Katholische
Datenschutzaufsicht Nord

8. Jahresbericht

2021

www.kdsa-nord.de

Herausgegeben von

Katholische Datenschutzaufsicht Nord

Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg, der Bistümer Hildesheim, Osnabrück und

des Bischöflich Münsterschen Offizialats in Vechta i.O.

Unser Lieben Frauen Kirchhof 20

28195 Bremen

Telefon: 0421 330056-0

E-Mail: info@kdsa-nord.de

Diesen Tätigkeitsbericht können Sie auch auf unserer Internetseite abrufen unter:

https://www.kdsa-nord.de/Jahresberichte

Sofern im Folgenden nur die männliche Bezeichnung gewählt wurde, so ist dies nicht geschlechtsspezifisch gemeint, sondern geschah ausschließlich aus Gründen der besseren Lesbarkeit.

Inhaltsverzeichnis

Vorwort

Anknüpfend an den Bericht des Vorjahres bleibt festzuhalten, dass die weltweite Pandemie immer noch alle Lebensbereiche tangiert und natürlich auch unsere Tätigkeit bei der Katholischen Datenschutzaufsicht Nord erheblich beeinflusst hat. Corona und kein Ende mag der ein oder andere deshalb denken, wenn der Jahresbericht für den Berichtszeitraum 2021 veröffentlicht wird, und etwas Neues wird es schon nicht geben. Doch ganz so ist es nicht.

Homeoffice, Hygienekonzepte und die Beschaffung von Masken und Desinfektionsmitteln sind Standard geworden. Die Erreichbarkeit der Aufsichtsbehörde und deren Mitarbeiter ist über mobile Kommunikationsstrukturen sichergestellt und die erforderlichen Absprachen und Konferenzen laufen über ein datenschutzrechtlich unbedenkliches Videokonferenzsystem.

Und unabhängig davon fehlt natürlich Allen der unmittelbar menschliche Kontakt im Rahmen von Beratungen, Prüfungen, Vor-Ort-Terminen und Begegnungen. Auch im letzten Jahr waren pandemiebedingt Präsenzveranstaltungen aus Schutzgründen für alle Beteiligten nur sehr eingeschränkt möglich.

Daher war es umso erfreulicher, dass es im laufenden Berichtszeitraum gelungen ist, zumindest mit den Entscheidungsträgern der zur Katholischen Datenschutzaufsicht Nord gehörenden (Erz)Bistümer und dem Offizialatsbezirk Vechta i. O. im Rahmen einer persönlichen Begegnung ins Gespräch gekommen zu sein. Auch eine Konferenz der Diözesandatenschutzbeauftragten konnte unter strengen Hygienemaßnahmen einmal als Präsenzveranstaltung abgehalten werden.

Im Übrigen haben wir unsere Aufgabenwahrnehmung wie gewohnt der allgemeinen Situation angepasst und uns neben der telefonischen und schriftlichen Beratung auf Prüfungen anhand von Aktenlagen fokussiert.

So ist die Auswertung der Querschnittsprüfung für den Bereich der katholischen Kindertagesstäten in unserer Zuständigkeit in dem vorliegenden Bericht ebenso enthalten wie der Hinweis auf eine neue Querschnittsprüfung im Bereich der Caritaseinrichtungen. Die Meldung von Datenschutzverletzung ist noch einmal angestiegen und die Anzahl der Beschwerden hat sich auf ein vergleichbares Maß wie im Jahr 2020 eingependelt.

Wie schon mehrfach berichtet, ist die Datenübermittlung in die Vereinigten Staaten von Amerika auf der Grundlage des „Privacy Shields“ durch ein Urteil des EuGH für

ungültig erklärt worden. Als Folge daraus wird dem Vernehmen nach zwischen der EU und den USA an einem Ersatzabkommen gearbeitet, um einen rechtssicheren Datentransfer zu ermöglichen. Eine Lösung ist noch nicht in Sicht. Andere Sicherungsmechanismen wie etwa Standardvertragsklauseln zur Absicherung der Datentransfers in die USA, sind im Hinblick auf ihre alleinige Anwendung auch rechtlich nicht zweifelsfrei. Auch die Datenschutzaufsichten der Länder sehen die Situation nicht ohne Bedenken. Beispielsweise hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) die Senatskanzlei der Freien und Hansestadt Hamburg (FHH) offiziell gewarnt, die Videokonferenzlösung von Zoom Inc. in der sog. on-demand-Variante zu verwenden, da eine solche Nutzung mit der Übermittlung personenbezogener Daten in die USA verbunden ist.[1]

Die Problemlage beschäftigt auch zunehmend die kirchlichen Datenschutzaufsichten.

Seit dem 18. Juni 2021 ist das Betriebsrätemodernisierungsgesetz in Kraft. Das Gesetz schafft, neben zahlreiche Neuregelungen für die Arbeit der Betriebsräte, durch den eingefügten § 79 a S. 2 BetrVG, Rechtssicherheit hinsichtlich der Frage, wer für die Verarbeitung von personenbezogenen Daten datenschutzrechtlich verantwortlich ist. Die Neuregelung konkretisiert die Vorgaben der DS-GVO dahingehend, dass die datenschutzrechtliche Verantwortlichkeit beim Arbeitgeber liegt. Die Regelung hat ebenfalls Relevanz für die Beurteilungsgrundlagen im Hinblick auf die MAVO.

Mit dem am 1. Dezember 2021 in Kraft getretenen Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG) soll datenschutzrechtliche Sicherheit im Bereich der Telekommunikation und dem Telemediengesetz geschaffen werden. Der Schutzzweck des TTDSG umfasst dabei insbesondere das Endgerät des Benutzers.

Im kirchlichen Bereich hat das Erzbistum Hamburg den Datenschutz an seinen Schulen neu geregelt. Die neue Durchführungsverordnung zum Schutz personenbezogener Daten in katholischen Schulen schafft auch Rechtsgrundlagen für den

[1] Pressemitteilung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg vom 16.08.2021; https://datenschutz-hamburg.de/pressemitteilungen/2021/08/2021-08-16-senatskanzlei-zoom

Einsatz digitaler Werkzeuge im Unterricht. Auch das Bistum Osnabrück hat eine vergleichbare Regelung erlassen.

Im Bistum Osnabrück und im Erzbistum Hamburg ist jeweils ein Gesetz zur Regelung des Rechtsinstruments nach § 29 KDG (§ 29-KDG-Gesetz) und eine Verordnung zur Durchführung des Gesetzes zur Regelung des Rechtsinstruments nach § 29 KDG (§ 29-KDG-Gesetz-DVO) veröffentlicht worden.

Ebenfalls wurden umfangreiche Regelungen zur Aufarbeitung von sexuellem Missbrauch für das Erzbistum Hamburg und das Bistum Osnabrück veröffentlicht und damit Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten im Bereich der Missbrauchs-Aufarbeitung generiert:

- Statut zur Errichtung eines gemeinsamen Betroffenenrates im Rahmen der unabhängigen Aufarbeitung von sexuellem Missbrauch in der Metropolie Hamburg
- Statut für die Aufarbeitungskommission im Rahmen der unabhängigen Aufarbeitung von sexuellem Missbrauch in der Metropolie Hamburg
- Rahmenordnung über die Führung von Personalakten und Verarbeitung von Personalaktendaten von Klerikern und Kirchenbeamten (Personalaktenordnung)
- Gesetz zur Regelung von Einsichts- und Auskunftsrechten für die Kommissionen zur Aufarbeitung von sexuellem Missbrauch Minderjähriger und schutz- oder hilfebedürftiger Erwachsener sowie beauftragte Forschungsinstitute in Bezug auf Personalaktendaten von Klerikern.

Im Bistum Hildesheim ist eine Veröffentlichung vergleichbarer Regelungen in Vorbereitung.

Auch im sechsten Jahr komme ich gerne der mir durch die (Erz-)Bischöfe von Hamburg, Osnabrück und Hildesheim und dem Offizial des Bischöflich Münsterschen Offizialats in Vechta übertragenen Aufgaben nach. Für das Vertrauen und die Unterstützung durch die Herren Generalvikare und die Mitarbeiter in den kirchlichen Behörden und Dienststellen bin ich dankbar. Wichtig ist mir aber auch die Feststellung, dass ich die der Katholischen Datenschutzaufsicht Nord obliegenden Aufgaben nicht allein erfüllen kann, sondern nur in einem motivierten und engagierten Team von Mitarbeitern. Ihnen gilt mein besonderer Dank.

