

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 1.10.2022

Dieser Bericht schließt an denjenigen vom 1.10.2021 an.

A. Die Entwicklung des Datenschutzrechts seit 1.10.2021

I. Europäische Union

1. Gesetzgebung der EU

Ein weiteres Mal wurde die geplante Evaluierung der EU-DS-GVO zeitlich verschoben. Grund dafür war nicht allein die Pandemie, sondern auch der Krieg Russlands gegen die Ukraine, der vielfach Kräfte bindet.

Die europäischen Mitgliedstaaten haben sich am 10. Februar 2021 zum Schutz der Privatsphäre und der Vertraulichkeit bei der Nutzung elektronischer Kommunikationsdienste (e-Datenschutz/ ePrivacy) geeinigt. Mit diesen aktualisierten e-Datenschutzvorschriften wird festgelegt, in welchen Fällen Diensteanbieter elektronische Kommunikationsdaten verarbeiten oder Zugang zu Daten erhalten dürfen, die auf den Geräten der Endnutzer gespeichert sind. Die Verordnung soll die DS-GVO um konkrete Regelungen im Bereich der digitalen Datenverarbeitung ergänzen. Wann sie in Kraft treten kann, ist noch ungewiss.

2. Datenverkehr EU – USA

Schon in meinem Bericht vom 1.10.2020 hatte ich dargestellt, warum durch das Urteil des Europäischen Gerichtshofes vom 16.7.2020 („Schrems II“) der Datenverkehr mit den USA erheblich belastet wurde. Die Situation besteht auf Vertragsebene zwar fort; allerdings führte der Krieg Russlands gegen die Ukraine zu einer Verbesserung der Verständigung zwischen den USA und der EU. Die vorhandenen politischen Anzeichen deuten darauf hin, dass im Frühjahr 2023 eine vertragliche Regelung über den Datenschutz als Nachfolge des „privacy shields“ zustande kommen könnte¹. Auch wenn dieses künftige Vertragswerk unter dem Vorbehalt der Billigung durch den EuGH

¹ https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100

steht, kann doch davon ausgegangen werden, dass die Fehler aus früheren Jahren nicht wiederholt werden und hieraus eine stabile vertragliche Basis entsteht.

Vielfach wird ein Ausweg aus dem Dilemma in der Verwendung von Standardvertragsbedingungen gesehen. Leider ist dieser Ausweg bei dem Datenverkehr mit den Vereinigten Staaten nicht wirklich hilfreich, weil die Gesetzgebung der USA in dieser Beziehung sehr strikt durchgreift. Der seit 2018 geltende „Cloud Act“ erlaubt es den amerikanischen Sicherheitsbehörden, von Unternehmen des Landes auch dann die Herausgabe von Daten zu verlangen, wenn diese im Ausland gespeichert sind. Eine etwaige Unterbindung dieses Verlangens ist natürlich durch Standardvertragsklauseln schon deswegen nicht möglich, weil sie sich nicht gegen geltendes Recht auswirken können. Der einzig sinnvolle Ausweg zum jetzigen Zeitpunkt besteht darin, im Datenverkehr mit den USA lediglich anonymisierte oder pseudonymisierte Daten zu verwenden. Dies ist den beteiligten Unternehmen jedoch meistens zu umständlich.

