

Gemeinsame Datenschutzaufsicht der Bayerischen (Erz-)Diözesen

Diözesandatenschutzbeauftragter

Schrammerstr.3, 80333 München
Telefon 089 2137 1796
Telefax 089 2137 27 1796
Email: jjoachimski@eomuc.de
München, den 1.10.2021

An die Hochwürdigsten Herren
Erzbischöfe und Bischöfe
der bayerischen Kirchenprovinzen

Bericht des Diözesandatenschutzbeauftragten
Berichtszeitraum 1.10.2020 bis 30.9.2021

Eminenzen,
Exzellenzen,

dieser Bericht schließt an denjenigen vom 1.10.2020 an. Er enthält keine organisatorischen Hinweise;
in dieser Beziehung bitte ich um Beachtung meines Berichts vom 9.9.2021.

A. Die Entwicklung des Datenschutzrechts seit 1.10.2020

I. Europäische Union

1. Gesetzgebung der EU

An sich stand die **Evaluierung der EU-DS-GVO** zum Mai 2020 an. Wegen der Corona-Pandemie kann weiterhin nur schwerlich davon ausgegangen werden, dass innerhalb kürzerer Zeit ein tragfähiges Ergebnis im EU-Parlament erzielt werden kann.

Bereits 2017 legte die EU-Kommission den ersten Entwurf für die **ePrivacy-Verordnung** vor. Die deutsche EU-Ratspräsidentschaft hat dann im November 2020 einen überarbeiteten Entwurf vorgelegt. Die Verordnung soll die Vertraulichkeit elektronischer Kommunikation stärken. Der EU-Ministerrat einigte sich am 10. Februar 2021 auf eine Version, die Grundlage

seiner Position in den folgenden Trilog-Verhandlungen werden soll. Dieser Entwurf wird aber von Deutschland und Österreich als unzureichend abgelehnt .

2. Datenverkehr EU – USA

In meinem Bericht vom 1.10.2020 habe ich dargestellt, warum durch das Urteil des europäischen Gerichtshofes vom 16.7.2020 („Schrems II“) der Datenverkehr mit den USA erheblich belastet wird. An dieser Situation hat sich bis jetzt nichts geändert. Es fehlt offensichtlich der Regierung der Vereinigten Staaten die Motivation, einen Ersatz für das vom europäischen Gerichtshof als obsolet betrachtete „privacy shield“ zu schaffen.

Zwar hat der Europäische Datenschutzausschuss am 18.6.2021 Empfehlungen für die Verwendung von Standarddatenschutzklauseln veröffentlicht¹ , doch ist allgemeine Meinung, dass durch Vertragsbestimmungen allein ein legaler Datenverkehr mit den USA nicht ermöglicht werden kann. Es bedarf drastischer Maßnahmen zur Beschränkung der Datenübermittlung seitens des Absenders in der Europäischen Union und des Empfängers in den Vereinigten Staaten. Solange kein neues Abkommen zwischen der US-Regierung und der EU geschlossen ist, kann von einem freien Datenverkehr nicht ausgegangen werden. Das wird sich spätestens am Ende der Pandemie vor allem auf die sozialen Medien auswirken. Es gibt jetzt bereits gewichtige Stimmen unter den Landesdatenschützern, welche den Datenverkehr in diesem Bereich als illegal ansehen.

3. Auswirkungen des Austritts von Großbritannien aus der EU

Bis 31.7.2021 galt insoweit eine Übergangsnorm, welche die Fortsetzung des Datenverkehrs mit Großbritannien in gleicher Weise wie mit einem EU-Land ermöglichte. Am 28. Juni 2021 hat die EU-Kommission einen Angemessenheitsbeschluss gem. Art. 45 DSGVO erlassen, wonach Großbritannien dauerhaft als sicherer Drittstaat eingestuft wird. Er gilt auch im kirchlichen Bereich. Damit bedürfen Datenübermittlungen aus der EU/dem EWR an das Vereinigte Königreich, im Rahmen des Anwendungsbereichs der Beschlüsse, keiner besonderen Genehmigung.

Der Angemessenheitsbeschluss hat eine Laufzeit von vier Jahren (27. Juni 2025). Während dieser Zeit will die EU-Kommission anhand festgelegter Verfahren überprüfen, ob das Datenschutzniveau in Großbritannien sich auch weiterhin auf dem geforderten Niveau bewegt. Sollte es Entwicklungen geben, durch die der Datenschutz abgebaut wird, behält sich die Kommission vor, den Beschluss einzuschränken oder sogar komplett aufzuheben. Schon jetzt gibt es zahlreiche kritische Stimmen zur Entwicklung des Datenschutzes im Vereinigten Königreich.

¹ https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

II. Änderungen des deutschen Datenschutzrechts

Der Bundestag hat das **Gesetz zum Schutz elektronischer Patientendaten**² in der Telemedizininfrastruktur am 3. Juli 2020 beschlossen, am 18. September 2020 hat das Gesetz den Bundesrat passiert. Im Oktober 2020 ist es in Kraft getreten, wirksam wurde es ab 1. Januar 2021.

