Gemeinsame Ordensdatenschutzbeauftragte der DOK (GDSB)

Deutsche Ordensobernkonferenz
Wittelsbacherring 9, 53115 Bonn
01.Februar 2025

An die Höheren Oberinnen und Oberen,
die an der Einrichtung des Gemeinsamen
Ordensdatenschutzbeauftragten der DOK
teilnehmen

Bericht der Ordensdatenschutzbeauftragten; Zeitraum 1.2.2024 - 31.1.2025

Sehr geehrte Damen und Herren,

nach § 44 Abs. 6 der Kirchlichen Datenschutzregelung für Ordensgemeinschaften (KDR-OG) haben wir jährlich einen Bericht zu erstellen, der auch der Öffentlichkeit zugänglich gemacht wird.

Die allgemeine Situation in Deutschland während des Berichtszeitraums war gekennzeichnet durch Meinungsverschiedenheiten zwischen den die Bundesregierung tragenden Parteien und durch den Bruch der Koalition im November 2024. Diese Ausgangslage ließ zwar manche Datenschutzfragen in Deutschland eher in den Hintergrund treten, doch hatten Maßnahmen der Europäischen Union und vorher bereits eingeleitete Gesetzesänderungen in sehr großem Umfang erste Auswirkungen in der Praxis.

1. Entwicklung des Datenschutzrechts

a. Die Europäische Kommission hatte schon im Dezember 2022 die sog. NIS-Richtlinie (Network and Information Security) 2016/1148, bekannt als NIS1, durch die Richtlinie 2022/2555 – NIS2 – ersetzt. „*NIS2 erhöht das gemeinsame Ambitionsniveau der EU im Bereich der Cybersicherheit durch einen breiteren Anwendungsbereich, klarere Vorschriften und stärkere Aufsichtsinstrumente. Sie verpflichtet die Mitgliedstaaten, ihre Cybersicherheitskapazitäten zu verbessern und gleichzeitig Risikomanagementmaßnahmen und Berichtspflichten für Einrichtungen aus mehr Sektoren einzuführen und Vorschriften für die Zusammenarbeit, den Informationsaustausch, die Beaufsichtigung und die Durchsetzung von Cybersicherheitsmaßnahmen festzulegen.*[1]“

   Die Richtlinie verpflichtet die Mitgliedstaaten, bis 17.10.2024 ihre Vorgaben in nationales Recht umzusetzen, was zum großen Teil noch nicht geschehen ist. Sie befasst sich in erster

[1] Begründung der Kommission unter https://digital-strategy.ec.europa.eu/de/policies/nis2-directive

Linie mit den Auswirkungen der Künstlichen Intelligenz, hat aber auch Auswirkungen auf das Datenschutzrecht. Aus der Begründung der EU-Kommission:

Zusätzlich zu den Sektoren, die bereits unter NIS 1 fallen, wie Energie, Verkehr, Gesundheitswesen, Finanzen, Wasserwirtschaft und digitale Infrastruktur, gelten diese Vorschriften für Anbieter öffentlicher elektronischer Kommunikationsdienste, mehr digitale Dienste wie soziale Plattformen, Abwasser- und Abfallbewirtschaftung, Herstellung kritischer Produkte, Post- und Kurierdienste, öffentliche Verwaltung sowohl auf zentraler als auch auf regionaler Ebene oder im Weltraum. In der Regel müssen mittlere und große Einrichtungen in diesen kritischen Sektoren geeignete Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen und die zuständigen nationalen Behörden über erhebliche Sicherheitsvorfälle informieren. Dabei handelt es sich um Vorfälle, die erhebliche Störungen oder Schäden verursachen können.

In der rechtlichen Entwicklung des staatlichen Datenschutzes gab es kaum nennenswerte Fortschritte. Wie im Vorjahr wurde die ursprünglich für 2018 angekündigte E-Privacy-Verordnung der EU immer noch nicht rechtswirksam erlassen. Sie soll im Schwerpunkt die Vertraulichkeit der Kommunikation (Fernmeldegeheimnis), die Verarbeitung von Kommunikationsdaten (bisher Verkehrsdaten) und das Speichern und Auslesen von Informationen auf Endeinrichtungen (z.B. Cookies) regeln. Darüber hinaus soll sie dem besseren Schutz der Privatsphäre im Zusammenhang mit der Anzeige von Rufnummern und Endnutzerverzeichnissen dienen, weiterhin die Direktwerbung mittels elektronischer Kommunikation und die Aufsicht regeln. Ziel der Verordnung ist es, die Regeln zur elektronischen Kommunikation an die DSGVO anzunähern, ohne dabei über deren Vorschriften hinauszugehen.