Die Auswirkungen der Rechtslage auch auf normale Dienststellen sind ganz erheblich: Nahezu alle kirchlichen Dienststellen nutzen MS Office. Bei der Installation von MS Office wird automatisch auch MS ONE installiert, ein Datenspeicherprogramm, das wiederum meist ungefragt die Daten auf einen zentralen Speicher von Microsoft lädt. Dort sind sie – wie geschildert – dem Zugriff der amerikanischen Behörden ausgesetzt und zwar unabhängig davon, wo sich der Speicher geographisch befindet. Ich bin dazu übergegangen, Neuinstallationen von MS Office nur noch dann zu genehmigen, wenn mir vom betrieblichen Datenschutzbeauftragten unterschriftlich bestätigt wird, dass die Installation von MS ONE abgeschaltet wird. Weiterhin lege ich Wert darauf, dass keine namensbezogenen Benutzerkonten verwendet werden, sondern lediglich funktionsbezogene. Mittelfristig werde ich diese Installationsvoraussetzungen auch bei bereits durchgeführten Installationen verlangen. Entschärft hat sich lediglich im Bereich der kirchlichen Datenschutzaufsicht und der Datenschutzaufsichten der Länder das Problem der Verwendung von US-basierten Videokonferenzsystemen wie Zoom oder MS Teams wegen der Zuordnung dieser Programme zur Telekommunikation; insoweit nehme ich auf den nächsten Absatz Bezug.

II. Änderungen des deutschen Datenschutzrechts

Am 1. Dezember 2021 trat das „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ (auch „Telekommunikations-Telemediendatenschutzgesetz“, „TTDSG“) in Kraft, in welchem im Wesentlichen die Datenschutzvorschriften aus den früheren Fassungen des Telekommunikationsgesetzes („TKG“) und Telemediengesetzes („TMG“) kombiniert wurden. In Konsequenz aus diesem Gesetz muss die Zuständigkeit der Datenschutzaufsicht neu geprüft werden, sofern es um Anwendungen geht, bei denen die Kommunikation im Vordergrund steht, insbesondere die sog. „Videokonferenzprogramme“ wie Teams; Zoom, Teamviewer oder Big Blue Button. Hierzu steht die Landesbeauftragte für den Datenschutz NRW auf dem zutreffenden Standpunkt, dass sich die

Zulässigkeit der Anwendung dieser Programme ausschließlich aus dem TTDSG ergebe und dass deswegen der Bundesbeauftragte für den Datenschutz die zutreffende Aufsichtsbehörde sei².

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder beschloss am 29 April 2022, dass neben weiteren Maßnahmen ein eigenständiges Beschäftigtendatenschutzgesetz notwendig sei³. In diesem sollten Grenzen der Verhaltens- und Leistungskontrolle festgeschrieben werden und die Frage der Einwilligung im Arbeitsverhältnis gesetzlich geregelt werden. Rechtswidrig erlangte Beschäftigtendaten sollten einem Beweisverwertungsverbot unterliegen. Ein weiterer Beschluss vom 13. April 2022 betrifft die Verarbeitung personenbezogener Daten im Zusammenhang mit einrichtungsbezogenen Impfpflichten⁴.

III. Änderungen des kirchlichen Datenschutzrechts

Nach seinem § 58 Abs. 2 sollte 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 nach jetziger Prognose erst im Jahre 2023 vorliegen. Es gibt noch eine Reihe strittiger Punkte, über die zu beraten ist. Insgesamt ist es wohl vernünftiger, diesen Streitpunkten auf den Grund zu gehen als zur Vermeidung einer Verspätung der Evaluation schnelle Lösungen anzustreben.

Die in meinem letzten Bericht erwähnten Vorschriften der EKD zur Aufarbeitung sexuellen Missbrauchs durch Kirchenbedienstete hat mittlerweile auch die katholische Kirche für ihren Bereich ausformuliert⁵. Dies sollte für einen sehr schwierigen Aspekt des kirchlichen Datenschutzes Klarheit und Rechtssicherheit bringen.

B. Wichtige Gerichtsentscheidungen

In einem Rechtsstaat erfolgt die Rechtsetzung nicht allein durch Gesetze und Verordnungen, sondern auch durch Gerichtsentscheidungen. 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:

² <https://www.lidi.nrw.de/handreichung-zu-online-pruefungen-hochschulen>

³ Der Beschluss ist unter https://datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf abrufbar.