III. Änderungen des kirchlichen Datenschutzrechts

Nach seinem § 58 Abs. 2 soll das **Kirchliche Datenschutzgesetz** innerhalb von drei Jahren überprüft werden. Diese Überprüfung ist immer noch im Gange und war bereits Gegenstand mehrerer Sitzungen der Konferenz der Diözesandatenschutzbeauftragten. Ein tragfähiger Entwurf für die Neufassung wird spätestens im Jahre 2022 vorliegen.

In mehreren deutschen (Erz-) Bistümern wurde die **Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen** in Kraft gesetzt. Ich hielt das für Bayern deswegen nicht notwendig, weil das Bayerische Krankenhausgesetz eine sehr sachgerechte Regelung anbietet. Gemäß § 2 Abs. 2 KDG findet dieses Gesetz Anwendung, sofern die Kirche kein eigenes spezielles Gesetz für diesen Zweck erlässt.

In allen deutschen (Erz-) Bistümern wurde das **Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz** in Kraft gesetzt. Es regelt die Handhabung von Eingaben durch die Datenschutzaufsicht und schafft Klarheit über die notwendigen Verfahrensvoraussetzungen.

Im Vorgriff auf eine Änderung des **Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)** hat die Evangelische Kirche in Deutschland zum 01. Juli 2021 eine gesetzesvertretende **Ordnung zum Zwecke der institutionellen Aufarbeitung sexualisierter Gewalt (Aufarbeitungsverordnung-AVO)** erlassen.

Mit der Änderung des EKD-Datenschutzgesetzes wird ein neuer § 50a DSG-EKD geschaffen, der auch Regelungsinhalte der zunächst geplanten Aufarbeitungsverordnung aufnimmt. Diese wird daneben nicht mehr benötigt. Die Änderung des DSG-EKD ist aber so gefasst, dass daneben eine ausführende Verordnung weiter möglich ist. § 50a ist das Ergebnis einer grundsätzlichen Interessenabwägung durch den Gesetzgeber. Auf der einen Seite steht das Recht auf informationelle Selbstbestimmung möglicher Betroffener sexualisierter Gewalt und möglicher Beschuldigter oder Täter/innen. Auf der anderen Seite steht das Interesse an der institutionellen Aufarbeitung sexualisierter Gewalt. Beide Interessen finden im vorliegenden Entwurf angemessene Berücksichtigung.

Satz 1 stellt fest, dass an der **institutionellen Aufarbeitung sexualisierter Gewalt** ein **überragendes kirchliches Interesse** besteht. Es wurde mit dem „überragenden Interesse“ bewusst ein neuer Terminus eingeführt. Bei der Verarbeitung nach § 50a geht es nicht nur um die abstrakte Möglichkeit, personenbezogene Daten zu verarbeiten, es soll vielmehr deutlich gemacht werden, dass zur institutionellen Aufarbeitung keine Alternative besteht.

² BGBl. 2020, 2115

Absatz 2 ermöglicht die **Offenlegung von personenbezogenen Daten** zum Zwecke der institutionellen Aufarbeitung sexualisierter Gewalt an zwei besondere Personengruppen, nämlich **unabhängige Wissenschaftler/innen** und **von der kirchlichen Stelle Beauftragte**.

Es erscheint mehr als nur sinnvoll, dass auch die katholische Kirche sichere Rechtsgrundlagen für eine transparente, konsequente und umfassende Aufarbeitung sexualisierter Gewalt im kirchlichen Kontext schafft.

B. Wichtige Gerichtsentscheidungen

In einem Rechtsstaat erfolgt die Rechtsetzung nicht allein durch Gesetze und Verordnungen, sondern auch durch Gerichtsentscheidungen. Im Gegensatz zum „Common Law“ (Großbritannien und USA) erlangen im deutschen Recht Gerichtsentscheidungen aber nicht quasi Gesetzeskraft, sondern bieten nur Anhaltspunkte für die Auslegung des kodifizierten Rechts. Wegen der sehr weit gehenden, wenn auch nicht vollständigen Begriffsgleichheit in der EU-DS-GVO und dem KDG sind auch die Entscheidungen des EuGH und der staatlichen deutschen Gerichte für die Rechtsauslegung gleichermaßen bedeutsam wie die Entscheidungen der kirchlichen Datenschutzgerichte. Folgende Entscheidungen staatlicher und kirchlicher Gerichte erschienen mir besonders erwähnenswert:

Entscheidungen zum materiellen Datenschutzrecht

IDSG 05/2019 vom 09.12.2020 zur Eintragung im Taufregister³

Die datenschutzrechtliche Prüfung der Eintragung eines Kirchenaustritts im Taufregister ist beschränkt auf die formelle Richtigkeit. Das Datenschutzgericht prüft nicht die materiellen innerkirchlichen Wirkungen einer Austrittserklärung.

OVG Hamburg, Beschluss vom 15.10.2020 zum Begriff der Datenverarbeitung veröffentlicht in ZD 2021, 278

Eine „Verarbeitung“ gem. Art. 4 Nr. 2 DS-GVO setzt eine Handlung im Sinne einer menschlichen Aktivität voraus. Die bloße Lagerung personenbezogener Daten, ohne dass mit diesen Daten „umgegangen“ wurde oder „umgegangen“ wird, stellt keine Verarbeitung in diesem Sinne dar.