Meinen Tätigkeitsbericht für das Jahr 2021 lege ich nachstehend vor. Wie üblich werde ich neben einer zusammenfassenden Darstellung der Entwicklung des Datenschutzrechtes auf europäischer, deutscher und kirchlicher Ebene auch exempla-

risch auf wesentliche Vorkommnisse in dem Berichtszeitraum hinweisen, die von allgemeiner Bedeutung für die Dienststellen in meinem Tätigkeitsbereich sein können.

Bremen, im März 2022

Andreas Mündelein

Diözesandatenschutzbeauftragter

1. Die Entwicklung des Datenschutzrechts

1.1. Europarecht

1.1.1. Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer

Nach der Entscheidung des EuGHs vom 16. Juli 2020 („Schrems II“) konnte ein Drittstaatentransfer mit personenbezogenem Daten in die USA (Drittland) nicht mehr auf das Datenschutzabkommen („Privacy Shield“) gestützt werden. In der Urteilsbegründung führt der EuGH aus, dass das erforderliche Datenschutzniveau der EU durch das Abkommen nicht gewährt werden konnte. Nicht für generell ungültig erklärt wurden die Standarddatenschutzklauseln der EU-Kommission nach Art. 46 Abs. 2 lit. c) und d) DS-GVO. Bei der Verwendung von Standarddatenschutzklauseln müssen die Einrichtungen jedoch künftig bei der Übermittlung personenbezogener Daten in ein Drittland überprüfen, ob dort – evtl. auch durch zusätzliche vertragliche Vereinbarungen – ein angemessenes Datenschutzniveau hergestellt werden kann und diese Vereinbarungen eingehalten werden können.

Mit dem „Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates“[2] hat die Europäische Kommission die Standardvertragsklauseln für die Übermittlung personenbezogener Daten (an Auftragsverarbeiter) in Drittländer nach der Richtlinie 95/46/EG (Entscheidung 2001/497/EG vom 15. Juni 2001 bzw. Beschluss 2010/87/EU vom 5. Februar 2010) mit Wirkung vom 27 September 2021 aufgehoben. Im Anhang des Durchführungsbeschlusses ist ein neues modulares Framework für die Gestaltung von Standardvertragsklauseln in unterschiedlichen Konstellationen (Verantwortlicher-Verantwortlicher, Verantwortlicher-Auftragsverarbeiter etc.) enthalten.

Aus Sicht der European Data Protection Board (EDPB) wie auch der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) sind für einen Datenexport in Drittländer ergänzende Prüfungen und Maßnahmen erforderlich[3]; ein Abstellen auf die Standardvertragsklauseln allein genügt nicht.

---

2 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914

3 https://www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_scc.pdf

Für Verträge, die vor dem 27. September 2021 abgeschlossen worden sind, ist es befristet bis zum 27.Dezember 2022 noch möglich, diese auf die Grundlage der auslaufenden Entscheidung bzw. Beschlüsse zu stützen. Für alle nach dem 27. September 2021 abzuschließenden Verträge sind die neuen Standartvertragsklauseln zu verwenden.[4]

Die nationalen Aufsichtsbehörden fordern vor einem Drittland-Transfer eine Untersuchung der jeweiligen nationalen Rechtslage in dem Drittland und ggf. zusätzliche Maßnahmen zur Herstellung eines mit der DS-GVO vergleichbaren Datenschutzniveaus. Die kirchlichen Datenschutzaufsichten werden sich dem für ihren Bereich anschließen müssen.

1.1.2. Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern

Mit dem „Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates“[5] hat die Europäische Kommission zusätzlich ein Framework zur Verfügung gestellt, mit dem das vertragliche Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter geregelt und standardisiert werden kann. Die im Anhang von 2021/915 aufgeführten Standardvertragsklauseln können als Vorlage für vertragliche Regelungen zwischen Verantwortlichem und Auftragsverarbeiter verwendet werden.

Diese Standardvertragsklauseln gelten jedoch ausschließlich für die Auftragsverarbeitungen ohne Drittlandsbezug. Sollte eine Übermittlung von personenbezogenen Daten in ein Drittland erfolgen, sind die Standardvertragsklauseln nach dem Durchführungsbeschluss 2021/914 heranzuziehen.

---

4 vgl. Amtsblatt der Europäischen Union, L 199/36 v. 07.6.2021(Art.4 Abs. 4)

5 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32021D0915

1.1.3. Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungsinstrumenten

Sofern der Anlass zur Vermutung besteht, dass das Recht oder die Praxis eines Drittlandes, in das Daten exportiert werden sollen, die Wirksamkeit der in den Übermittlungsinstrumenten gemäß Art. 46 DS-GVO enthaltenen geeigneten Garantien beeinträchtigt, besteht laut dem Urteil „Schrems II“ die Möglichkeit, zusätzliche Maßnahmen zu ergreifen, um diese Schutzlücken zu schließen und die Garantien auf das vom EU-Recht geforderte Niveau zu bringen. Dies ist von den Datenexporteuren laut dem EuGH von Fall zu Fall zu ermitteln und muss gemäß der Rechenschaftspflicht aus Art 5 Abs.2 DS-GVO nachgewiesen werden können.

In diesem Zusammenhang hat das European Data Protection Board die “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data” nach einer öffentlichen Kommentierungsphase am 18. Juni 2021 beschlossen und zur Verfügung gestellt.[6] Einerseits sollen diese Empfehlungen die Datenexporteure bei der komplexen Aufgabe unterstützen, Drittländer im Hinblick auf Recht und Praxis im Datenschutz zu bewerten (s. Klausel 14 „Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken“ der neuen Standardvertragsklauseln). Andererseits sollen Hilfestellungen gegeben werden, um geeignete zusätzliche Maßnahmen zu ermitteln und umzusetzen.

1.1.4. Schrems II und Untersuchungen auf europäischer Ebene

In den vorausgegangenen Tätigkeitsberichten war von den im April 2019 begonnenen Untersuchungen des European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski bzgl. der vertraglichen Verhältnisse zwischen den EU-Einrichtungen (EUIs) und Microsoft berichtet worden. Überprüft worden war die Einhaltung (datenschutz-)rechtlicher Anforderung in den zugrundeliegenden Inter-Institutional Licensing Agreements (ILA). Die Veröffentlichung der Ergebnisse[7] – zusammen mit Feststellungen und Empfehlungen zur Nutzung von Microsoft-Produkten und Services durch EUIs – war im Rahmen des The Hague Forums im Juli 2020 erfolgt. Im

---

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

7 https://edps.europa.eu/sites/default/files/publication/20-07-02_edps_paper_euis_microsoft_contract_investigation_en.pdf

Ergebnis war die Nutzung von Microsoft-Produkten und -Diensten unter den gegebenen Voraussetzungen als nicht unproblematisch angesehen worden [8].

Im Zuge der “Strategy for EU institutions to comply with “Schrems II” Ruling” des EDPS aus dem Oktober 2020[9], die u. a. eine Bestandsaufnahme bestehender Datentransfers bei den EUIs beinhaltet und vor dem Hintergrund der o. g. Ergebnisse, wurden vom EDPS im Mai 2021 zwei Untersuchungen in Folge des Schrems II-Urteils (C-311/18) eröffnet. Gegenstand ist einerseits die Nutzung der Cloud-Dienste von Amazon Webservices und Microsoft seitens der EUI, andererseits die Nutzung von Microsoft (Office) 365 durch die europäische Kommission.

Vorab sei erwähnt, dass die den Untersuchungen vorausgegangene Datenerhebung zu bestehenden Datentransfers ergeben hatte, dass im Rahmen von diversen Verarbeitungsschritten – insbesondere bei der Nutzung von Tools großer Diensteanbieter – personenbezogene Daten nach außerhalb der EU und speziell in die USA übermittelt werden. Bestätigt hat die Datenerhebung ebenfalls, dass eine zunehmende Abhängigkeit von Cloud-basierten Software-, Infrastruktur- und Plattform-Diensten großer Anbieter besteht. Einige dieser Diensteanbieter sind US-basiert und unterliegen der dortigen, im Schrems II-Urteil thematisierten Gesetzgebung.