⁴ abrufbar unter https://datenschutzkonferenz-online.de/media/dskb/2022_13_04_beschluss_DSK_20a_IfSG.pdf

⁵ https://www.dbk.de/fileadmin/redaktion/diverse_downloads/dossiers_2021/2021-ORDNUNG-Verfahren-zur-Anerkennung-des-Leids.pdf

Entscheidungen zum materiellen Datenschutzrecht

25.04.2022 [IDSG 19/2021](#) (Rechtsmittel anhängig DSG-DBK 03/2022)

1. Wenn personenbezogene Daten lediglich in einer Gesprächssituation offengelegt werden, ist das KDG grundsätzlich nicht anwendbar.
2. Can. 220 CIC ist keine spezifische Datenschutznorm im Sinn von - neben dem KDG - "anderen Datenschutzvorschriften" gemäß § 48 Abs. 1 KDG.

25.02.2022 [IDSG 23/2020](#)

Zur praktischen Konkordanz zwischen dem Recht eines minderjährigen Jugendlichen auf informationelle Selbstbestimmung und dem Auskunftsrecht der Eltern.

21.02.2022 [IDSG 07/2019](#)

Zur Frage des Vorliegens personenbezogener Daten bei einem Homepage-Foto, das den PKW eines Mitarbeiters (Halbansicht ohne amtl. Kennzeichen) auf dem Parkplatz vor dem Dienstgebäude zeigt.

09.12.2021 [IDSG 03/2020](#) (Rechtsmittel anhängig DSG-DBK 02/2022⁶)

1. Die Angabe, Vorsitzender eines öffentlichen katholischen Vereins zu sein, gehört zu den besonderen Kategorien personenbezogener Daten gemäß § 4 Ziffer 2. Satz 1 KDG (Art. 9 Abs. 1 DSGVO).
2. Zu den Pflichten des Verantwortlichen gemäß § 11 Abs. 4 KDG bei der Verbreitung eines Visitationsberichts.

25.04.2022 [IDSG 10/2021](#)

Zur Aufbewahrungspflicht der Akte eines Verfahrensbeistands gemäß § 158 FamFG

LG München I, Urteil vom 20.1.2022 ZD 2022, 290

1. Wird bei Aufruf einer Webseite die dynamische IP-Adresse des Nutzers auf Grund der Nutzung von Google Fonts durch den Webseitenbetreiber automatisch an Google weitergeleitet, so stellt dies einen unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht dar.
2. Auf Grund des damit eintretenden Kontrollverlusts über die an Server von Google in den USA übermittelten Daten stellt dies jedenfalls einen erheblichen Eingriff dar, der Ansprüche auf immateriellen Schadensersatz begründet.

ÖDSB, Teilbescheid vom 22.12.2021 – D155.027, 2021-0.586.257 ZD 2022, 215

⁶ In dieser Sache ist vor dem Beschwerdegericht der DBK für den 298.10.2022 Termin zur mündlichen Verhandlung anberaumt.

Der Einsatz von Google Analytics auf einer Webseite eines Unternehmens ist nach dem Urteil des EuGH in der Rechtssache Schrems II nur auf Basis der mit Google (online) abgeschlossenen Standarddatenschutzklauseln ohne zusätzliche Maßnahmen nicht zulässig.

ÖBVwG, Erkenntnis vom 21.12.2021 ZD 2022, 439

Ruft ein Mitarbeiter personenbezogene Daten aus einer vom Arbeitgeber zur Verfügung gestellten Datenbank (hier: Melderegister) zu privaten Zwecken ab, ist er hinsichtlich dieser Datenverarbeitung selbst Verantwortlicher i. S. d. Artikel 4 Nummer 7 DS-GVO.