IDSG 02/2019 vom 18.06.2020 zur Zulässigkeit der Datenweitergabe an die Caritas

Wenn eine Pfarrei oder ein Pfarrverband die in ihrer/seiner Meldedatenbank gespeicherten Namen und Anschriften der Pfarr(verbands)angehörigen zu dem Zweck nutzt, Spendenaufrufe für Caritas-Sammlungen, zu deren Durchführung die Pfarreien durch bischöfliche Anordnung verpflichtet sind, in die Briefkästen der Pfarr(verbands)angehörigen einwerfen zu

³ Sämtliche Entscheidungen des IDSG sind auf der Webseite der DBK abrufbar: <https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen>

lassen, nimmt sie/er eine nach dem kirchlichen Datenschutzrecht zulässige Verarbeitung personenbezogener Daten vor.

IDSG 02/2018 vom 05.05.2020 zu Bewerbungsunterlagen

Unzulässigkeit der Weiterleitung einer Bewerbung an einen früheren Arbeitgeber zwecks Erlangung von Informationen über den Bewerber.

IDSG 03/2019 vom 22.04.2020 zur Veröffentlichung von Mitarbeiterdaten

Die Veröffentlichung der mit dem Namen und Vornamen gebildeten dienstlichen E-Mail-Adresse eines Mitarbeiters mit Außenkontakten (hier eine Küsterin) auf der Homepage der Pfarrgemeinde verletzt keine kirchlichen Datenschutzrechte.

BGH, 28.5.2020, zur Einwilligung als Rechtfertigung der Datenverarbeitung; veröffentlicht in ZD 20230, 467

Eine wirksame Einwilligung in telefonische Werbung i.S.v. § 7 Absatz 2 Nummer 2 Fall 1 UWG liegt nicht vor, wenn der Verbraucher bei der Erklärung der Einwilligung mit einem aufwändigen Verfahren der Abwahl von in einer Liste aufgeführten Partnerunternehmen konfrontiert wird, das ihn dazu veranlassen kann, von der Ausübung dieser Wahl Abstand zu nehmen (= „opt out“) und stattdessen dem Unternehmer die Wahl der Werbepartner zu überlassen. Weiß der Verbraucher mangels Kenntnisnahme vom Inhalt der Liste und ohne Ausübung des Wahlrechts nicht, die Produkte oder Dienstleistungen welcher Unternehmer die Einwilligung erfasst, liegt keine wirksame Einwilligung für den konkreten Fall vor.

LG Frankfurt/M zum Strafschadensersatz nach Art. 82 DS-GVO veröffentlicht in ZD 2020, 639

Nicht jede Datenschutzrechtsverletzung in Form einer nicht (vollständig) rechtskonformen Datenverarbeitung stellt automatisch einen ersatzfähigen Schaden dar. Vielmehr muss die Verletzungshandlung auch zu einer konkreten Verletzung von Persönlichkeitsrechten der betroffenen Person geführt haben. Eine weite Auslegung des Schadensbegriffs gem. Art. 82 DS-GVO, wonach mit jedem Verstoß ein Schaden begründet wird, widerspricht der Systematik des deutschen Rechts.

BayVerfGH, Entscheidung vom 21.10.2020 zur Kontaktdatenerfassung anlässlich der Corona-Pandemie, veröffentlicht in BayVBI 2021, 20

Im des Infektionsschutzes, der bei Eintritt eines Pandemiegeschehens kurzfristige Reaktionen Bereich des Ordnungsgebers auf sich ändernde Gefährdungslagen erforderlich machen

kann, erscheint es nicht offensichtlich unzulässig, wenn der Gesetzgeber eine offene Generalklausel als Ermächtigungsgrundlage vorhält, die dem Ordnungsgeber ein breites Spektrum an geeigneten Maßnahmen eröffnet.

IDSG vom 01.03.2021 zur Einsichtnahme des Pfarrers in Gottesdienstbesucherlisten, (rechtskräftig seit 12.07.2021 - DSG-DBK 01/2021)

Die Einsichtnahme in Gottesdienstbesucherlisten durch den leitenden Pfarrer zur Überprüfung der Vollständigkeit der Liste und der Einhaltung sowie Evaluierung des Coronaschutzkonzeptes ist durch § 6 Abs. 1 Buchstaben a und d KDG in Verbindung mit der Coronaschutzverordnung NRW gedeckt.

OVG Lüneburg, Beschluss vom 22.7.2020, zur Übersendung eines Bescheids per Fax veröffentlicht in ZD 2020, 653

Bei der Übermittlung von personenbezogenen Daten per Fax muss die Behörde zur Gewährleistung des Grundrechts auf informationelle Selbstbestimmung des Betroffenen Sicherungsvorkehrungen treffen. Welches Schutzniveau dabei einzuhalten ist, richtet sich nach der Sensibilität und Bedeutung der zu übermittelnden Daten, den potenziellen Gefahren bei der Faxübermittlung, dem Grad der Schutzbedürftigkeit des Betroffenen und dem mit den Sicherungsmaßnahmen verbundenen Aufwand.