Im Hinblick auf die Nutzung der Cloud-Dienste von Amazon Webservices und Microsoft wird nun untersucht, ob die EUIs die Anforderungen aus dem Schrems II-Urteil erfüllen. Die zugrunde liegenden „Cloud II Verträge“ sind noch vor der Verkündung des Schrems II-Urteil geschlossen worden; laut dem EDPS ist eine genaue Prüfung erforderlich, ob die nach Urteilsverkündung seitens Amazons und Microsofts angekündigten weiteren Maßnahmen zur Erlangung einer Rechtskonformität ausreichen.

Gegenstand der zweiten Untersuchung ist die Überprüfung, ob die Europäische Kommission beim Einsatz von Microsoft (Office) 365 die vom EDPS im Juli 2020 veröffentlichten Empfehlungen zur Nutzung von Microsoft Produkten und Diensten[10] berücksichtigen.

---

8 https://www.kdsa-nord.de/20200714

9 https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en

10 https://edps.europa.eu/data-protection/our-work/publications/investigations/outcome-own-initiative-investigation-eu_en

1.1.5. Brexit

Seit Beginn des Jahres ist das Vereinigte Königreich nicht mehr Mitglied der Europäischen Union mit der Folge, dass es sich unter datenschutzrechtlichen Voraussetzungen nunmehr um ein sog. Drittland handelt. Insoweit waren die Regelungen für einen Drittlandtransfer zu beachten. Wie berichtet, haben sich die Europäische Union (EU) und das Vereinigte Königreich Großbritannien und Nordirland auf ein Handelsabkommen geeinigt[11]. In dem Abkommen war eine befristete Übergangsregelung im Hinblick auf den Transfer von personenbezogenen Daten von der EU nach Großbritannien aufgenommen worden

Kurz vor Ablauf der Frist hat die Kommission zwei Angemessenheitsbeschlüsse zum Vereinigten Königreich angenommen[12]. Personenbezogene Daten können nun wieder ungehindert aus der Europäischen Union in das Vereinigte Königreich fließen, wo für sie ein Schutzniveau gilt, das dem nach dem EU-Recht garantierten Schutzniveau der Sache nach gleichwertig ist. Die Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG sind somit auch weiterhin zulässig.

1.2. Bundesrecht

1.2.1. Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Mit dem am 1. Dezember 2021 in Kraft getretenen Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG) soll datenschutzrechtliche Sicherheit im Bereich der Telekommunikation und dem Telemediengesetz geschaffen werden. Durch den Zusammenschluss der Datenschutzbestimmungen in einem eigenen Gesetz ist auch die datenschutzrechtliche Umsetzung von Vorgaben aus der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) erfolgt, welche durch die Cookie-Richtlinie (RL 2009/136/EG) geändert worden ist. Der Schutzzweck des TTDSG umfasst insbesondere das Endgerät des Nutzers.

Durch die Regelungen des TTDSG werden alle Anbieter von Telemedien und Telekommunikation gebunden. Auch die katholische Kirche und ihre Stellen können in den Anwendungsbereich des TTDSG fallen (vgl. § 2 Abs. 2 Nr. 1 TTDSG), sofern

[11] https://www.kdsa-nord.de/20201229

[12] https://www.kdsa-nord.de/20210629

sie Anbieter von Telemedien oder Telekommunikation sind (Bsp.: Betreiber und Anbieter von Webseiten, Apps, Speichermöglichkeiten im Netz etc.). Insbesondere das Einwilligungserfordernis für Cookies – unabhängig davon, ob personenbezogene Daten verarbeitet werden oder nicht – ist für die Webseiten der Kirchengemeinden von beachtlicher Bedeutung im Hinblick auf die datenschutzrechtliche Kompatibilität des jeweiligen Produktes. Noch nicht geklärt scheint die Frage der Zuständigkeit der Landesaufsichtsbehörden für den Datenschutz zu sein. Gleiches ist auch noch für die kirchlichen Datenschutzaufsichtsbehörden zu prüfen.

1.2.2. Betriebsrätemodernisierungsgesetz

Wie oben dargestellt, ist seit dem 18. Juni 2021 das Betriebsrätemodernisierungsgesetz in Kraft. Das Gesetz schafft, neben zahlreiche Neuregelungen für die Arbeit der Betriebsräte, durch den eingefügten § 79 a S. 2 BetrVG, Rechtssicherheit hinsichtlich der Frage, wer für die Verarbeitung von personenbezogenen Daten datenschutzrechtlich verantwortlich ist. Die Neuregelung konkretisiert die Vorgaben der DS-GVO dahingehend, dass die datenschutzrechtliche Verantwortlichkeit beim Arbeitgeber liegt. Die Regelung hat zumindest eine gewisse Relevanz für die Beurteilungsgrundlagen im Hinblick auf die MAVO.

Zwar hat die Einführung des § 79a BetrVG zunächst keine unmittelbare Auswirkung auf die Rechtslage im kirchlichen Arbeits- oder Datenschutzrecht. Es kann aber als Anhaltspunkt zur Beurteilung für die im kirchlichen Datenschutzrecht umstrittene Frage, ob die Mitarbeitervertretung „Verantwortlicher“ ist, dienen. Da sich Aufgaben und Rechtsstellung der Mitarbeitervertretung nicht grundsätzlich von denen eines Betriebsrates unterscheiden, erscheint es sachgerecht, auch ohne eine entsprechende gesetzliche Regelung, die Mitarbeitervertretungen nicht als eigene Verantwortliche zu betrachten, sondern die Verantwortlichkeit auch in diesem Teil der Einrichtung beim Arbeitgeber zu sehen. [13]

1.2.3. Gesetzesentwurf zur Änderung des Infektionsschutzgesetzes und der Arbeitsschutzverordnung

Aufgrund der sprunghaft angestiegener Infektionszahlen hat der Bundestag am Donnerstag, den 18. November 2021 dem Gesetzesentwurf zur Änderung des In-

[13] vgl. hierzu Matthias Ullrich in ZMV, Heft 3, 2022

fektionsschutzgesetzes und der Arbeitsschutzverordnung zugestimmt. Mit diesem Gesetzesentwurf wurden bundesweit die Corona-Regeln für Arbeitgeber verschärft.

Ab dem 22. November 2021 galt wieder eine generelle Home-Office-Pflicht für Büromitarbeiter, sofern keine zwingenden betrieblichen Gründe oder Gründe auf Arbeitnehmerseite entgegenstehen; ferner dürfen alle verbliebenen Mitarbeiter seit dem den Betrieb nur dann betreten, wenn sie entweder geimpft, genesen oder getestet sind (3-G Pflicht).

Nach § 28 b Abs. 4 IfSG n.F. haben Arbeitgeber ihren Mitarbeitern im Fall von Büroarbeit oder vergleichbaren Tätigkeiten anzubieten, diese Tätigkeiten im Home-Office auszuführen, wenn keine „zwingenden betriebsbedingten Gründe“ entgegenstehen. Die Mitarbeiter haben dieses Angebot anzunehmen, soweit ihrerseits keine Gründe entgegenstehen. Der Impf- oder Genesenenstatus spielt insofern keine Rolle; die Home-Office-Pflicht gilt grundsätzlich für alle Mitarbeiter, die eine Bürotätigkeit verrichten.

In der Sache gelten bei der Home-Office-Plicht im Wesentlichen dieselben Regeln wie schon im ersten Halbjahr 2021.

Die Mitarbeiter sind zwar grundsätzlich verpflichtet, das Home-Office Angebot anzunehmen. Allerdings können diese das Angebot bereits dann ablehnen, wenn Gründe entgegenstehen. Das können beispielsweise räumliche Enge, Störungen durch Dritte oder unzureichende technische Ausstattung sein. Eine Offenlegung der Gründe gegenüber dem Arbeitgeber dürfte nicht erforderlich sein. Vielmehr soll eine Mitteilung des Beschäftigten ausreichen, dass ihm das Arbeiten von zu Hause aus nicht möglich ist.