29.11.2021 [IDSG 04/2019](#)

Offener E-Mail-Verteiler und Kontextinformationen

26.11.2021 LG Siegen, (ZD 2022, 161)

1. Eine Patientin kann sich für ihren Datenauskunftsanspruch gegen eine als GmbH organisierte Klinik in Trägerschaft der Evangelischen Kirche nicht auf Art. 15 DS-GVO berufen, sondern nur auf § 19 DSGVO-EKD.
2. Aus dem gleichen Grund stehen der Patientin bei verweigerter Datenauskunftserteilung keine Schadensersatzansprüche gem. Artikel 82 Absatz 1 DS-GVO gegen die Klinik zu.

04.10.2021 OLG München (ZD 2022, 399)

1. Bei Schreiben oder Mails des Betroffenen an den Verantwortlichen handelt es sich ebenso um personenbezogene Daten wie bei Telefonnotizen, Aktenvermerken oder Protokollen als interne Vermerke des Antragsgegners, die Informationen über den Antragsteller enthalten.
2. Der Anspruch auf Überlassung von Kopien aus Art. 15 Abs. 3 DS-GVO besteht als eigenständiger Anspruch neben dem Auskunftsanspruch aus Art. 15 Abs. 1 DS-GVO.
3. Der Gegenstand dieses Anspruchs richtet sich nicht lediglich auf eine abstrakte Aufzählung der vorhandenen Informationen. Vielmehr umfasst der Anspruch die Überlassung der Informationen in der Form, wie sie dem Verantwortlichen vorliegen. Ein notwendiger Schutz des Anspruchsgegners wird durch die Möglichkeit der Schwärzung nach Art. 15 Abs. 4 DS-GVO gewährleistet.

27.09.2021 [IDSG 08/2021](#) (Rechtsmittel anhängig DSG-DBK 03/2021)

Zur Frage eines Datenschutzverstößes bei einer ordinariatsinternen Weitergabe eines an einen Ordinariatsrat gerichteten Schreibens.

16.09.2021 - [DSG-DBK 05/2020](#)

Bei einem Kirchenaustritt kann nicht gem. § 18 Absatz 1 Satz 1 KDG die Eintragung einer Ergänzung im Taufregister verlangt werden, wonach die betroffene Person aus der Katholischen Kirche als „Körperschaft des öffentlichen Rechts“ ausgetreten ist.

20.07.2021 OLG Düsseldorf (NJW-RR 2021, 1343)

Die Rechtfertigung der Verwendung von Fotos des Kindes in digitalen sozialen Medien gem. Art. 6 Abs. 1 Buchst. a DS-GVO erfordert die Einwilligung beider sorgeberechtigter Elternteile.

09.02.2021 – LG Karlsruhe (nicht rechtskräftig, ZD 2022, 55)

1. Der Verpflichtung zum Ausgleich eines immateriellen Schadens i.S.d. Art. EWG DSGVO Artikel 82 Abs. 1 DS-GVO muss eine benennbare und insoweit tatsächliche Persönlichkeitsverletzung gegenüberstehen, die z.B. in der mit einer unrechtmäßigen Zugänglichmachung von Daten liegenden „Bloßstellung“ liegen kann. Auch im Bereich des immateriellen Schadens kommt ein Anspruch nur dann in Betracht, wenn für den Betroffenen ein zwar immaterieller, aber dennoch spürbarer Nachteil entstanden ist; der Verstoß gegen Vorschriften der DS-GVO allein führt nicht unmittelbar zum Schadensersatz.

2. Über einen Bagatellschaden hinausgehende Schädigungen werden z.B. bei dem Verlust von Gesundheitsdaten, dem Verlust der Vertraulichkeit von anderen dem Berufsgeheimnis unterliegenden personenbezogenen Daten, dem Verlust von Daten mit sexuellem Bezug oder Daten, die gesellschaftlich kompromittierenden Inhalt haben, regelmäßig anzunehmen sein, nicht aber bei der Verbreitung von Name, Geburtsdatum, Geschlecht, E-Mail-Adresse und Telefonnummer einer Person. Ebenso enthalten Transaktionsdaten keine kompromittierenden Inhalte, die einen Anspruch auf Schmerzensgeld begründen könnten.

