des Kath. Datenschutzzentrums Frankfurt/M. zur Verfügung:

https://www.kath-datenschutzzentrum-ffm.de/beschluesse-der-konferenz/

8 Arbeitshilfe zum Einsatz von Office 365

Im Berichtszeitraum hat das Kath. Datenschutzzentrum Frankfurt/M. in Zusammenarbeit mit den Kollegen in Dortmund eine Arbeitshilfe erstellt, um bei der datenschutzrechtlichen Bewertung eines Einsatzes von Office 365 auf der Plattform der Microsoft Cloud zu unterstützen. Die Arbeitshilfe „Datenschutzrechtliche Bewertung eines Einsatzes von Office365 auf der Plattform der Microsoft Cloud“ aus dem Februar 2019 im Wortlaut:

Datenschutzrechtliche Bewertung eines Einsatzes von Office 365 auf der Plattform der Microsoft Cloud

Vorbemerkung:
Das Katholische Datenschutzzentrum Frankfurt/M. (KDSZ-FFM) hat sich bereits von Juli 2017 bis Februar 2018 mit der Frage befasst, ob die als „Microsoft Cloud Deutschland“ beworbene Cloud-Lösung der Microsoft Deutschland, die zusammen mit der T-Systems als Datentreuhänder und völlig getrennt vom restlichen globalen Microsoft-Netz erbracht wurde unter Datenschutzaspekten zulässig betrieben werden kann. Eine europäische oder weltweite Cloud-Lösung des Unternehmens wurde damals nicht betrachtet und nicht bewertet. Inzwischen hat Microsoft am 31.08.2018 das Angebot der „Deutschland Cloud“ zum Jahresende 2018 – zumindest für Neukunden – abgekündigt. Stattdessen sollen die deutschen Rechenzentren in Berlin und Frankfurt als neue „Rechenzentrumsregion Deutschland“ in das globale Microsoft-Netz integriert werden. Die Moderation durch einen Daten-Treuhänder wird komplett entfallen. Microsoft sichert die umfassende Befolgung der DSGVO zu, macht aber über die konkrete Umsetzung keine weiteren Angaben.

> „Damit ist Microsoft definitiv dazu verpflichtet, US-Behörden auf Anforderung Beweismaterial von europäischen Servern zur Verfügung zu stellen.“

Wenige Monate zuvor wurde mit Unterzeichnung am 28. März 2018 der US-amerikanische „CLOUD-Act“ (Clarifying Lawful Overseas Use of Data-Act) verabschiedet. Dieses Gesetz verpflichtet US-Unternehmen, amerikanischen Sicherheitsbehörden Zugriff auch auf Nutzerdaten zu ermöglichen, die außerhalb der USA gespeichert sind. Hintergrund der umstrittenen Gesetzgebung in den USA war ein jahrelanger Streit über den Zugriff auf Daten, die US-Firmen auf Servern im Ausland gespeichert haben. Der US-Supreme Court sollte eigentlich in diesem Jahr ein Urteil fällen, ob Microsoft E-Mails von einem in Irland stehenden Server herausgeben muss. Doch nach der Verabschiedung des CLOUD-Acts erklärte das oberste US-Gericht den Fall für erledigt. Damit ist Microsoft definitiv dazu verpflichtet, US-Behörden auf Anforderung Beweismaterial von europäischen Servern zur Verfügung zu stellen. Damit werden normalerweise

übliche Verfahren in internationalen Rechtsstreitigkeiten und Strafverfolgungen, nämlich die Anwendung von Rechtshilfeabkommen (Mutual Legal Assistance Treaty) unter Beteiligung der heimischen Behörden, umgangen. Dies wäre ein bußgeldbewehrter Verstoß gegen Artikel 48 DSGVO.

Durch die neuen Rahmenbedingungen wird die datenschutzrechtliche Betrachtung von Office 365-Projekten nicht einfacher. Auf den ersten Blick sind die Datenschutzrisiken in Office 365-Projekten durch den Verzicht auf den Treuhänder, die Integration der Microsoft-Rechenzentren in das globale Netzwerk sowie die drohende Anwendung des CLOUD-Acts deutlich größer geworden. Jeder Verantwortliche, der Microsoft mit der Auftragsverarbeitung seiner Daten z.B. im Rahmen einer Office 365-Anwendung beauftragt, muss sich dieser Risiken bewusst sein und entsprechende Maßnahmen treffen.