Nach § 28b Abs. 1 IfSG dürfen Mitarbeiter, bei denen physische Kontakte zu anderen Mitarbeitern oder zu Dritten nicht ausgeschlossen werden können, den Betrieb nur noch dann betreten, wenn sie entweder geimpft, genesen oder getestet sind und einen Impf-, Genesenen- oder Testnachweis mit sich führen, zur Kontrolle verfügbar halten oder bei dem Arbeitgeber hinterlegt haben. Die Impfung, Genesung oder Testung ist also Zugangsvoraussetzung. Abweichend hiervon darf der Mitarbeiter den Betrieb nur betreten, sofern unmittelbar vor der Arbeitsaufnahme ein Test durchgeführt werden soll oder um ein Impfangebot des Arbeitgebers wahrzunehmen. Über diese betrieblichen Zugangsregelungen hat der Arbeitgeber seine Mitarbeiter zu informieren. Diese Vorgaben bestehen unabhängig von der Betriebsgröße.

Nach § 28b Abs. 3 IfSG sind Arbeitgeber verpflichtet, den 3-G Status ihrer Mitarbei-

ter durch Nachweiskontrollen täglich zu überwachen und regelmäßig zu dokumentieren. Die Mitarbeiter sind verpflichtet, einen Impf-, Genesenen- oder Testnachweis auf Verlangen des Arbeitgebers vorzulegen. Stichprobenartige Kontrollen genügen nicht (Umkehrschluss aus § 28b Abs. 5 IfSG).

Unter datenschutzrechtlichen Gesichtspunkten darf der Arbeitgeber zur Kontrolle der Zugangsvoraussetzungen personenbezogene Daten zum Impf-, Genesungs- und Teststatus verarbeiten. Nach § 28b Abs. 1 Satz 1 IfSG kann der Impf- und Genesungsnachweis auch bei dem Arbeitgeber hinterlegt werden.[14]

1.2.4. Landesrechtliche Regelungen

Nur der Vollständigkeit halber ist auf die jeweils aktualisierten Regelungen für den Umgang mit der Pandemie mit unmittelbaren Auswirkungen auf die kirchlichen Bereiche in den norddeutschen Diözesen hinzuweisen (grundsätzlich s. Bericht 2020). Rechtsgrundlage ist die Vorschrift des § 32 des Infektionsschutzgesetzes. Danach sind Maßnahmen im Rahmen der Pandemiebekämpfung zu treffen. Die im Bereich der Katholischen Datenschutzaufsicht Nord (KDSA Nord) liegenden Bundesländer haben davon Gebrauch gemacht und die Regelungen der jeweiligen Pandemiesituation aktuell angepasst. Sie dienten für den kirchlichen Bereich als Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten.

1.2.5. Neuer Leiter der Hamburger Aufsichtsbehörde

Herr Thomas Fuchs wurde zum neuen „Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit“ (HmbBfDI) gewählt und löste damit Prof. Johannes Caspar als Leiter der obersten Landesbehörde ab.

Herr Fuchs leitet seit dem 1. November 2021 die Hamburger Datenschutzbehörde.

[14] Eine Zusammenfassung findet sich u.a. hier: Noerr_news, Rückkehr zur Home-Office-Pflicht und 3-G Pflicht am Arbeitsplatz,18.11.2021

1.3. Datenschutzrecht der Kirche

1.3.1. Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG)

Wie berichtet, hat der Verband der Diözesen Deutschlands (VDD) ein Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG)[15] auf den Weg gebracht, dass das Verwaltungsverfahren im Bereich des kirchlichen Datenschutzes regelt und damit die erforderliche – mit dem kanonischen Recht vereinbare – Rechtsgrundlage für die Tätigkeit der kirchlichen Datenschutzaufsichten bietet.

Das Erzbistum Hamburg und die Bistümer Osnabrück und Hildesheim haben die Regelung in Kraft gesetzt und in den unten genannten Amtsblättern veröffentlicht.[16]

1.3.2. Durchführungsverordnung zum Schutz personenbezogener Daten in katholischen Schulen im Erzbistum Hamburg vom 19. Mai 2021

Gemäß § 56 KDG hat das Erzbistum Hamburg Regelungen zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft im Erzbistum Hamburg erlassen. Die Durchführungsverordnung ist am 1. Juni 2021 in Kraft getreten.[17]

Inhaltlich unterscheidet sich die Regelung nur wenig von der Anordnung zum Schutz personenbezogener Daten in katholischen Schulen (SchulDSO) im Bistum Hildesheim oder Osnabrück. Die Anordnung ergänzt die Regelungen des Gesetzes über den Kirchlichen Datenschutz (KDG) sowie die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) hinsichtlich der Verarbeitung personenbezogener Daten über Einzuschulende, Schülerinnen und Schüler und Schulbewerberinnen und -bewerber sowie deren Erziehungsberechtigte oder gesetzlich bestellte Betreuer. Als bereichspezifische Regelung geht die Regelung den allgemeinen Bestimmungen des KDG vor.

---

[15] (Kirchliches Datenschutzrecht / hg. vom Sekretariat der Deutschen Bischofskonferenz - Bonn 2021. – 194 S. – (Arbeitshilfen; 320))

[16] Kirchliches Amtsblatt Erzbistum Hamburg, 26. Jahrgang, Nr. 12, 18.12.2020; Kirchliches Amtsblatt Osnabrück Nr. 17 vom 2. August 2021; Kirchlicher Anzeiger für das Bistum Hildesheim NR. 1/2021

[17] vgl. Kirchliches Amtsblatt des Erzbistums Hamburg vom 31. Mai 2021, Jahrgang 27, Nr.6, Art. 77, S. 120 ff

1.3.3. Gesetz zur Regelung des Rechtsinstruments nach § 29 KDG (§ 29-KDG-Gesetz) und eine Verordnung zur Durchführung des Gesetzes zur Regelung des Rechtsinstruments nach § 29 KDG (§ 29-KDG-Gesetz-DVO)

Nach § 29 Absatz 3 des Gesetzes über den Kirchlichen Datenschutz (KDG) erfolgt die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem kirchlichen Recht. Das Erzbistum Hamburg und das Bistum Osnabrück haben inhaltlich vergleichbare Regelungen in Kraft gesetzt, die die Schaffung dieses anderen Rechtsinstruments nach § 29 Absatz 3 des Gesetzes über den Kirchlichen Datenschutz (KDG) zum Inhalt haben. Ergänzend sind jeweils Durchführungsverordnungen zu dem Gesetz erlassen worden.

Die Gesetze gelten für juristische Personen im Bereich der (Erz-) Bistümer Hamburg und Osnabrück, die öffentlich-rechtlich verfasst sind.

Gegenstand der jeweiligen Verordnung ist die Verarbeitung personenbezogener Daten durch das Erzbistum Hamburg bzw. Bistum Osnabrück für die ihrer Aufsicht unterstehenden vorgenannten Einrichtungen

1.3.4. Entscheidungen der Datenschutzgerichte

Das Interdiözesane Datenschutzgericht hat im Berichtszeitraum insgesamt sechs Entscheidung bekannt gegeben. Diese können auf der Webseite der Deutschen Bischofskonferenz heruntergeladen werden.[18] Das Datenschutzgericht der Deutschen Bischofskonferenz als zweite Instanz hat im Berichtzeitraum insgesamt vier Entscheidung veröffentlicht, die ebenfalls dort zu finden sind [19].

1.3.5. Konferenz der Diözesandatenschutzbeauftragten

Die kirchlichen Datenschutzaufsichten haben sich im Rahmen einer „Konferenz der Diözesandatenschutzbeauftragten“ mit dem Ziel zusammengeschlossen, eine möglichst einheitliche Anwendung der kirchlichen Datenschutzbestimmungen zu gewährleisten. Sie entsprechen damit den gesetzlichen Vorgaben nach § 46 KDG.

---

[18] https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen

[19] https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-2-instanz/entscheidungen

Die Konferenz tagt mehrfach im Jahr nach einem abgestimmten Verfahrensablauf. Dazu hat sich die Konferenz eine Geschäftsordnung gegeben.

Danach fördert die Konferenz den Datenschutz und verständigt sich auf gemeinsame Positionen. Dies geschieht unter anderen durch Entschließungen, Beschlüsse oder Orientierungshilfen, Stellungnahmen oder Pressemitteilungen. Der jeweils für ein Jahr gewählte Sprecher der Konferenz nimmt neben den sitzungsorganisatorischen Belangen u. a. auch die Kontaktfunktion zur Konferenz der staatlichen Datenschutzbeauftragten wahr. Er hat dabei repräsentative und kommunikative Aufgaben zu erfüllen, verfügt aber nicht über eine Entscheidungskompetenz für die Konferenz. Damit ist sichergestellt, dass die gesetzlich normierte Unabhängigkeit der Diözesandatenschutzbeauftragten gewährleistet ist.