Entscheidungen zum Bereich der Datenschutzaufsicht:

VG Wiesbaden, Urteil vom 27.9.2021, ZD 2022,247

Ein Anspruch auf ermessensfehlerfreie Ausübung des Einschreitermessens der Datenschutzaufsichtsbehörde besteht, wenn die Datenverarbeitung rechtswidrig ist und die rechtswidrig gespeicherten Daten zu löschen sind.

Entscheidungen zum gerichtlichen Verfahren nach der KDSGO

31.12.2021 [IDSG 06/2019](#)

Zur Frage des Nachweises der Weitergabe personenbezogener Daten bei Bewerbungsverfahren.

08.03.2022 [IDSG 06/2021](#)

1. Zum Fehlen des Rechtsschutzbedürfnisses, wenn der Verantwortliche eine Datenschutzverletzung eingeräumt hat.
2. Zur mündlichen Weitergabe von Daten.

C. Datenpannen

Im Vergleich zu meinem letztjährigen Bericht ergaben sich in diesem Bereich insofern gravierende Änderungen, als kirchliche Dienststellen deutlich vermehrt Angriffen von Hackern ausgesetzt waren. Das gilt auch für die sogenannten Erpresserviren, die im Berichtszeitraum für erhebliches Aufsehen sorgten. Offensichtlich haben sich die Angreifer in jüngster Zeit auf gemeinnützige Organisationen konzentriert, weil der Aufwand zur Überwindung der Abwehrmaßnahmen in der freien Wirtschaft offensichtlich zu groß ist. Dabei sind ganz erhebliche Lösegelder geflossen, die zum Teil bis in den Millionenbereich gingen.

Es erscheint unverzichtbar, alle Beschäftigten in kurzen Abständen immer wieder darauf hinzuweisen, wie derartige Infektionen verhindert werden können. Regelmäßig werden nämlich die Erpresserviren über E-Mails und darin enthaltene Weblinks eingeschleust. Wenn es jedem Beschäftigten völlig klar wäre, dass er durch Anklicken eines solchen Links eine Gefahr für das gesamte System heraufbeschwört, könnten zahlreiche Schadensfälle vermieden werden.

Die verstärkte Arbeit der Beschäftigten von ihrem Privat PC aus („Mobiles Arbeiten“ oder „home office“) machte sich weiterhin bei den Datenpannen nicht wirklich bemerkbar. Keine einzige dieser Pannen war dadurch entstanden, dass Mitarbeiter während der Corona-Pandemie von zu Hause aus ihrer Beschäftigung nachgingen. Es entsteht der Eindruck, dass die entspanntere Arbeitssituation zu Hause auch für einen entspannteren Umgang mit der EDV sorgt.

Auch im Berichtszeitraum konzentrierte sich die weit überwiegende Mehrzahl der Datenpannen auf Flüchtigkeitsfehler von Mitarbeitern. Das nach § 51 Abs. 1 KDG geforderte Verschulden der Einrichtungs- oder Dienststellenleitung ließ sich in keinem Fall nachweisen. Schon aus diesem Grund unterblieben im Hinblick auf derartige Fälle Bußgeldverfahren. Anders als das Interdiözesane Datenschutzgericht⁷ stehe ich auf dem Standpunkt, dass das Funktionsträgerprinzip wegen seines Verstoßes gegen § 30 OWiG im Bereich des KDG nicht anwendbar ist. Ich sehe keinen Anlass, eine Geldbuße in Fällen zu verhängen, in denen es u. U. später zu einer Aufhebung wegen einer anderslautenden Entscheidung des Europäischen Gerichtshofs kommen kann. Das Berliner Kammergericht hat nämlich diese Frage dem EuGH zur Vorabentscheidung vorgelegt⁸.