BayVerfGH, Beschluss vom 21.5.2019, zur Namensnennung von Bewerbern gegenüber der Personalvertretung, veröffentlicht in ZD 2020, 663

I.R.d. Mitbestimmung der Personalvertretung über Arbeitnehmersetzungen ohne Bestenauslese kann die namentliche Übermittlung sozialer Auswahldaten über Beschäftigte, die eine Versetzung beantragen, aber nicht zum Zuge kommen, einen gravierenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art.2 Abs. 1 GG) bzw. das Grundrecht auf Schutz personenbezogener Daten (Art. EUGRCHARTA2007 Artikel 8 GRCh) darstellen, im Vergleich zu dem der Informationsanspruch der Personalvertretung nach bayerischem Landesrecht nicht pauschal überwiegt, was einem generellen Anspruch der Personalvertretung auf eine nicht anonymisierte Preisgabe dieser Auswahldaten entgegensteht.

AG Hannover, Urteil vom 9.3.2020, zum Schadensersatz bei Datenschutzverstößen, veröffentlicht in ZD 2021, 176

Sofern Ansprüche auf Ersatz des immateriellen Schadens gem. Art. 82 Abs. 1 DS-GVO im Wege der Abtretung von Dritten geltend gemacht werden, besteht – mangels Übertragbarkeit dieses höchstpersönlichen Anspruchs – keine Aktivlegitimation. Nicht bereits jede Datenschutzrechtsverletzung in Form einer nicht (vollständig) rechtskonformen Datenverarbeitung ist automatisch auch ein ersatzfähiger Schaden. Für einen Bagatelverstoß ohne ernsthafte

Beeinträchtigung bzw. für jede bloß individuell empfundene Unannehmlichkeit ist kein Schmerzensgeld zu gewähren; vielmehr muss dem Betroffenen ein spürbarer Nachteil entstanden sein und es muss um eine objektiv nachvollziehbare, mit gewissem Gewicht erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen gehen.

Entscheidungen zum Bereich der Datenschutzaufsicht:

VG Mainz, Urteil vom 22.7.2020, zu den Anforderungen an eine datenschutzrechtliche Beschwerde, veröffentlicht in ZD 2021, 59

Eine datenschutzrechtliche Beschwerde muss alle Informationen enthalten, die erforderlich sind, dass die Aufsichtsbehörde den Sachverhalt erfassen und ggf. weiter aufklären, ihre Zuständigkeit überprüfen und etwaige Datenschutzverstöße feststellen kann. Die Beschwerde muss daher zumindest Angaben über die betroffene Person und den Verantwortlichen enthalten und zumindest ansatzweise zum Ausdruck bringen, welcher Verstoß gegen datenschutzrechtliche Vorschriften gerügt wird. Der Beschwerdeführer kann von der Aufsichtsbehörde keine Ermittlungen ins Blaue hinein verlangen.

VG Ansbach, Urteil vom 16.3.2020, zur Reaktion der Datenschutzaufsicht, veröffentlicht in ZD 2020, 607

1. Ein Anspruch des Betroffenen eines Datenschutzverstoßes auf aufsichtliches Einschreiten der Datenschutzaufsichtsbehörde ergibt sich lediglich bei einer Ermessensreduktion auf Null.
2. Dies gilt auch für einen Anspruch auf Verhängung eines Bußgelds nach Art. 83 DS-GVO, da ein solches ebenfalls im Ermessen der Datenschutzaufsichtsbehörde steht.

OVG Rheinland-Pfalz, Urteil vom 26.10.2020, zum Prüfungsumfang bei Datenschutzbeschwerden, veröffentlicht in ZD 2021, 446⁴

Erhebt eine betroffene Person eine Beschwerde i.S.v. Art. 77 DS-GVO, muss sich die Aufsichtsbehörde mit der Beschwerde befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten. Maßstab für den Umfang der Ermittlungen sind insb. die individuelle Bedeutung der Sache und die Schwere des in Rede stehenden Verstoßes. Ein Beschwerdeführer hat jedoch weder Recht auf einen Bescheid bestimmten Inhalts noch auf eine bestimmte Entscheidung in seiner Sache. Eine im Verwaltungsrechtsweg erhobene Klage gem. Art. 78 DS-GVO gegen die Entscheidung der Aufsichtsbehörde kann sich nur auf die Überprüfung der ordnungsgemäßen Entgegennahme,

⁴ Diese Entscheidung lässt sich m. E. nicht problemfrei auf das Verfahren nach dem KDG bzw. der KDSGO anwenden. § 14 Abs. 2c KDSGO gibt dem Betroffenen das Recht, jedenfalls die Feststellung der Datenschutzverletzung als Ziel zu verfolgen.

Prüfung und Bescheiderteilung, nicht jedoch auf die materielle Rechtmäßigkeit des Bescheids der Aufsichtsbehörde beziehen.