Folgende Beschlüsse sind durch die Konferenz der Diözesandatenschutzbeauftragten im Berichtsjahr getroffen worden:

- Beschluss betreffend die Datenverarbeitungen im Auftrag im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG vom 4. Januar 2021
- Beschluss zur Verlängerung des Geltungszeitraumes zum Beschluss vom 22. April 2021
- Beschluss zur Beurteilung von Messenger- und anderen Social Media-Diensten vom 15. September 2021

Sämtliche Beschlüsse können auf unserer Homepage abgerufen werden.[20]

2. Katholische Datenschutzaufsicht Nord

2.1. Die Struktur der Katholischen Datenschutzaufsicht Nord

Wie schon mehrfach berichtet hat die kirchliche Datenschutzaufsicht die in Kapitel VI der DS-GVO niedergelegten Bedingungen zu erfüllen (Art. 51, 59 i.V.m. Art. 91 Abs. 2 DS-GVO), und die katholische Kirche hat dies durch die §§ 42 – 46 KDG sichergestellt. Die Verpflichtung der Diözesen umfasst darüber hinaus die Sicherstellung der personellen, technischen und finanziellen Ressourcen. (vgl. Art. 52 Abs. 4 i.V.m. Art. 91 Abs. 2 DS-GVO). Die KDSA Nord ist rechtlich als unabhängige Stelle eigener Art konfiguriert.

[20] https://www.kdsa-nord.de/beschluesse

Die geplante Umsetzung der rechtlichen Neustrukturierung der Aufsichtsbehörde in eine Körperschaft des öffentlichen Rechts (s. Bericht 2019) ist in der Konkretisierung auch im letzten Jahr an der Pandemie gescheitert. Zwar hat unter der Federführung des Katholischen Büros in Bremen ein erstes Treffen stattgefunden, bei dem noch einmal die grundsätzliche Absicht und Bereitschaft der beteiligten Diözesen für die Umstrukturierung der KDSA Nord bestätigt wurde und ein vorläufiger Arbeitsplan abgestimmt wurde, nach dem das Bistum Osnabrück als Belegenheitsbistum die notwendigen schriftlichen Vorarbeiten erstellen soll. Das Katholische Büro wurde gebeten, im Anschluss daran den ersten Kontakt in dieser Angelegenheit mit dem Senat der Freien Hansestadt Bremen zu vereinbaren und das weitere Procedere abzustimmen. Das ist aber noch nicht erfolgt, so dass mit einem neuen Anlauf im laufenden Jahr 2022 zu rechnen ist.

Das Stellentableau umfasst aktuell vier Vollzeitstellen unter Einbeziehung des Sekretariats.

2.2. Statistik und Zahlen

Die Beratungsanfragen sind im Vergleich zum Vorjahr nahezu gleichgeblieben. Hier scheint sich das Niveau der Beratungsanfragen zu festigen.

Die Meldungen von Verletzungen des Schutzes personenbezogener Daten haben sich im Vergleich zum Vorjahr noch einmal erhöht. Diese Erhöhung ist auf den Anfang des Jahres bekanntgewordenen Schwachstellen in Exchange-Servern zurückzuführen. Betroffen hiervon waren insbesondere Kirchengemeinden.

Bei den Prüfungen im Berichtszeitraum haben wir uns auf den Abschluss der Querschnittsprüfungen in den Kindertagesstätten sowie auf Vorbereitung und den Beginn der Querschnittsprüfung bei den Caritasverbänden beschränkt. Prüfungen vor Ort haben nicht stattgefunden. Für das kommende Jahr werden die Prüfungen planmäßig wieder aufgenommen. Von Fall zu Fall wird entschieden, ob es sich um eine rein dokumentenbasierte Prüfung oder um eine Prüfung vor Ort handeln wird.

Die Mitarbeiter der KDSA Nord haben im Berichtszeitraum an sieben Arbeitsgruppen (extern und intern) teilgenommen, die im Wesentlichen als Videokonferenzen durchgeführt wurden.

2.3. Betriebliche Datenschutzbeauftragte in den Einrichtungen

Es ist schon eine gute Tradition geworden, an dieser Stelle des Berichts auf die gesetzlich normierte Notwendigkeit der kirchlichen Einrichtungen zur Bestellung betrieblicher Datenschutzbeauftragter nach § 36 Abs. 1 KDG hinzuweisen und feststellen zu können, dass die Bistümer im Zuständigkeitsbereich der KDSA Nord dieser Verpflichtung weitestgehend nachgekommen sind.

Das führt insbesondere bei den Einrichtungen in der Fläche dazu, dass durch den professionellen Support das eingelöst werden konnte, was zum Beginn der neuen Regelungen des KDG durch die Entscheidungsträger zugesagt worden ist, nämlich dass keine Einrichtung mit den datenschutzrechtlichen Anforderungen allein gelassen wird.

Der Vorteil liegt im Ergebnis aber nicht nur bei den Einrichtungen, sondern ist auch für die KDSA Nord positiv zu vermerken. Die Kommunikation bei Beschwerden, Datenschutzvorfällen oder Prüfungen lässt sich unter fachkundiger Begleitung der Einrichtungen durch professionelle Datenschutzbeauftragte in der Regel ziel- und ergebnisorientiert führen. Insoweit tragen die betrieblichen Datenschutzbeauftragten auch im Sinne der Datenschutzaufsicht dazu bei, dass dem Schutz der personenbezogenen Daten in den kirchlichen Einrichtungen Rechnung getragen wird. An dieser Stelle dürfen wir uns für die Zusammenarbeit bedanken und die betrieblichen Datenschutzbeauftragten auffordern, sich auch zukünftig im Rahmen der etablierten Verfahren bei der Aufsichtsbehörde einzubringen.

2.4. Kirchliches Datenschutz Modell (KDM)

Ein Thema, welches viel Zeit und Ressourcen in Anspruch genommen hat, ist das aus dem Standard-Datenschutzmodell der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) abgeleitete Kirchliche Datenschutzmodell (KDM). Bereits im 6. Jahresbericht hatten wir darüber berichtet, dass die Datenschutzaufsichten der katholischen und evangelischen Kirche den gemeinsamen Entschluss gefasst haben, das Standard-Datenschutzmodell (SDM) an die kirchlichen Gegebenheiten anzupassen. Die daraus resultierende ökumenische Projektgruppe hat – unter Beteiligung der KDSA Nord – auch im Jahr 2021 ihre Arbeit fortgesetzt. Auf dem ökumenischen Datenschutztag am 21. April 2021 hat die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche und der Konferenz der Beauftragten für den Datenschutz in der Evangelischen Kirche in

Deutschland das Kirchliche Datenschutzmodell (KDM) verabschiedet. Das KDM basiert auf dem SDM, wurde jedoch an einigen Stellen angepasst und insbesondere um eine Richtlinie für die Risikoanalyse erweitert. Als zentrale Anlaufstelle für Informationen rund um das KDM haben die katholischen und evangelischen Datenschutzaufsichten eine eigene Webseite eingerichtet (https://www.kirchliches-datenschutzmodell.de).

Die bereits zum Standard-Datenschutzmodell veröffentlichten SDM-Bausteine der DSK sind um Anwendungshinweise zum KDM ergänzt worden. Diese enthalten eine Gegenüberstellung der in den Bausteinen zum SDM dargestellten Angaben zur DS-GVO zu den Vorgaben des KDG und der KDG-DVO sowie des DSG-EKD und können auch weitere kirchlich-spezifische Angaben enthalten. Folgende Anwendungshinweise zum KDM sind im Berichtszeitraum bereits erschienen:

- KDM-Anwendungshinweise zum Baustein 11 – Aufbewahren
- KDM-Anwendungshinweise zum Baustein 41 – Planen und Spezifizieren
- KDM-Anwendungshinweise zum Baustein 42 – Dokumentieren
- KDM-Anwendungshinweise zum Baustein 43 – Protokollieren
- KDM-Anwendungshinweise zum Baustein 50 – Trennen
- KDM-Anwendungshinweise zum Baustein 60 – Löschen und Vernichten
- KDM-Anwendungshinweise zum Baustein 61 – Berichtigen
- KDM-Anwendungshinweise zum Baustein 62 – Einschränken der Verarbeitung

Weitere Anwendungshinweise zum KDM sind in Bearbeitung und werden in der kommenden Zeit veröffentlicht.