Die Europäische Kommission hatte zwar für das zweite Quartal 2023 eine Gesetzesinitiative zur Änderung der DSGVO in Aussicht gestellt[2], dieses Vorhaben wurde aber bis 31.1.2025 nicht verwirklicht.

b. Der Abschluss der für 2021 vorgesehenen Evaluierung des Kirchlichen Datenschutzgesetzes von 2018 (KDG) verzögert sich weiterhin. Nach dem gegenwärtigen Stand ist wohl noch im Jahre 2025 mit dem Abschluss zu rechnen. Er wird eine Reihe von Anpassungen des KDG beziehungsweise der KDR-OG mit sich bringen. Die Anpassungen beruhen auf gesetzlichen Änderungen wie zum Beispiel dem BDSG oder tragen den praktischen Erfahrungen Rechnung. Es liegt jedoch zum Berichtszeitpunkt immer noch kein abgestimmter Vorschlag für eine neue Regelung vor.

   Die durchaus wünschenswerte Eingliederung der KDR-OG in das KDG ist bisher auch nicht realisiert. Deswegen ist davon auszugehen, dass auch künftig für die Bereiche der verfassten Kirche und der Ordensgemeinschaften päpstlichen Rechts zwar inhaltlich gleiche, aber unterschiedlich bezeichnete Normen gelten werden. Soweit Änderungen des KDG als Ergebnis der Evaluierung erfolgen sollten, werden sie in den KDR-OG-Entwurf übernommen, soweit sie nicht speziell für die verfasste Kirche gelten sollen.

2. Auswirkungen äußerer Umstände auf die Datenschutzaufsichten

a) Die Beschwerdeeingänge nahmen im Berichtszeitraum leicht ab.

b) Zu beobachten war weiterhin eine stetige Zunahme von Datenpannen, mehr und mehr ausgelöst durch Einschleusen von Computerviren und daraus folgendem Zusammenbruch des EDV-Systems und weniger durch Fehler der Anwender z.B. bei der Adressierung von E-Mails.

[2] https://www.dr-datenschutz.de/diese-dsgvo-aenderungen-plant-die-eu-kommission/

In dieser Hinsicht war natürlich Beratung gefordert. Es wird aber auch in der nahen Zukunft erforderlich sein, alle Beteiligten – gerade auch die mit der IT wenig vertrauten – auf die Gefahren dieser Angriffe hinzuweisen und vorausschauendes, vorsichtiges Handeln immer wieder einzuüben. Das lässt sich allerdings weniger gut in großen Fortbildungsveranstaltungen erreichen. Günstiger erscheint es, solche Hinweise bei den nunmehr wieder möglichen persönlichen Besuchen der Prüfungsbeauftragten (s. unter c) in einer sich an die Prüfung anschließenden Unterrichtsstunde für alle Mitarbeiter zu geben.

c) Die beiden im Außendienst tätigen Mitarbeiter Penot und Gleißner hatten im Frühjahr 2023 bereits die zeitliche Struktur ihrer Prüfungstätigkeit festgelegt und begannen im Sommer 2024 wieder damit, die Ordensgemeinschaften persönlich aufzusuchen. Beide Mitarbeiter vermeiden eine Heraushebung ihrer Aufsichtsstellung und haben stets die Hilfestellung im Vordergrund. Sie wollen ihre Erfahrung nutzen, nicht um zu kritisieren, sondern um zu zeigen, wie die rechtlichen Anforderungen besser zu bewältigen sind. Daraus ergibt sich häufig auch eine kleine Hilfestellung bei der Bewältigung von EDV-Problemen.

   Die Aufsichtsgruppe prüfte persönlich im August 2024 zwei Ordenskrankenhäuser, was naturgemäß mit größerem Zeitaufwand verbunden war. Im Januar 2025 fanden dann Prüfungen zweier Ordensverwaltungen statt.