Durch den Auftraggeber zu beachtende / zu regelnde Aspekte:
Bei Office 365 von Microsoft handelt es sich um einen Cloud-Dienst, konkret in Form eines SaaS (Soft-ware-as-a-Service). Zwischen dem Kunden und Microsoft ist daher regelmäßig ein Auftragsverarbeitungsvertrag gem. § 29 KDG bzw. Art. 28 DSGVO abzuschließen. Microsoft hat sich nach den Regeln des „EU/U.S.PrivacyShields“ selbst auditiert und in die Privacy-Shield-Liste eintragen lassen. Damit ist die erste Hürde, nach der eine Auftragsverarbeitung im außereuropäischen Ausland nur nach Nachweis eines angemessenen Datenschutzniveaus erlaubt ist, zunächst genommen, zumindest so lange, wie das Konstrukt des Privacy-Shield-Abkommens von der europäischen Datenschutzrechtsprechung akzeptiert wird.

Unseres Wissens stellt Microsoft einen Vertragsentwurf zu Verfügung und wird i.d.R. im Vertrag zusichern, die Bestimmungen der europäischen Datenschutznormen einzuhalten. Es sind jedoch Zweifel erlaubt, was eine solche Zusicherung wert ist, wenn Microsoft gemäß des CLOUD-Acts gezwungen werden kann, entgegen den Bestimmungen des Auftragsverarbeitungsvertrages, Daten gegenüber Dritten (den US-Behörden) offenzulegen.

Demnach bestehen zwei hauptsächliche Risiken, deren Eintritt zum Entfall der Rechtsgrundlage einer Auftragsverarbeitung durch Microsoft führen:

- die eventuell gerichtlich festgestellte Unwirksamkeit des Privacy-Shield-Abkommens
- die Erzwingung einer Offenlegung von Daten aufgrund des CLOUD-Acts durch US-amerikanische Behörden.

Dazu kommen die üblichen Risiken, die immer mit der Auswahl und Beauftragung eines externen Dienstleisters verbunden sind: ungeplanter, plötzlicher Ausfall des Dienstleisters durch Insolvenz oder mangelndes Interesse des Dienstleisters an der Weiterführung

der Geschäftsbeziehung, ungeplante Erhöhung der Kosten durch Ausnutzen einer Monopolstellung, Abfluss von unternehmenskritischem Know-how.

Der Verantwortliche ist nach § 26 KDG verpflichtet, technische und organisatorische Maßnahmen zu treffen, die die Sicherheit der Datenverarbeitung gewährleisten. Zu den Schutzzielen gehören u. a. die Vertraulichkeit und die Verfügbarkeit der Daten. Identifizierte Risiken sind zu berücksichtigen und zusammen mit der Wirksamkeit der getroffenen Maßnahmen kontinuierlich zu beobachten.

Exit-Strategie:
Aufgrund der hohen Wahrscheinlichkeit des Eintritts eines der o. a. Risiken ist aus Sicht des KDSZ-FFM, für den Fall der erzwungenen Vertragsbeendigung eine realistische Exit-Strategie vorzuhalten, die es erlaubt, die an Microsoft ausgelagerten Dienste innerhalb der meistens 90-tägigen Kündigungsfrist ins eigene Haus oder zu anderen, datenschutzkonform arbeitenden Dienstleistern zu übertragen.

Eine Exit-Strategie umfasst mindestens die folgenden Elemente:

- Auswahl eines Ersatz-Dienstleisters (ggf. Insourcing), der ggf. vertraglich zu einer Stand-By-Bereitschaft im erforderlichen Umfang verpflichtet wird
- Erstellung von Beschaffungsplänen für alle notwendigen Beschaffungen, die mit einem Dienstleisterwechsel oder einem Insourcing verbunden sind, einschließlich evtl. Infrastrukturmaßnahmen
- Hochrechnung von Laufzeiten für die Rückübertragung der Daten auf Basis der aktuellen und der prognostizierten Datenmengen
- Überprüfung der Machbarkeit und der Laufzeit einer Datenrückübertragung anhand von Stichproben
- Vorbereitung von Benutzeranleitungen für die Datenrückübertragung sowie geänderten Prozessbeschreibungen für den Betrieb nach der Umstellung

Die Exit-Strategie ist während der gesamten Laufzeit der Dienstleistung aktuell zu halten, an organisatorische und technische Änderungen anzupassen und ihre Wirksamkeit zu überprüfen (z. B. die Zeit, die für eine Rückladung großer Mengen von Daten (Postfächer) aus der Microsoft-Cloud benötigt wird oder auch die Lieferzeit für evtl. neu zu beschaffende Hardware im eigenen Haus).