Das Interdiözesane Datenschutzgericht setzt sich auch nicht mit der Unterschiedlichkeit der Regelungen in der EU-DS-GVO und dem KDG auseinander. Nach der Datenschutz-Grundverordnung, deren analoge Anwendung letztlich von dem zitierten Beschluss gefordert wird, ist das Funktionsträgerprinzip jedenfalls nicht ausgeschlossen. Die Vorlagefrage des Kammergerichts beschränkt sich darauf, die Anwendbarkeit des Funktionsträgerprinzips auf das deutsche Recht trotz der Existenz von § 30 OWiG zu prüfen. § 51 KDG verlangt jedoch in seinem Abs. 1 ausdrücklich ein Verschulden des Verantwortlichen, nicht nur dasjenige eines Mitarbeiters. Selbst wenn also der EuGH die Vorlagefrage bejahen würde, wäre damit über die

⁷ https://www.dbk.de/fileadmin/user_upload/Beschluss-IDSG-21-2020_vom_16.07.2021_anonym.Fas_geschw%C3%A4rzt.pdf

⁸ BeckEuRS 2021, 750343

Anwendbarkeit des Funktionsträgerprinzips trotz des Vorhandenseins von § 51 Abs.1 KDG nichts festgelegt.

Das Problem könnte sich noch als größer darstellen, wenn man der Meinung eines Teils meiner Kollegen folgt: Sie sind der Ansicht, dass kirchliche Kindergärten am Wettbewerb teilnehmen und dass deswegen § 51 Abs. 6 KDG – Verbot der Verhängung von Geldbußen gegen öffentlich-rechtlich verfasste Dienststellen – nicht greifen könne. Damit würden im Ergebnis die Kirchenstiftungen, die ihrerseits öffentlich-rechtlich verfasst sind, für die Geldbußen der Kindergärten haften, weil diese am Wettbewerb teilnehmen. Die Kindergärten aber verursachen einen recht beachtlichen Anteil an den Datenpannen. Ich vertrete diese Ansicht auch deswegen nicht, weil amtsbekannt gerade bei Kindergärten nicht wirklich ein Wettbewerb stattfindet, sondern die Eltern der zu betreuenden Kinder für ihre Auswahl die der Wohnung näher liegenden Einrichtungen bevorzugen. Kinderbetreuungseinrichtungen sind auch Teil der Daseinsvorsorge und gemäß Art. 6 Abs.2 KiBiG Inhalt des Planungsverfahrens nach § 80 SGB VIII.

D. Beschwerden

In diesem Teilbereich setzte sich wie schon in den letzten Jahren der Trend fort, dass Beschwerdeführer ihre eigentlich auf anderen Gebieten liegenden Ziele mit Datenschutzbeschwerden verfolgten, weil sie mit den eigentlich statthaften Rechtsbehelfen ihr Ziel nicht erreichen konnten.

Die Zahl der Beschwerden ging gegenüber dem Vorjahr insgesamt noch einmal um ca. 20 % zurück. Ihre Erfolgsquote wiederum liegt bei etwa 30 %. Bei den erfolgreichen Beschwerden zeigte sich, dass vor allem unterlassene oder verspätete Auskünfte sehr oft 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. Anhängige Verfahren vor den kirchlichen Datenschutzgerichten

Gegenwärtig sind nur noch zwei der aus meinem Zuständigkeitsbereich stammenden Verfahren bei dem Interdiözesanen Datenschutzgericht anhängig. In einem weiteren Fall habe ich mich einer Beschwerde des Verantwortlichen gegen die Entscheidung des BDSG angeschlossen. Das Verfahren ist momentan beim Datenschutzgericht der DBK anhängig.

F. Soziale Medien

Die unter B erwähnten Entscheidungen der österreichischen Datenschutzaufsicht waren für die Datenschutzkonferenz des Bundes und der Länder Veranlassung, sich erneut mit der Verwendung von Facebook-Fanpages zu befassen.