   Das Ergebnis aller Prüfungen ist insgesamt sehr positiv. Wie schon vielfach festgestellt, sind Ordensmitglieder den Datenschutzbelangen gegenüber regelmäßig aufgeschlossen, was sicher damit zusammenhängt, dass ihnen der Persönlichkeitsschutz wichtig ist. Soweit betriebliche Datenschutzbeauftragte bestellt sind, zeigen sie Interesse, Engagement und gute Kenntnisse. Sie scheuen auch nicht die Einarbeitung in schwierige Probleme.

3. Fortsetzung: Probleme im Datenverkehr mit den USA

In früheren Berichten sind wir unter anderem auf das Urteil des EuGH vom 16.7.2020 („Schrems II“) und seine Folgen für den Datenverkehr mit den USA eingegangen. Am 10.7.2023 kam es zu einem Angemessenheitsbeschluss der EU-Kommission für den Datenverkehr mit den USA[3], der einen Großteil der Probleme zunächst beheben sollte. Dazu gibt es Anwendungshinweise der DSK[4].

*Die Prüfung der Zulässigkeit des Datenverkehrs mit den USA beginnt mit der Teilnehmerabfrage[5]. Ist der von der jeweiligen Ordensgemeinschaft gewählte Partner in der Liste enthalten, dann wird der Datenverkehr rechtmäßig nach § 40 Abs.1 KDR-OG. Auf Beschäftigtendaten bezieht sich die Rechtfertigung aber nur, wenn unter „covered data“ auch „**HR** “ steht.*

Auf diese Weise kann bis zu einer etwaigen Änderung der Rechtslage ein legaler Datenverkehr mit den USA abgewickelt werden. Nach den Erfahrungen in der Vergangenheit könnte sich eine solche Änderung durch eine neuerliche Entscheidung des EuGH oder eine Umwälzung in den Vertragsbeziehungen zwischen den USA und der EU ergeben. Die erste Alternative ist nicht völlig unwahrscheinlich, weil auch der neue Angemessenheitsbeschluss der EU-Kommission schon jetzt einer Klage ausgesetzt ist. Eine mögliche Änderung in den Vertragsbeziehungen könnte darauf beruhen, dass z.B. das EU-U.S. „Data Privacy Framework“ gekündigt wird.

---

[3] https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2023/17_Angemessenheitsbeschluss-EU-US-DPF.html
[4] https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf
[5] http://www.dataprivacyframework.gov/s/participant-search

Für derartige Fälle sollten die Ordensgemeinschaften Vorsorge treffen. Ein wesentlicher Gesichtspunkt ist dabei, nur Cloudanwendungen europäischer Provider für die Datenspeicherung zu wählen, da sonst im Zeitpunkt der Änderung ein kompletter Datenumzug nötig wird. Diese Frage ist auch jetzt – ohne Eintritt einer Rechtsänderung – schon zu beachten, sofern Microsoft 365 Anwendung findet. Gegen den Einsatz bestehen trotz des Angemessenheitsbeschlusses verbleibende datenschutzrechtliche Bedenken der EU[6]. Zwar wird vielfach ein datenschutzkonformer Einsatz für möglich gehalten, doch erfordert er intensive Maßnahmen der Sicherung, z. B. die Abschaltung von MS Onedrive. Sollte der Rechtsgrund für den Angemessenheitsbeschluss ganz wegfallen, gerät jeder Datenverkehr mit den USA in die Zone der Unzulässigkeit. Ein bisschen Vorsorge für diesen Fall wäre es z.B. schon, im eigenen IT-Bereich völlig auf namensgebundene E-Mail-Adressen zu verzichten, da mit ihnen schon personenbezogene Daten in ein Drittland übertragen werden. Erheblich besser sind unter diesem Gesichtspunkt reine Funktionsadressen wie z.B. oekonom@beispielorden.de.