Des Weiteren arbeitet eine ökumenische Projektgruppe an einem Fallbeispiel, an dem die Anwendung des KDM in einer fiktiven Kindertageseinrichtung für eine ausgewählte Verarbeitungstätigkeit aufgezeigt und dargestellt werden soll. Die in diesem Zusammenhang erarbeiteten Materialien und Ergebnisse sollen ebenfalls auf der o.g. Webseite bereitgestellt werden.

2.5. Arbeitshilfen zu Windows 10

Mit Meldung vom 11. Mai 2021 hat die Konferenz der Diözesandatenschutzbeauftragten technische Empfehlungen zu Windows 10 veröffentlicht[21]. Ziel der vom Arbeitskreis Technik der Diözesandatenschutzbeauftragten erarbeiteten „Technischen Hinweise für Windows 10 im Rahmen der Verarbeitungstätigkeiten“ ist es, Hilfestellungen für eine möglichst datensparsame Nutzung von Windows 10 zur Verfügung zu stellen.

Die technischen Hinweise bestehen zum einen aus einem Mantelbogen, der Informationen grundsätzlicher Art und allgemeine Angaben für einen datensparsamen Betrieb von Windows 10 enthält. Ergänzt wird dieser Mantelbogen um themenspezifische Anlagen, in denen grundlegende Datenschutzeinstellungen des Betriebssystems sowie die Konfigurationsmöglichkeiten einzelner Dienste, wie z. B. die Windows-Suche, vorgestellt und Konfigurationsempfehlungen formuliert werden.

Im Berichtszeitraum wurden die Technischen Empfehlungen zu den Themen

- Installation
- Applikationen
- Online-Spracherkennung
- Suchfunktion
- Webbrowser

bereitgestellt. Diese sind auf der Webseite der KDSA Nord abrufbar[22].

Nicht Gegenstand der Arbeitshilfe ist dabei die grundsätzliche Fragestellung, ob Windows 10 auf Grund der Übermittlung personenbezogener Daten an ein Drittland überhaupt datenschutzkonform einsetzbar ist; dies ist separat zu bewerten.

2.6. Öffentlichkeitsarbeit

Die KDSA Nord hat die Öffentlichkeitsarbeit auch im Jahr 2021 auf vielfältige Weise fortgesetzt. So wurde u.a. der Aufbau der Internetseite aktualisiert und die Inhalte neu strukturiert. Die von der KDSA Nord bereitgestellten Arbeitshilfen sind unter folgendem Link abrufbar:

---

21 https://www.kdsa-nord.de/20210511

22 https://kdsa-nord.de/arbeitshilfen

– https://www.kdsa-nord.de/arbeitshilfen

Die Arbeitshilfe „Datenschutz im Pfarrbüro“ befindet sich derzeit in Überarbeitung. Im Berichtsjahr haben ist ein Aufruf[23] gestartet worden, damit Interessierte Vorschläge, Kritik und/oder Anmerkungen zu der Arbeitshilfe einreichen konnten. Die eingereichten Anregungen werden in der Aktualisierung des Arbeitshilfe berücksichtigt. Die Veröffentlichung der überarbeiteten Arbeitshilfe „Datenschutz im Pfarrbüro“ ist für das Jahr 2022 geplant.

Ebenso hat die KDSA Nord die Öffentlichkeit über Meldungen auf der Homepage stets über aktuelle und wichtige Themen informiert. Folgende Meldungen sind im Berichtsjahr veröffentlicht worden:

- Brexit Handelsabkommen II
- Microsoft Exchange Schwachstellen
- Arbeitshilfe „Datenschutz im Pfarrbüro“
- Evangelische und katholische Datenschutzaufsichtsbehörden veröffentlichen „Kirchliches Datenschutzmodell“
- Konferenz der Diözesandatenschutzbeauftragten veröffentlicht technische Empfehlung zu Windows 10
- Brexit: Kommission nimmt Angemessenheitsbeschlüsse zum Vereinigten Königreich an
- Die Digitalisierung der Datenschutzprüfung
- Die Europäische Kommission veröffentlicht neu gefasste Standardklauseln
- Jahresbericht 2020
- Technische Empfehlung zu Windows 10 II
- „Kommunikation im Medizinwesen (KIM)“ als Alternative zu Fax und unverschlüsselter E-Mail

Alle Meldungen können unter folgendem Link noch einmal abgerufen werden: https://www.kdsa-nord.de/meldungen

[23] https://www.kdsa-nord.de/20210413

2.7. Informationsveranstaltungen

Es gehört zu den Aufgaben (Beratung) der KDSA Nord, der Nachfrage nach Informationsbedarf in den kirchlichen Einrichtungen nachzukommen. Die Mitarbeiter der KDSA Nord stehen dafür zur Verfügung. Pandemiebedingt hat es keine Anfragen nach einer Präsenzveranstaltung gegeben, so dass alle Anfragen entweder telefonisch oder im Rahmen von Videokonferenzen abgearbeitet worden sind. Auch die regelmäßigen Termine wie etwa

- Jour Fixe mit den betrieblichen Datenschutzbeauftragten
- IT Tagungen
- Treffen mit den Diözesanjuristen

wurden virtuell durchgeführt.

Zudem besteht nach wie vor die Möglichkeit, sich über den kirchlichen Datenschutz im Rahmen der ständig aktualisierten und erweiterten Homepage der KDSA Nord zu informieren.

3. Exemplarische Darstellung von Einzelfragen und Einzelfällen

3.1. Beratungen

3.1.1. Anwendung Luca-App

Aus unterschiedlichen Bereichen erreichten uns Anfragen zur Verwendung der Luca-App als digitales Erfassungssystem bei der Durchführung von kirchlichen Veranstaltungen.

Die KDSA Nord hat dazu folgende Auffassung vertreten.

Ebenso wie die Landesbeauftragte für den Datenschutz in Niedersachsen ist auch die KDSA Nord der Auffassung, dass die Einführung eines digitalen Erfassungssystems zur Information von Besuchern in Fällen eines Infektionsvorkommens an einem Veranstaltungsort grundsätzlich eine gute Möglichkeit der Prävention zur Vermeidung der Ausbreitung der Pandemie darstellt.

Unabhängig davon muss das digitale Verfahren zur Verarbeitung von Kontakt- und Anwesenheitsdaten, so wie es die DSK beschrieben hat, datenschutzkonform betrieben werden können. Diese Voraussetzung war im Hinblick auf die Luca-App noch nicht endgültig abgeschlossen. Fragen ergeben sich schon deswegen, weil

Kontakt- und Bewegungsdaten zentral an einer Stelle gesammelt werden. Auch wenn den Bedenken einer zentralen Speicherung mit dem Argument der Verschlüsselung der Daten begegnet wird, war die Qualität der Verschlüsselung ein nicht unerhebliches Problem. Das Ausspähen oder der Missbrauch dieses Schlüssels würde den unberechtigten Zugriff auf eine hohe Anzahl der von dem System zentral verwalteten Bewegungsdaten möglich machen. Die DSK hat diese Argumente in ihrer Stellungnahme ausführlich dargestellt und darüber hinaus die Anwendung der App auch von einer gesetzlichen Regelung mit abhängig gemacht.

Letzteres begegnet jedenfalls der Nutzung auf einer rein freiwilligen Basis. Es würde dazu führen, dass alle die Besucher bei Veranstaltungen abgewiesen würden, die jedenfalls die Luca-App nicht in Gebrauch haben wollen. Auch wenn die Corona-Warn-App aufgrund der in 2021 bestehenden Verpflichtung zur Erhebung der Kontaktdaten nicht eingesetzt werden konnte, bestanden regional Alternativen, die die Luca-App ersetzen konnten.

Nicht zu vernachlässigen ist im Übrigen die Frage, was mit der Masse der personenbezogenen Daten geschehen könnte, die über die Luca-App durch private Verantwortliche verarbeitet worden sind. Es sind jedenfalls nicht unerheblich lukrative Möglichkeiten denkbar, die mit dem ursprünglichen Zweck der Verarbeitung nicht im Einklang stehen dürften.