Ein von der Deutschen Datenschutzkonferenz in Auftrag gegebenes Gutachten zur Rechtmäßigkeit der Verwendung von **Facebook-Fanpages** kam zu folgendem Ergebnis:

Für die bei Besuch einer Fanpage ausgelöste Speicherung von Informationen in den Endeinrichtungen der Endnutzer und den Zugriff auf Informationen, die bereits in der Endeinrichtungen gespeichert sind, sowie für die Verarbeitungen personenbezogener Daten, die von Seitenbetreibern verantwortet werden, sind keine wirksamen Rechtsgrundlagen gegeben. Darüber hinaus werden die Informationspflichten aus Art. 13 DSGVO nicht erfüllt.⁹

Die EKD erließ hierzu eine eigene Verlautbarung¹⁰. Am 3.6.2022 ordnete der BfDI eine Anhörung der Bundesbehörden zu dem Thema an¹¹.

Die künftige Entwicklung hinsichtlich der sozialen Medien und insbesondere hinsichtlich Facebook lässt sich derzeit noch nicht absehen. Es kann sein, dass sich durch den Nutzerrückgang und den Druck der Datenschützer die Geschäftspolitik von Facebook ändert und mehr Datenschutzoptionen integriert. Das bisherige Verhalten der Geschäftsleitung von Facebook lässt allerdings nicht auf eine hohe Wahrscheinlichkeit dieser Variante schließen. Deswegen sollte die zweite Variante, dass Facebook die europäischen Märkte aus Datenschutzgründen völlig verliert, nicht von vornherein ausgeschlossen werden.

Was für Facebook gilt, ist prinzipiell auch auf die anderen sozialen Medien anwendbar, wenn auch häufig nicht in der Klarheit und Rigorosität. Es wird zwar nicht so viel darüber verlautbart, doch erscheint es durchaus naheliegend, dass Tiktok und Twitter ähnliche Datenschutzfragen aufwerfen wie Facebook.

G. 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.

In der Praxis arbeiten Herr Gleißner und ich diese Punkte jeweils selbständig durch und vergleichen danach unsere Ergebnisse, um möglichst sicher zu gehen. Das gemeinsame Ergebnis wird auf der Webseite meiner Dienststelle veröffentlicht¹². Dort findet sich auch eine Anleitung dafür, was bei Einführung neuer Software zu prüfen ist und wie zu verfahren ist.¹³

⁹ https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/103DSK-Kurzgutachten-Facebook.pdf?__blob=publicationFile&v=3 S.20

¹⁰ https://datenschutz.ekd.de/wp-content/uploads/2022/05/Entschliessung_Facebook-Fanpages.pdf

¹¹ https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2022/07_Anhoerung-BPA.html

¹² <https://www.erzbistum-muenchen.de/cms-media/media-56259320.pdf>

¹³ <https://www.erzbistum-muenchen.de/cms-media/media-36460820.pdf>

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

Entgegen den Erwartungen Mitte 2021 ließen sich die Vor-Ort-Prüfungen wegen der Entwicklung der Pandemie nicht wieder zum 1.10.2021 aufnehmen. Gerade auch wegen der Mutation des Virus lag eine erhöhte Ansteckungsgefahr im Berichtszeitraum vor. Sie machte persönliche Besuche von Herrn Gleißner in den Dienststellen zu einem nicht hinnehmbaren Risiko für ihn und die Beschäftigten der jeweiligen Dienststellen. Nur in einem Beschwerdefall waren vor Ort persönliche Ermittlungen und Befragungen durchzuführen, die Herr Gleißner unter Zuhilfenahme der üblichen Vorsichtsmaßnahmen absolvierte.

Im Übrigen versandte Herr Gleißner Fragebögen, die auf die jeweilige Dienststellenart zugeschnitten sind, an die Dienststellen. Diese wurden ihm vom Datenschutzkoordinator des zuständigen (Erz-) Bistums nach von ihm bezeichneten Kriterien benannt. Gerade bei dieser Gelegenheit zeigen sich wieder die Vorzüge des in Bayern mittlerweile überwiegend eingeführten Systems „Leitender Betrieblicher Datenschutzbeauftragter“¹⁴.