4. Meldeportal – Meldestelle nach dem Hinweisgeber-Schutzgesetz

Es war in der Vergangenheit immer störend, dass Ordensgemeinschaften päpstlichen Rechts Meldungen über Datenpannen gemäß § 33 KDR-OG nur über die Datenbank der deutschen Diözesandatenschutzbeauftragten abgeben konnten und dabei für die Ermittlung der Aufsichtszuständigkeit die Diözese benennen mussten, der sie angehörten. Dies führte zu Zeitverszögerungen, die vermieden hätten werden können. Im Zuge der Neugestaltung der Webseite für den Ordensdatenschutz wurde im Sommer 2024 eine Meldeplattform[7] hinzugefügt, die Meldungen wegen Datenschutzverletzungen, Hinweise auf sexuellen Missbrauch und solche nach dem Gesetz zum besseren Schutz von Hinweisgebern weiterleitet.

Seit Anfang 2024 bietet nämlich die DOK ihren Mitgliedern an, sich für Meldungen nach dem Hinweisgeberschutzgesetz entweder

- der von ihr eingerichteten gemeinsamen Meldestelle (bei Ordensgemeinschaften mit bis zu 249 Beschäftigten) oder
- der speziellen Meldestelle für größere Gemeinschaften zu bedienen.

Die Beitragshöhe berücksichtigt den Umstand, dass Ordensgemeinschaften in der Regel keine erheblichen Gewinne haben oder anstreben. Verantwortlicher der Meldungsseiten ist der Unterfertigte Joachimski.

5. Einige wichtige Gerichtsentscheidungen

Die kirchlichen Gerichte in Datenschutzsachen sind auch für Verfahren zuständig, in denen Ordensgemeinschaften betroffen sind. Die von ihnen und auch die von den staatlichen Gerichten vorgenommene Gesetzesauslegung betrifft direkt die Gesetzesanwendung. Soweit hier das KDG zitiert wird, entsprechen die zitierten Vorschriften voll und ganz denjenigen der KDR-OG, soweit die EU-DSGVO zitiert wird, haben wir die entsprechenden KDR-OG-Vorschrift in Kammern hinzugefügt.

---

[6] https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf vgl. auch https://www.kuketz-blog.de/kommentar-eu-und-microsoft-365-alternativlosigkeit-als-bequeme-ausrede/

[7] https://meldeplattform.orden.de/

a. **EuGH, Urteil vom 26.10.2023 – C-307/22 - ZD 2024, 22**
Artikel 12 und 15 EU- DS-GVO (§§ 14 und 17 KDR-OG) sind dahin auszulegen, dass die Verpflichtung des Verantwortlichen, der betroffenen Person unentgeltlich eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, zur Verfügung zu stellen, auch dann gilt, wenn der betreffende Antrag mit einem anderen als den in Erwägungsgrund EU-DSGVO 1 Nummer 63 S. 1 DS-GVO genannten Zwecken begründet wird.

b. Datenschutzgericht der DBK vom 09.11.2023 - DSG-DBK 07/2022[8]

I. Ebenso wie von der Löschung personenbezogener Daten geht auch von der Nichterhebung personenbezogener Daten keine Verletzung aus. Das Recht auf informationelle Selbstbestimmung, dessen Schutz das Datenschutzrecht nach § 1 KDR-OG dient, kann durch eine Nichterhebung von personenbezogenen Daten nicht verletzt sein, weil es bereits an einer Verletzungshandlung fehlt.

II. Die Norm des § 35 KDR-OG stellt auch mit Blick auf den Schutzzweck des Gesetzes (§ 1 KDR-OG) keine Schutznorm dar, die Einzelnen ein subjektives Recht auf die Durchführung einer derartigen Folgenabschätzung vermittelt.

c. EuGH, Urteil vom 5.12.2023 – C80/21 - NJW 2024,343

I. Art. 58 DSGVO Absatz II Buchst. i und Art. 83 DSGVO Absatz I – VI VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (EU-DS-GVO entspricht § 51 KDR-OG) sind dahin auszulegen, dass sie einer nationalen Regelung entgegenstehen, wonach eine Geldbuße wegen eines in Art. 83 Absatz IV – VI DS-GVO genannten Verstoßes gegen eine juristische Person in ihrer Eigenschaft als Verantwortliche nur dann verhängt werden kann, wenn dieser Verstoß zuvor einer identifizierten natürlichen Person zugerechnet wurde.