ähnlich: VG Berlin, Beschluss vom 21.4.2021, veröffentlicht in ZD 2021, 452

Es besteht auch nach Maßgabe der DS-GVO kein Anspruch gegen die Datenschutzaufsichtsbehörde auf eine konkrete Maßnahme.

und VG Ansbach, Urteil vom 7.12.2020, veröffentlicht in ZD 2021, 452:

Bei der Abschlussmitteilung einer Datenschutzaufsichtsbehörde handelt es sich um eine vom Verwaltungsgericht gem. Art. 78 DS-GVO überprüfbare Maßnahme mit Außenwirkung, jedoch nicht um einen Verwaltungsakt mit Regelungscharakter, sodass nicht die Versagungsklage, sondern die allgemeine Leistungsklage statthaft ist. Die Untersuchungspflicht des Art. 57 Abs. 1 lit. f DS-GVO enthält dezidierte Vorgaben zum Verfahren und dessen Umfang, die über Art. 78 Abs. 2 DS-GVO zu einem Rechtsanspruch des Betroffenen auf Befassung und Überprüfung seiner Beschwerde führen können. Der Beschwerdeführer hat gegen die Aufsichtsbehörde gem. Art. 58 DS-GVO einen Anspruch auf fehlerfreie Ermessensausübung, jedoch grundsätzlich nicht auf aufsichtliches Einschreiten. Die Aufsichtsbehörde hat ein weites Entschließungs- und Auswahlermessen.

Zur Verhängung von Geldbußen

IDSG vom 16.7.2020⁵

Juristische Personen haften in Bezug auf Geldbußen als Verantwortliche gemäß dem Funktionsträgerprinzip für schuldhaftes Datenschutzverstöße aller ihrer Mitarbeiter unabhängig davon, ob die Mitarbeiter eine Organstellung oder eine andere Führungsposition (§ 30 Abs. 1 OWiG) innehaben.

Dies wird wie folgt begründet: Das für die Geldbußen gemäß der DSGVO geltende Funktionsträgerprinzip ist auch bei der Verhängung von Geldbußen nach kirchlichem Datenschutzrecht gemäß § 51 KDG anzuwenden. Die Übertragung des europarechtlichen Funktionsträgerprinzips auf das kirchliche Bußgeldrecht wird bereits durch die Präambel des KDG nahegelegt. Danach will das KDG den Einklang des kirchlichen Datenschutzrechts mit der DSGVO herstellen. Außerdem gebietet der Grundsatz der Effektivität des Datenschutzes die Anwendung des Funktionsträgerprinzips (§ 51 Abs. 2 KDG, Art. 83 Abs. 1 DSGVO).⁶

⁶ Hier übersieht das IDSG § 3 OWiG („nulla poena sine lege“): Aus rechtstaatlichen Gründen kann die Anwendung einer Strafnorm nicht mit einer Analogie begründet werden. Das KDG enthält in § 51 Abs.1 die Schuld des Verantwortlichen als Voraussetzung für die Geldbuße. Eine dem Art. 82 Abs.3 DSGVO entsprechende Vorschrift fehlt im kirchlichen Datenschutzrecht.

IDSG-01-2020_vom_14.12.2020

Werden personenbezogene Daten im Bereich einer juristischen Person verarbeitet, ist grundsätzlich die juristische Person als Rechtsträger der betroffenen Einrichtung oder des betroffenen Unternehmens Verantwortlicher und nicht die jeweils handelnde natürliche Person.

Entscheidungen zum Bußgeldverfahren

IDSG vom 16.7.2021 zur Zuständigkeit des IDSG im Bußgeldverfahren

Das Interdiözesane Datenschutzgericht ist für die Überprüfung von Bescheiden der Datenschutzaufsicht zuständig, die Geldbußen gemäß § 51 KDG verhängen.⁷

Entscheidungen zum gerichtlichen Verfahren nach der KDSGO

IDSG 09/2020 vom 02.02.2021

Wenn der Antragsteller die Antragsfrist des § 8 Abs. 2 Satz 1 KDSGO ohne Verschulden nicht eingehalten hat, kommt eine Wiedereinsetzung in den vorigen Stand entsprechend den Grundsätzen des § 60 Verwaltungsgerichtsordnung in Betracht.

C. Datenpannen

Im Vergleich zu meinem letztjährigen Bericht ergaben sich in diesem Bereich kaum Änderungen. Die Ursache der gemeldeten Datenpannen blieb völlig durchgehend Einzelfallversehen meist ungeübter Mitarbeiter. Nachforschungen nach unterlassenen Instruktionen oder zu hohem Druck auf die Beschäftigten blieben durchwegs ergebnislos.

Eine nennenswerte Änderung bestand darin, dass auch Auftragnehmer kirchlicher Dienststellen Angriffen von Hackern ausgesetzt waren, die auch bei den kirchlichen Behörden dann zu Datenproblemen führten. Im Gesamtergebnis hat sich aber das Sicherheitskonzept der kirchlichen Dienststellen bewährt, weil letztlich ein vollständiger Datenverlust nicht zu beklagen war. Das gilt auch für die sogenannten Erpresserviren, die im Berichtszeitraum für erhebliches Aufsehen sorgten.