Nach alledem rät auch die KDSA Nord von der Nutzung der Luca-App im Hinblick auf den kirchlichen Bereich ab.[24]

3.1.2. Zulässigkeit der Nutzung von Faxgeräten

Nachdem im Mai 2021 die Landesbeauftragte für Datenschutz und Informationsfreiheit[25] in Bremen verkündete, dass die Nutzung von Faxgeräten für die Übermittlung von besonderen Kategorien personenbezogener Daten unzulässig ist, teilte im September 2021 der Hessische Beauftragte für Datenschutz und Informationsfreiheit[26] ebenfalls mit, dass eine Übermittlung von personenbezogenen Daten mit einem ho-

[24] https://www.kdsa-ost.de/aktuelles/107-luca-app-datenschutzrechtlich-zweifelhaft-und-demnaechst-ueberfluessig.html

[25] https://www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen-und-handlungshilfen/telefax-ist-nicht-datenschutz-konform-16111

[26] https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/zur-übermittlung-personenbezogener-daten-per-fax

hen Schutzbedarf ein Verstoß gegen Art. 5 Abs. 1 lit. f) und Art. 32 DS-GVO darstellen kann.

Nachdem diese Meldungen bekanntgeworden sind, erreichte auch die KDSA Nord die Anfrage, ob die Nutzung von Telefaxgeräten zur Übermittlung von besonderen Kategorien personenbezogener Daten, hier Gesundheitsdaten, im kirchlichen Bereich ebenfalls unzulässig sei.

Anders als im staatlichen Bereich haben kirchliche Einrichtungen die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) einzuhalten. Diese konkretisiert die allgemeinen Anforderungen nach § 26 KDG durch Maßnahmenvorgaben und unterstützt so die kirchlichen Einrichtungen bei der Auswahl notwendiger technischer und organisatorischer Maßnahmen.

Bei Gesundheitsdaten handelt es sich um personenbezogene Daten der Datenschutzklasse III gemäß § 13 Abs. 1 KDG-DVO. Bei der Verarbeitung von personenbezogenen Daten der Datenschutzklasse III müssen neben dem Schutzniveau II auch die weiteren Voraussetzungen nach § 13 Abs. 2 KDG-DVO erfüllt sein. Bereits das Schutzniveau II sieht in § 12 Abs. 2 lit. e) KDG-DVO vor, dass die „*Übermittlung personenbezogener Daten außerhalb eines geschlossenen und gesicherten Netzwerks (auch über automatisierte Schnittstellen) […] grundsätzlich verschlüsselt zu erfolgen*“ hat. Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen. Hinweise zu dem einzusetzenden Verschlüsselungsverfahren gibt bspw. die BSI-Technische Richtlinie BSI TR-02102-1[27].

Somit gilt auch für besondere Kategorien personenbezogener Daten, insbesondere für Gesundheitsdaten, die Pflicht, diese grundsätzlich verschlüsselt zu übertragen, sofern die Übermittlung außerhalb eines geschlossenen und gesicherten Netzwerkes erfolgt.

Alternativ zu der Übermittlung von Gesundheitsdaten per Telefax sollte geprüft werden, ob eine Ende-zu-Ende-verschlüsselte E-Mail-Übertragung in Betracht kommt. Hierfür stehen zwei unterschiedliche Standards (S/MIME und PGP) zur Verfügung. Ebenso kann, wie bereits auf der Homepage der KDSA Nord berichtet[28], zumindest in Krankenhäusern die Einführung des Dienstes „Kommunikation im Medizinwesen

[27] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

[28] https://www.kdsa-nord.de/20210929

(KIM)“ Abhilfe schaffen. KIM soll sicherstellen, dass Leistungserbringer einen elektronischen und sicheren Weg zur Übermittlung u. a. von Arztbriefen und Befunden nutzen können.

Nach wie vor hält die KDSA Nord jedoch die Übermittlung von personenbezogenen Daten in Ausnahmefällen, z. B. in medizinischen Notfällen, für zulässig, wenn die ergänzenden organisatorischen Maßnahmen nach § 24 Abs. 4 KDG-DVO (Abstimmung des Sendezeitpunktes sowie des Empfangsgeräts) strikt eingehalten werden.

3.2. Beschwerden

3.2.1. Nutzung der privaten Telefonnummer

Eine Beschwerde richtet sich gegen die dienstliche Nutzung einer privaten Telefonnummer. Die Kirchengemeinde als Beschwerdegegnerin hatte auf Anfrage eines Kirchengemeindemitglieds die private Festnetz-Telefonnummer zur Kontaktaufnahme mit der Beschwerdeführerin – ohne deren Einverständnis – herausgegeben. Die Kirchengemeinde teilte mit, dass Anfragen von Kirchengemeindemitgliedern grundsätzlich per E-Mail an die zuständigen Mitarbeiter weitergeleitet werden, sodass diese dann die Möglichkeit haben, auf die Kontaktanfrage zu reagieren. Die anwesende Mitarbeiterin im Pfarrbüro war jedoch als Urlaubsvertretung nicht in Gänze mit dem üblichen Vorgehen vertraut, sodass die private Telefonnummer an das anfragende Kirchengemeindemitglied herausgegeben worden ist. Da keine Einwilligung zur Herausgabe der privaten Telefonnummer durch die Beschwerdeführerin vorlag, war die Herausgabe datenschutzrechtlich unzulässig.

3.2.2. Datenschutzerklärungen Homepage

Auch in diesem Jahr gab es Beschwerden zu (zumeist unvollständigen) Datenschutzerklärungen der Homepages von kirchlichen Einrichtungen.

Exemplarisch genannt seien zwei Beschwerden, die sich mit fehlenden Hinweisen zu Verarbeitungen personenbezogener Daten befassten.

Die eine Einrichtung teilte mit, dass nach einer Wiederherstellung der Webseite aus einem Backup nicht geprüft worden sei, welchen Stand die Datenschutzerklärung nach der Wiederherstellung hatte. So wurde eine veraltete Fassung der Datenschutzerklärung online gestellt. Diese Fassung enthielt jedoch nicht den datenschutzrechtlichen Hinweis auf die beschwerdegegenständliche Verarbeitung durch einen Dritten.

Die zweite Einrichtung teilte mit, dass durch ein Update des Content-Management-Systems der Link für die lokale Einbindung eines Skriptes durch Default-Werte überschrieben worden ist. Hierdurch baute die Webseite eine Verbindung zu einer Drittseite auf, wodurch auch personenbezogene Daten unzulässigerweise übermittelt worden sind.

Beide Einrichtungen haben noch im Laufe des Beschwerdeverfahrens die Fehler behoben, sodass keine datenschutzrechtlichen Anordnungen getroffen werden mussten.

3.2.3. Fotografien von Impfzertifikaten

Am Ende des Jahres erreichte uns eine Beschwerde, in welcher der Beschwerdeführer vorgetragen hat, dass ein Foto seines Impfzertifikates sowie des Personalausweises im Rahmen der 3G-Einlasskontrolle zu einem Gottesdienst gemacht worden ist. Als Begründung ist dem Beschwerdeführer mitgeteilt worden, dass das Foto dazu dienen soll, das Zertifikat beim nächsten Gottesdienstbesuch nicht mehr vorzeigen zu müssen.

Noch am Tag des Eingangs der Beschwerde ist bis zur abschließenden Klärung des Sachverhalts ein vorläufiges Verbot der Erhebung und weiteren Verarbeitung von Fotografien der Impfzertifikate und der Personalausweise ausgesprochen worden. Von der Möglichkeit, sich zu den erhobenen Vorwürfen zu äußern, hat die Kirchengemeinde keinen Gebrauch gemacht, sodass das Verbot der Erhebung und weiteren Verarbeitung von Fotografien der Impfzertifikate und der Personalausweise bestätigt werden konnte. Zudem ist angeordnet worden, die bereits erhobenen Daten unverzüglich zu löschen.