Customer Lockbox:
Um Transparenz über die Zugriffe auf personenbezogene Daten sicherzustellen, die im Wartungsfall von Beschäftigten von Microsoft und der von diesem Unternehmen eingesetzten Unterauftragnehmer vorgenommen werden, die in einem Drittland außerhalb der EU ansässig sind, für das kein Angemessenheitsbeschluss der Europäischen

Kommission i.S. v. § 40 KDG vorliegt, und Zugriffsbegehren bei besonderen Risikokonstellationen ablehnen zu können, ist die Funktion „Customer Lockbox“ zu aktivieren. Hiervon kann nur dann abgesehen werden, wenn die Datenverarbeitung keine Risiken für die Rechte und Freiheiten der betroffenen Personen birgt. Der Einsatz der Funktion bewirkt, dass zuständige Mitarbeiter des Auftragnehmers vor jedem Supportfall mit Zugriff auf Kundendaten eine explizite Einwilligung des Auftraggebers einholen müssen. Die sachkundige Beantwortung dieser Anfragen und die Erteilung der Einwilligung sind sicherzustellen.

Berechtigungskonzept:
Die Cloud-Angebote von Microsoft bieten detaillierte Möglichkeiten, Zugriffsrechte der Mitarbeiter der eigenen Institution zu verwalten. Die Cloud-Berechtigungen müssen im Rollen- und Rechtekonzept der Institution festgelegt werden.

Um eventuelle unberechtigte Datenzugriffe sowohl durch Mitarbeiter des Kunden als auch durch Supportmitarbeiter von Microsoft zumindest nachträglich erkennen zu können, sind die für die jeweiligen Produkte vorgesehenen Protokollierungsfunktionen zu aktivieren und die Protokolle regelmäßig zumindest stichprobenartig unter Beteiligung des behördlichen bzw. betrieblichen Datenschutzbeauftragten zu prüfen.

Mehr-Faktor-Authentifizierung:
Sobald personenbezogene Daten mit den Cloud-Angeboten verarbeitet werden sollen, ist Mehr-Faktor-Authentifizierung einzusetzen, wobei einer der Faktoren der Nachweis des Besitzes z. B. eines Endgerätes oder Sicherheitstokens sein muss. Der zum Nachweis des Besitzes eingesetzte Faktor darf durch die Nutzer nicht kopiert werden können. (Die Anfertigung von Sicherheitskopien im Rahmen des Notfallmanagements ist zulässig.) Microsoft bietet mehrere Mehr-Faktor-Authentifizierungsverfahren an. Ein weltweit möglicher Zugriff der Nutzer auf personenbezogene Daten, welche allein durch ein Passwort geschützt sind, ist nicht zulässig.

Datenklassifizierung:
Sollten Daten der Kategorien gemäß § 4 Abs. 2 KDG verarbeitet werden, so sind die von Microsoft angebotenen Verfahren zur Klassifizierung von Daten entsprechend ihres Schutzbedarfes zu nutzen. In Grenzen kann die Klassifizierung auch automatisiert erfolgen.

Verschlüsselung der Daten:
Soweit Daten gemäß § 4 Abs. 2 KDG nicht umfänglich, aber mehr als gelegentlich verarbeitet werden sollen, sind weitere Schutzmaßnahmen zu treffen, die gewährleisten, dass diese Daten verschlüsselt in der Cloud gespeichert werden, wobei die Hoheit über die Schlüssel bei dem Auftraggeber liegen muss. Aufgrund der damit einhergehenden hohen Risiken (vgl. § 35 Abs. 4 KDG) ist eine umfangreiche Verarbeitung von

Daten der o. g. Kategorien der Microsoft Cloud voraussichtlich nicht zulässig. Als Alternative bietet sich dann nur der Einsatz äquivalenter Microsoft-Produkte in einer privaten Cloud an.