Die verstärkte Arbeit der Beschäftigten von ihrem Privat PC aus („home office“) machte sich bei den Datenpannen überhaupt nicht bemerkbar. Keine einzige dieser Pannen war dadurch entstanden, dass Mitarbeiter während der Corona-Pandemie von zu Hause aus ihrer Beschäftigung nachgingen. Ich habe im Gespräch mit Kollegen und anderen Mitarbeitern versucht, die Gründe dafür zu finden. Ein ganz wesentlicher Gesichtspunkt scheint mir zu sein, dass der

⁷ Die Entscheidung begegnet erheblichen Bedenken: Das Verfahren bei Ordnungswidrigkeiten richtet sich nach dem OWiG, auch wenn eine Selbstverwaltungskörperschaft die Geldbuße verhängt hat (BVerfGE 5, 329/342). Das OWiG sieht aber eine Zuständigkeit der staatlichen Gerichte vor.

weitgehende Wegfall der Fahrt zum Arbeitsplatz zu entspannterem Arbeiten als sonst führte. Nicht unerheblich dürfte auch gewesen sein, dass die Ablenkung durch Gespräche mit Kollegen geringer war als sonst.

D. Beschwerden

In diesem Teilbereich setzte sich der schon in den letzten Jahren erkennbare Trend fort, dass Beschwerdeführer ihre eigentlich auf anderen Gebieten liegenden Ziele mit Datenschutzbeschwerden verfolgten, weil sie mit anderen Mitteln ihr Ziel nicht erreichen konnten. Mitunter entstand sogar der Eindruck, dass die Beschwerde dem Eingabeführer die Durchsetzung finanzieller Forderungen gegen die Dienststelle erleichtern sollte.

Die Zahl der Beschwerden ging gegenüber dem Vorjahr insgesamt um ca. 20 % zurück. Ihre Erfolgsquote wiederum liegt bei etwa 30 %. Bei den erfolgreichen Beschwerden zeigte sich, dass vor allem unterlassene oder verspätete Auskünfte vielfach das Beschwerdebegehren begründeten. Auf der anderen Seite ist zu vermerken, dass gerade keine grundlegenden Schwächen in der Organisation oder Struktur der Dienststellen zu begründeten Beschwerden führten. Meist waren es bloße Versehen, welche den Beschwerden ihren Erfolg bescherten.

E. Verfahren vor den kirchlichen Datenschutzgerichten

Mittlerweile sind nur noch drei der aus meinem Zuständigkeitsbereich stammenden Verfahren bei dem Interdiözesanen Datenschutzgericht anhängig.

F. Datenschutzfolgeabschätzungen

Seit Inkrafttreten des KDG kann sich der Verantwortliche einer Dienststelle – auch durch den jeweiligen betrieblichen Datenschutzbeauftragten gemäß § 35 Abs.3 an die Datenschutzaufsicht wenden und ihr den der Folgeabschätzung zu Grunde liegenden Sachverhalt zur Stellungnahme vorlegen. Diese Stellungnahme ersetzt nicht etwa die Folgeabschätzung, sondern bereitet sie nur vor. Angesichts der Besetzung meiner Dienststelle wäre auch nichts anderes machbar.

Trotz des daraus resultierenden Verzichts auf möglicherweise umfangreiche Ausführungen nach § 35 Abs.7 KDG gestaltet sich die Abarbeitung von Anfragen nach § 35 Abs.3 KDG vor allem bei Einführung neuer Programme keineswegs als einfach, wie der folgende Ablauf zeigt:

- Einholung der Information zum Ablauf (meist beim Hersteller bzw. auf dessen Webseite)
- Prüfung der Listen nach § 35 Abs. 6 KDG
- Prüfung auf Schwachstellen, vor allem aber
- Prüfung auf Drittlandbezug i. S. des EuGH-Urteils vom 16.7.2020 („Schrems II“)
- Bewertung der Risiken

- Gegenüberstellung der Vor- und Nachteile

In der Praxis arbeiten Herr Gleißner und ich diese Punkte jeweils selbständig durch und vergleichen danach unsere Ergebnisse, um möglichst sicher zu gehen.

Das Ergebnis wird auf der Webseite meiner Dienststelle veröffentlicht⁸. Dort findet sich auch eine Anleitung dafür, was bei Einführung neuer Software zu prüfen und zu geschehen ist⁹.

G. Die Auswirkungen der Corona-Pandemie auf die Tätigkeit der Datenschutzaufsicht

Auch in den letzten zwölf Monaten beeinträchtigte die Pandemie im Wesentlichen die Außenprüfung von Dienststellen. Wegen der erhöhten Ansteckungsgefahr war es immer noch nicht möglich, Außenprüfungen durch persönliche Kontrollen vorzunehmen. Deren Notwendigkeit wäre den zu prüfenden Dienststellen nicht vermittelbar gewesen. Deswegen musste sich Herr Gleißner darauf beschränken, unter Einschaltung der Datenschutzkoordinatoren in den Ordinariaten schriftliche Prüfungen vorzunehmen. Dabei erhalten die vom betrieblichen Datenschutzbeauftragten des Ordinariats benannten Einheiten einen mehrseitigen Fragebogen, den sie mit ihren Angaben füllen. Herr Gleißner arbeitet die Fragebögen durch und teilt mir die Ergebnisse mit. Schwachstellen erörtert er telefonisch mit den Datenschutzkoordinatoren und danach mit der Dienststelle.