II. Art. 83 VO (EU) 2016/679 ist dahin auszulegen, dass nach dieser Bestimmung eine Geldbuße nur dann verhängt werden darf, wenn nachgewiesen ist, dass der Verantwortliche, der eine juristische Person und zugleich ein Unternehmen ist, einen in Art. 83 DSGVO Absatz IV– VI genannten Verstoß vorsätzlich oder fahrlässig begangen hat.

d. **EuGH, Urteil vom 5.12.2023 – C-683/21 - ZD 2024,209**
Art. 4 Nr. 7 DS-GVO (§ 4 Nr. 9 KDR-OG) ist dahin auszulegen, dass eine Einrichtung, die ein Unternehmen mit der Entwicklung einer mobilen IT-Anwendung beauftragt und in diesem Zusammenhang an der Entscheidung über die Zwecke und Mittel der über die Anwendung vorgenommenen Verarbeitung personenbezogener Daten mitgewirkt hat, als Verantwortlicher im Sinne dieser Bestimmung angesehen werden kann, auch wenn sie selbst keine personenbezogene Daten betreffenden Verarbeitungsvorgänge durchgeführt, keine ausdrückliche Einwilligung zur Durchführung der konkreten Verarbeitungsvorgänge oder zur Bereitstellung dieser mobilen Anwendung für die Öffentlichkeit gegeben und die mobile Anwendung nicht erworben hat, es sei denn, sie hat, bevor die Anwendung der Öffentlichkeit bereitgestellt wurde, dieser Bereitstellung und der sich daraus ergebenden Verarbeitung personenbezogener Daten ausdrücklich widersprochen.

[8] Entscheidungssammlungen: https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/

e. **OLG Köln, Urteil vom 7.12.2023 – 15 U 108/23 - ZD 2024, 240**
Der Verlust der Kontrolle über personenbezogene Daten ist lediglich die „negative Folge“ eines Datenschutzverstoßes, nicht aber für sich genommen bereits ein immaterieller Schaden. Es müssen stets darüberhinausgehende Auswirkungen auf die Person oder die Lebensumstände des Betroffenen vorliegen. Diese Frage kann nur im Einzelfall und nur unter Berücksichtigung der Art des konkreten personenbezogenen Datums beantwortet werden.

f. **KG, Beschluss vom 22.1.2024 – 3 Ws 250/21 – ZD 2024, 585**
Geldbußen nach Art. 83 EU-DSGVO (§ 51 KDR-OG) können unmittelbar gegen juristische Personen verhängt werden, wenn diese als für die betreffende Verarbeitung Verantwortliche eingestuft werden. Unternehmen haften nicht nur für Verstöße, die von ihren Vertretern, Leitern oder Geschäftsführern begangen wurden, sondern auch für Verstöße, die von jeder anderen Person begangen wurden, die im Rahmen der unternehmerischen Tätigkeit und im Namen dieser juristischen Personen gehandelt hat.

g. Beschluss vom 12.08.2024 - IDSG 15/2023

I. § 14 Abs. 3 Satz 2 KDG lässt die Fristverlängerung nur zu, wenn die Komplexität und die Anzahl der Auskunftsanträge kumulativ dies erfordern.

II. Der Begriff der personenbezogenen Daten ist weit auszulegen. Er umfasst potentiell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur, wenn es sich um Informationen "über" die in Rede stehende Person handelt.

III. Der durch das Evangelium geprägte Auftrag der Kirche (vgl. can. 747 § 1 CIC) verlangt einen konsequenten Einsatz für den Opferschutz. Die Glaubwürdigkeit ihres Dienstes (§ 6 Abs. 2 lit. j) KDG) kann die Kirche nur wahren oder wiederherstellen, wenn sie gravierendes Fehlverhalten ihrer Bediensteten umfassend aufklärt.

h. EuGH, Urteil vom 11.4.2024 – C-741/21, ZD 2024, 381

I. Art. 82 DS-GVO (§ 50 KDR-OG) ist dahin auszulegen, dass ein Verstoß gegen Bestimmungen dieser Verordnung, die der betroffenen Person Rechte verleihen, für sich genommen nicht ausreicht, um unabhängig vom Schweregrad des von dieser Person erlittenen Schadens einen „immateriellen Schaden“ im Sinne der DS-GVO darzustellen.