I. Kontakt mit anderen Datenschutzaufsichten

Die nachlassenden Inzidenzwerte von Covid-19 ermöglichten immerhin drei persönliche Konferenzen der Diözesandatenschutzbeauftragten, eine weitere wurde als Videokonferenz durchgeführt.

Konferenzen der Diözesandatenschutzbeauftragten fanden statt am

10.11.2021	5. Konferenz 2021 München – persönlich, zweitägig
27.01.2022	1. Konferenz (Videokonferenz)
27.04.2021	Ökumenischer Datenschutztag Berlin – persönlich
28.04.2022	2. Konferenz Berlin - persönlich
15.06.2022	3. Konferenz (Videokonferenz)
14./15.09.2021	4. Konferenz Dachau – persönlich, zweitägig

In der Konferenz vom 14./15.9.2022 hielt der Bayerische Landesbeauftragte für den Datenschutz, Prof. Dr. Petri, einen Vortrag zum Thema „Was erwarten die staatlichen Datenschutzaufsichten von den kirchlichen?“ und stand anschließend zu einer Aussprache auch über andere Datenschutzfragen zur Verfügung.

Die Beschlüsse der Konferenz deutscher Diözesandatenschutzbeauftragter sind auf der Webseite der Gemeinsamen Datenschutzaufsicht veröffentlicht¹⁵.

¹⁴ vgl. unter J2

¹⁵ <https://www.erzbistum-muenchen.de/ordinariat/datenschutzstelle/konferenz-der-dioezesandatenschutzbeauftragten/90605>

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

besteht nun seit 1978. Sie war zunächst bis 2003 sowohl für die Organisation des Datenschutzes als auch für die Überwachung berufen. Seit der KDO 2003, mit welcher der „betriebliche Datenschutzbeauftragte“ eingeführt wurde, ergab sich eine Umverteilung der Aufgaben hin zur reinen Aufsicht. Sie ist auch so im KDG verankert.

1. Zuständigkeit:

Die 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.

2. Abgrenzung zu den betrieblichen Datenschutzbeauftragten

Eine Arbeitsgruppe kirchlicher Juristen, der ich auch angehörte, schlug 2018 für den Bereich der bayerischen (Erz-) Diözesen eine gegenüber dem Rest von Deutschland etwas veränderte Struktur der Zuständigkeit von betrieblichen Datenschutzbeauftragten (§ 36 KDG) vor. Es sollte für jede (Erz-) Diözese eine Person geben, die für ihren gesamten Zuständigkeitsbereich die notwendigen Organisationstätigkeiten außerhalb der Aufsicht übernehmen sollte. Sie sollte also z.B. die Fortbildung der Mitarbeiter, die Einzelfallberatung und das Vorhalten von Mustern und Formblätter organisieren. Die im Hinblick auf den Datenschutz eher kritischen Stellen ihres Zuständigkeitsbereichs sind diesen Mitarbeitern oder auch externen Beauftragten naturgemäß besser geläufig als der räumlich meist weit entfernten gemeinsamen Datenschutzaufsicht; dies sorgt für eine bessere Erfüllung der Datenschutzerfordernungen. Eine Verankerung der Position im KDG erschien zu Recht deswegen als unnötig, weil die Amtsinhaber – „Leitende Betriebliche Datenschutzbeauftragte“ oder „Datenschutzkoordinatoren“ – nur verwaltungsinterne Funktionen haben. Diese Personen sind auf meiner Webseite namentlich aufgeführt¹⁶.

(Joachimski)

Diözesandatenschutzbeauftragter

¹⁶ <https://www.erzbistum-muenchen.de/ordinariat/datenschutzstelle/leitende-betriebliche-dsb/90602>