Dieses Verfahren wird zwar von den übrigen Datenschutzaufsichten der (Erz-) Diözesen im Rest von Deutschland normalerweise immer durchgeführt, entspricht aber nicht meinen Zielvorstellungen. Ich halte den persönlichen Kontakt für besonders wichtig und auch effizient; Herr Gleißner nutzt deswegen seine Aufenthaltszeit bei den Dienststellen stets auch für Tipps zur EDV für die Dienststellen. Ab 4.10.2021 ist die Wiederaufnahme persönlicher Prüfungen wieder vorgesehen.

H. Corona-Pandemie, Homeoffice und mobiles Arbeiten

Die Corona-Pandemie hat die Digitalisierung in den kirchlichen Dienststellen seit März 2020 noch einmal kräftig vorangetrieben. Durch die zahlreichen Bayerischen Verordnungen zu Ausgangsbeschränkungen und Infektionsschutzmaßnahmen zur Vermeidung unnötiger Infektionsrisiken haben die Mitarbeiterinnen und Mitarbeiter in den kirchlichen Einrichtungen ihre dienstlichen Tätigkeiten bis heute ganz überwiegend aus dem Homeoffice heraus verrichtet. Ohne zeitlichen Vorlauf mussten dazu technische und organisatorische Maßnahmen durch die Ordinariate auf den Weg gebracht werden, um die Funktions- und Arbeitsfähigkeit der Dienststellen sicherzustellen. Dies stellte insbesondere die IT-Abteilungen vor größere Herausforderungen. Auch die leitenden betrieblichen Datenschutzbeauftragten und

⁸ <https://www.erzbistum-muenchen.de/cms-media/media-56259320.pdf> (bei Veröffentlichung, jetzt: Downloadbereich-Allgemeines-Folgeabschätzungen)

⁹ <https://www.erzbistum-muenchen.de/cms-media/media-36460820.pdf>

Informationssicherheitsbeauftragten waren besonders gefragt, ein möglichst gleichbleibendes Schutzniveau der Vertraulichkeit, Verfügbarkeit und Integrität von personenbezogenen Daten unter den besonderen Arbeitsbedingungen aufrechtzuerhalten.

Trotz der vielfältigen pandemischen Herausforderungen, gerade auch für die kirchlichen Schulen, die Seelsorge und die Übertragung von Gottesdiensten über Videostreaming, die Einführung neuer Messenger und zahlreiche neuer Videokonferenzsysteme musste ich in keinem Fall die Nutzung eines Dienstes unterbinden. Teilweise haben die Hersteller solcher Dienste eigenständig ihr Datenschutzniveau erhöht und damit ihren Service verbessert, andererseits erfolgte der Einsatz der Dienste ganz überwiegend nach besonders sorgfältiger Auswahl und nach internen Vereinbarungen zum Schutz der betroffenen Personen.

Folgende Empfehlungen habe ich den Dienststellen auf den Weg gegeben:

- Auf Dienste aus Drittstaaten, für die kein Angemessenheitsbeschluss besteht, sollte bestenfalls verzichtet werden. Andernfalls sind die technisch erforderlichen Anpassungsmaßnahmen für einen rechtskonformen Einsatz als besonders hoch anzusehen. Auf unentgeltliche Dienste sollte im Übrigen grundsätzlich verzichtet werden, da hier regelmäßig mit den personenbezogenen Daten in einer Ersatzwährung gezahlt wird.
- Verarbeitungstätigkeiten durch die Mitarbeitenden auch von außerhalb der kirchlichen Dienststellen sind datenschutzkonform möglich. Erforderlich dazu sind allgemeine organisatorische und technische Regelungen, die den Vorgaben des Kirchlichen Datenschutzgesetzes entsprechen und eine ausreichend sichere Verarbeitung gewährleisten, was auch nach § 7 Abs. 2 KDG durch die Verantwortlichen zu belegen ist.
- Insbesondere müssen heimische und mobile Bildschirmarbeitsplätze vor unbefugtem Zugang, wenigstens aber das IT-System vor unberechtigtem Zugriff geschützt sein. Vorzugswürdig ist die Einrichtung von verschlüsselten Remotezugriffen über ein virtuelles privates Netzwerk (VPN) auf die dienstlichen Informationen, um derart das lokale Speichern personenbezogener Daten zu vermeiden.
- Automatische Bildschirmsperren, Passwortschutz und die Festplattenverschlüsselung sind einzurichten. Das IT-System sollte nicht am Fenster im Erdgeschoss stehen, um unbefugten Einblicken oder gar dem Datendiebstahl bei offenen Fenstern vorzubeugen. Ausreichender Virenschutz und ein aktuelles Betriebssystem sind sicherzustellen, auch wenn es sich bei dem zu verwendenden IT-System um ein Privatgerät zu dienstlichen Nutzung handelt. Die Nutzung privater Geräte zu dienstlichen Zwecken ist nach § 20 KDG-DVO besonders zu begründen. Dienstliche und private Daten sind stets voneinander zu trennen, am besten durch unterschiedliche Laufwerke, Partitionen oder Benutzer-Accounts.
- Wo sich ein Arbeitsablauf außerhalb der Dienststellen nicht ohne Papierdokumente gestalten lässt, sollten die schriftlichen Unterlagen in einer Mappe oder einem abschließbaren Schrank gelagert werden und nur nach einer geeigneten Zerkleinerung sorgfältig entsorgt werden.
- Meine Kollegen aus den anderen Bundesländern und ich haben in der Konferenz der Diözesandatenschutzbeauftragten – wie auch die weltlichen Aufsichtsbehörden –