II. Art. 82 DS-GVO (§ 51 KDR-OG) ist dahin auszulegen, dass es für eine Befreiung des Verantwortlichen von seiner Haftung nach Art. 82 Abs. 3 DS-GVO nicht ausreicht, dass er geltend macht, dass der in Rede stehende Schaden durch ein Fehlverhalten einer ihm im Sinn von Art. 29 DS-GVO (§ 29 KDR-OG) unterstellten Person verursacht wurde.

i. **BGH, Urteil vom 14.5.2024 – VI ZR 370/22 (LG Darmstadt, AG Seligenstadt) – ZD 2024, 698**
Bei Mitteilung der Kontaktdaten des Datenschutzbeauftragten nach Artikel 13 Abs.1b DS-GVO (§ 15 Abs.1b KDR-OG) ist die Nennung des Namens nicht zwingend. Entscheidend und zugleich ausreichend für den Betroffenen ist die Mitteilung der Informationen, die für die Erreichbarkeit der zuständigen Stelle erforderlich sind. Ist die Erreichbarkeit ohne Nennung des Namens gewährleistet, muss dieser nicht mitgeteilt werden.

j. BAG, Urteil vom 20.6.2024 – 8 AZR 91/22 (LAG Berlin-Brandenburg, ArbG Berlin) - ZD 2025, 50

I. Ein Anspruch auf Schadensersatz nach Art. 82 DSGVO (§ 50 KDR-OG) setzt kumulativ einen Verstoß gegen die DS-GVO, das Vorliegen eines Schadens und einen Kausalzusammenhang zwischen Verstoß und Schaden voraus. Der Anspruchsteller hat das Vorliegen dieser drei Voraussetzungen darzulegen und zu beweisen.

II. Wird der Anspruch auf Auskunft nach Art. 15 DS-GVO (§ 17 KDR-OG) nicht erfüllt, reicht allein die Befürchtung weiterer Verstöße gegen die DS-GVO für die Annahme eines Schadens nicht aus.

6. Tätigkeiten auf Eingaben hin

Auch in diesem Berichtszeitraum war die Mehrzahl der Eingaben auf Rechtsauskünfte gerichtet. Insgesamt kamen 107 schriftliche Auskunftsersuchen und weitere ca. 190 telefonisch. Sie betrafen Fragen zur Aufarbeitung von Unrecht, um Datenverkehr mit Drittländern, Aufbewahrung von Unterlagen, Weitergabe von Daten an Behörden, Folgen von Cyber-Angriffen, fehlgeleiteten E-Mails, Verlust von Mobiltelefonen, Auskunftserteilung und die Herausgabe von Urkunden.

Beschwerden (insgesamt 33) gingen u. a. zu folgenden rechtlichen Gesichtspunkten ein: Unterlassene oder verspätete Auskunftserteilung, Zusendung von Informationsmaterial oder Bitten um Spenden trotz einer vorhandenen Abmeldung des Empfängers, Datenweitergabe bei Vorbereitung von Entschädigungszahlungen.

Von den Dienststellen gingen insgesamt ca. 63 Meldungen über Datenpannen ein. Sie betrafen vor allem die Folgen von Cyberangriffen, fehlgeleitete Briefe oder E-Mails, vermisste oder entwendete Datenträger. In keinem Fall musste ein Bußgeldverfahren durchgeführt werden.

7. Fortbildungsmaßnahmen

Der Unterfertige Joachimski hielt am 21.Januar 2025 einen Videovortrag zur Einführung in das Datenschutzrecht für neu beginnende betriebliche Datenschutzbeauftragte (vormittags) sowie einen Erfahrungsaustausch für alle betrieblichen Datenschutzbeauftragten (nachmittags). An dieser Fortbildung nahmen 59 Personen teil. Die Präsentation ist auf der Webseite[9] abrufbar und kann von allen Interessierten z.B. für interne Fortbildungen verwendet werden.

8. Zusammenarbeit mit anderen Datenschutz-Aufsichtsstellen

Die Unterfertigten nahmen an insgesamt neun persönlichen oder Videokonferenzen der deutschen Diözesandatenschutzbeauftragten teil.

Mit dem Ausdruck unserer vorzüglichen Hochachtung

gez. Jupp Joachimski Christine Haumer Dieter Fuchs

Datenschutzbeauftragte

[9] https://datenschutz.orden.de/downloadbereich/fortbildung