Fazit

Eine datenschutzkonforme Nutzung der Microsoft-Cloud-Angebote ist nach Auffassung des KDSZ-FFM aktuell zwar möglich, die Verantwortlichen tragen jedoch ein hohes Risiko, dass die Konformität zu KDG und DSGVO kurzfristig entfallen kann. Das wiederum führt dazu, dass der Verantwortliche jederzeit bereit und in der Lage sein muss, die Dienstleistung schnellstmöglich zu beenden und seinen Rechenbetrieb trotzdem fortzuführen.

Das Risiko besteht zwar grundsätzlich bei jeder Auftragsverarbeitung, ist aber im Fall von Office 365 besonders hoch einzustufen, da der Geschäftsbetrieb i. d. R. ohne Office-Anwendungen kaum fortgesetzt werden kann und der Standort des Dienstleisters in den USA ein besonders hohes Risiko der Nichtvereinbarkeit mit Datenschutzregeln mit sich bringt.

Der Mehraufwand einer deshalb unverzichtbaren Exit-Strategie muss von Anfang an in die Projekte und den laufenden Aufwand eingerechnet werden.

Weitere Maßnahmen zur Erhöhung der Datensicherheit und des Datenschutzes, besonders im Zusammenhang mit der Bearbeitung von Servicefällen (Tickets), sind dringend empfohlen.

9 Ausblick

Das Kirchliche Datenschutzgesetz hat seinen Platz im Gefüge des Datenschutzes selbstbewusst neben der Europäischen Datenschutzgrundverordnung eingenommen. Es zeigt sich bereits – trotz seines erst kurzen Bestehens –, dass es das Grundrecht jedes Einzelnen auf informationelle Selbstbestimmung tatkräftig unterstützt und voranbringt. Konkrete Hilfestellung leistet dabei die zugehörige Durchführungsverordnung zum KDG, die im März 2019 in Kraft getreten ist.

Die gestiegene Bedeutung des Datenschutzes ist auch in den (Erz-)Bischöflichen Ordinariaten und kirchlichen Einrichtungen deutlich zu spüren. Das Bemühen vor Ort ist unverkennbar. Deshalb stehen für das Kath. Datenschutzzentrum Frankfurt/M. Beratung und Hilfe immer im Vordergrund. Dennoch wird es in Zukunft wohl nicht zu vermeiden sein, dass die Datenschutzaufsicht auch Sanktionierungen von Datenschutzverstößen bis zur Verhängung von Bußgeldern vornehmen muss.

Eine Schlüsselstellung kommt den internen und externen betrieblichen Datenschutzbeauftragten zu, die an der Schnittstelle von Praxis und Aufsicht in beide Richtungen wichtige Arbeit leisten. Sie sind für die Datenschutzaufsicht ein zentraler Hebel, um den Schutz personenbezogener Daten auch künftig weiter effektiv zu verbessern.

10 Die fünf Datenschutzaufsichten der Katholischen Kirche in Deutschland

Der Diözesandatenschutzbeauftragte der (Erz-)Bistümer Hamburg, Hildesheim, Osnabrück und des Bischöflich Münsterschen Offizialats in Vechta i.O.

Unser Lieben Frauen Kirchhof 20
28195 Bremen
Diözesandatenschutzbeauftragter:
Andreas Mündelein

Katholisches Datenschutzzentrum (KdöR)

Brackeler Hellweg 144
44309 Dortmund
Diözesandatenschutzbeauftragter:
Steffen Pau

Kath. Datenschutzzentrum Frankfurt/M. KdöR

Haus am Dom, Domplatz 3
60311 Frankfurt am Main
Diözesandatenschutzbeauftragte:
Ursula Becker-Rathmair

Diözesandatenschutzbeauftragter der ostdeutschen Bistümer und des Katholischen Militärbischofs

Im Badepark 4
39218 Schönebeck
Diözesandatenschutzbeauftragter:
Matthias Ullrich

Datenschutzbeauftragter der Bayerischen (Erz-)Diözesen

Kapellenstraße 4
80333 München
Diözesandatenschutzbeauftragter:
Jupp Joachimski

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

Kath. Datenschutzzentrum Frankfurt/M.

Tätigkeitsbericht 2019