zahlreiche allgemeine und spezielle Informationen und Handreichungen veröffentlicht, um die Rechte und Freiheiten betroffener Personen bei der Datenverarbeitung im Homeoffice im Teleunterricht und bei mobilen Arbeiten sicherzustellen.

Wie sich im Berichtszeitraum zeigte, sind der Datenschutz und die Informationssicherheit kein Hindernis für die Digitalisierung, sondern stellen vielmehr den regulatorischen Gestaltungsrahmen dar, wie Datenverarbeitungen im Homeoffice, bei Teleunterricht und bei mobilen Arbeiten angemessen und sicher möglich sind.

Beanstandungen durch betroffene Personen oder meldepflichtige Datenpannen im Kontext von Homeoffice und mobilem Arbeiten kann ich für den Berichtszeitraum jedenfalls nicht feststellen.

I. Kontakt mit anderen kirchlichen Datenschutzaufsichten

Auch im Kontakt mit anderen Diözesandatenschutzbeauftragten oder mit den Kollegen von der EKD machte sich die Pandemie bemerkbar: Seit nun mehr als einem Jahr fanden Konferenzen ausschließlich per Videoschaltung statt. Verwendet wurden die im Hinblick auf die §§ 39ff KDG unbedenklichen Programmangebote von Big Blue Button, Bliss oder Teamviewer.

Konferenzen der Diözesandatenschutzbeauftragten fanden statt am

04.01.2021 (Zwischenkonferenz)
27.01.2021
23.03.2021 (Zwischenkonferenz)
22.04.2021
17.06.2021
06.07.2021 (Zwischenkonferenz)
15.09.2021

Die ökumenische Datenschutzkonferenz wurde am 22.04.2021 ebenfalls als Videokonferenz abgehalten. Der Unterfertigte nahm zusätzlich am 28.5.2021 an einer Informationsveranstaltung zum Thema „Drei Jahre kirchliches Datenschutzrecht“ teil.

J. Die Gemeinsame Datenschutzaufsicht der bayerischen (Erz-) Diözesen

besteht nach wie vor aus meinem Mitarbeiter, Herrn Stephan Gleißner, und mir. Unser gemeinsames Büro wurde im November 2020 wegen Bauarbeiten vom Ordinariatsgebäude München, Kapellenstr. 4 in ein anderes Gebäude des Ordinariats in der Schrammerstr. 3, München, verlegt, am 7.9.2021 wegen des Platzbedarfs einer anderen Abteilung innerhalb dieses Gebäudes in ein kleineres Zimmer.

Durch lediglich inoffizielle Hinweise erfuhr ich, dass die Aufstufung der Dienststelle zur Körperschaft des öffentlichen Rechts, die Erstellung einer Satzung für diese und die Ausschreibung meiner Stelle demnächst in Angriff genommen werden sollte, anschließend dann der

Umzug der Behörde nach Nürnberg. Meine Bestellung lief mit dem 30.9.2020 aus; gegenwärtig bin ich seit einem Jahr kommissarisch tätig.

Zur Klärung der Frage, welche kirchlichen Dienststellen ihrer Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten nachgekommen sind, setzte ich eine studentische Hilfskraft auch 2021 für etwa 16 Arbeitstage ein. Sie erstellte auch statistische Aufstellungen und prüfte stichprobenartig Webseiten von Kirchenstiftungen auf das Vorhandensein und die Vollständigkeit der notwendigen Datenschutzerklärungen.

Zuständigkeit:

Meine Zuständigkeit ergibt sich aus § 43 KDG. Sie umfasst nicht nur die verfasste Kirche, also die Bistümer und die Kirchengemeinden (einschließlich deren Einrichtungen, z.B. der Kindertagesstätten der Pfarreien), sondern auch ohne Rücksicht auf ihre Rechtsform alle Stellen und Einrichtungen der Caritas einschließlich z.B. der Jugendfürsorgevereine und Sozialdienste für Frauen und Männer und alle sonstigen kirchlichen Einrichtungen und Rechtsträger, insbesondere auch alle Ordensgemeinschaften bischöflichen Rechts einschließlich ihrer selbstständigen (z.B. Träger GmbH) oder nichtselbstständigen Stellen.

Ich habe mir erlaubt, dem Herrn Bischof von Speyer sowie den Hochwürdigsten Herren Generalvikaren je einen Abdruck dieses Berichts nachrichtlich zuzuleiten.

Mit dem Ausdruck meiner vorzüglichen Hochachtung

A handwritten signature in black ink, appearing to be 'Joachimski', written in a cursive style.

(Joachimski)
Diözesandatenschutzbeauftragter