3.3. Datenpannen

3.3.1. Exchange Server („Hafnium“)

Anfang März 2021 hat Microsoft Patches für insgesamt vier Schwachstellen in Microsoft Exchange Servern (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 und CVE-2021-27065) bereitgestellt. Laut einer Zeitleiste auf der von den Entdeckern von zweien der Schwachstellen betriebenen Webseite [29] waren diese zu Beginn des Jahres 2021 an Microsoft gemeldet worden. Die Bereitstellung der Patches erfolgte durch das Microsoft Security Response Center (MSRC) am 2. März

[29] https://proxylogon.com

2021[30], am selben Tag, an dem das Unternehmen Volexity über die aktive Ausnutzung von multiplen Zero-Day Schwachstellen in Microsoft Exchange Installationen berichtet hat[31]. Dabei hat sich die Art der Ausnutzung der Schwachstelle gemäß der Veröffentlichung des Bundesamts für Sicherheit in der Informationstechnik „Microsoft Exchange Schwachstellen (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), Detektion und Reaktion, Version 2.4“ im Laufe der Zeit gewandelt. Scheinen diese Schwachstellen zunächst nur für Angriffe auf ausgewählte Einrichtungen wie Universitäten und Nicht-Regierungs-Organisationen sowie Kanzleien und Rüstungsfirmen vorwiegend in Nordamerika eingesetzt worden zu sein (diese Angriffe werden der Gruppe Hafnium zugeschrieben), hat sich dies mit der Veröffentlichung dahingehend geändert, dass Angriffe fortan weltweit und gegen „Tausende von Zielen“ gestartet worden sind. Die nach Ausnutzung der Schwachstellen eingesetzte Schadsoftware wie auch die Ziele der Angreifer waren gemäß der o. g. Publikation des BSI vielfältig. Erschwert wurde eine Detektion auch dadurch, dass eine Ausnutzung der Schwachstellen, die über einen Fernzugriff über das Internet möglich ist, zum Teil automatisiert erfolgte und zum Teil lediglich ein Zugang zu den Systemen – vermutlich zur späteren Verwendung – etabliert worden ist. Das BSI stufte das Angriffsrisiko in einer Pressemitteilung vom 5. März 2021 als sehr hoch ein und empfahl dringend die Überprüfung der Systeme auf die bis dahin bekannt gewordene Auffälligkeiten. Diese Empfehlung wurde auch von der KDSA Nord in einer Meldung vom 26. März 2021 im Zusammenhang mit dem von Microsoft zwischenzeitlich vermeldeten Patch-Stand noch einmal aufgegriffen und insbesondere auf die Gefahr der Infektion mit bis dato unbekannter Schadsoftware hingewiesen.

Aus Datenschutzsicht galt für die Einrichtungen, bei denen unter Ausnutzung dieser Lücke ein unbefugter Zugriff auf personenbezogene Daten des Microsoft Exchange-Servers erfolgt ist, dass dies einen datenschutzrechtlichen Verstoß darstellt. Nach § 6 Abs. 2 lit. c) 2. Hs. KDG-DVO dürfen die personenbezogenen Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Die Meldepflicht ergibt sich in diesem Fall aus § 33 Abs. 1 KDG. Je nach Ausgestaltung des Patchmanagements kann auch ein Verstoß gegen § 16 Abs. 3 KDG-DVO vorliegen.

---

30 https://msrc.microsoft.com/update-guide/de-de/vulnerability/CVE-2021-26855 (bzw. 26857/26858/27065)

31 https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

3.3.2. Einbruchdiebstahl Kindertagesstätten

Auch im Berichtsjahr 2021 gingen Meldungen zu Einbrüchen in Kindertagesstätten bei der KDSA Nord ein. In der Regel sind nicht die auf den Datenträgern abhandengekommenen personenbezogenen Daten das Ziel der Täter, sondern die Datenträger selbst. Dennoch kommen bei solchen Einbrüchen auch personenbezogene Daten wie Bilder aus dem Kita-Alltag oder Kommunikationsdaten mit den Eltern abhanden.

Leider konnte wieder festgestellt werden, dass die mobilen Datenträger wie Laptops nur mit einem Passwort gesichert waren. Eine Verschlüsselung der Festplatte konnte lediglich in Teilen festgestellt werden.

Kindertagesstätten arbeiten häufig mit personenbezogenen Daten der Datenschutzklasse II nach § 12 Abs. 1 KDG-DVO. Bereits die Angabe von Geburtsdaten bedeutet, dass die Mindestvorgaben nach § 12 Abs. 2 KDG-DVO ebenfalls zu beachten sind. Nach § 12 Abs. 2 S. 2 lit. d) KDG-DVO sind personenbezogene Daten der Datenschutzklasse II auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu speichern, sofern keine begründeten Ausnahmefälle gegeben sind. Zentrale Systeme können bspw. der in der Einrichtung selbst betriebene oder durch einen Dienstleister betriebene Server in einem Rechenzentren sein. Ein besonders gegen unbefugten Zutritt gesicherter Raum soll einen unbefugten Zutritt zur Datenverarbeitungsanlage verhindern. Dies kann durch Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner und/oder Alarmanlagen sichergestellt werden.

In den Einrichtungen ist angeordnet worden, die gesetzlichen Vorgaben nach § 12 Abs. 2 S. 2 lit. c) KDG-DVO umzusetzen.

3.3.3. Telefonische Auskunft

Telefonische Auskünfte können in datenschutzrechtlicher Hinsicht durchaus schwierig sein. In einem Fall ist gemeldet worden, dass einer Person telefonisch Auskunft über eine Mitarbeiterin der kirchlichen Einrichtung erteilt worden ist. Bei dem Anrufer handelte es sich um den möglichen künftigen Vermieter der Mitarbeiterin, welchem Auskunft über den Bestand des Arbeitsverhältnisses erteilt worden ist. Bei dieser Person handelt es sich nicht um eine befugte Person, welche diese Informationen erhalten durfte. Als Folge aus diesem Sicherheitsvorfall führt die Einrichtung eine Schulung durch, um die Mitarbeiter im Umgang mit telefonischen Auskünften zu unterrichten.

3.3.4. Anwendung der Regelung zum Schutz personenbezogener Daten in Katholischen Schulen (Hamburg)

Bei der Erfüllung ihrer Aufgaben sind die katholischen Schulen darauf angewiesen, personenbezogene Daten zu verarbeiten. Daraus ergibt sich die Verpflichtung, die Daten vertraulich zu behandeln, sie nur zu verwenden, soweit es für die rechtmäßige Erfüllung ihrer Aufgaben erforderlich ist, und die Betroffenen vor jedem Missbrauch zu schützen. Was zur Aufgabenerfüllung notwendig ist, ergibt sich aus dem geltenden Recht.

Folgendes Beispiel macht dies deutlich:

Durch eine schadhafte Software auf einem privaten PC einer Lehrkraft ist es zu einem Datendiebstahl gekommen. Der privaten Rechner wurde zunächst für schulische Zwecke genutzt, später dann durch einen dienstlichen Rechner ersetzt. Die Daten auf dem privaten PC sind nie gelöscht worden. Dies erfolgte nachweisbar erst durch die Zerstörung der Festplatte des privaten PC unter Mitwirkung einer Fachfirma nach Feststellung des Abhandenkommens der personenbezogenen Schuldaten.

Eine schriftliche Genehmigung durch die Schulleitung zur Verarbeitung personenbezogener Daten von Schülern auf dem privaten EDV-Gerät ist nicht erfolgt, beziehungsweise lag nicht vor. Eine Kontrollroutine durch die Schule im Hinblick auf die Verwendung privater Geräte war nicht vorhanden.

Das Erzbistum Hamburg hat Regelung zum Schutz personenbezogener Daten in seinen katholischen Schulen erlassen (s.o.). Im Rahmen der geltenden Verordnung ist abschließend geregelt, welche Anforderungen bei der Verwendung privater EDV-Anlagen zwingend einzuhalten sind. Die Voraussetzungen wurden nicht erfüllt. Die verantwortlichen Stellen haben die Regelungen einzuhalten.

Die Datenschutzaufsicht kann Anordnungen treffen, die geeignet sind, Verarbeitungsvorgänge innerhalb einer von der Datenschutzaufsicht zu bestimmenden Frist mit den kirchlichen Datenschutzgesetzen in Einklang zu bringen. Es wurde daher unter Fristsetzung angeordnet, ein dokumentiertes Verfahren für die Verarbeitung von personenbezogenen Daten gemäß den Bestimmungen der Durchführungsverordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft im Erzbistum Hamburg zu etablieren.

3.4. Prüfungen

Die Datenschutzaufsicht ist gem. § 44 KDG verpflichtet, über die Einhaltung der Vorschriften des Datenschutzgesetzes und anderer Vorschriften über den Datenschutz zu wachen. Hierbei ist die Aufsicht berechtigt, anlasslos oder anlassbezogen, notwendige Untersuchungen einzuleiten. Diese können z.B. im Rahmen von Vor-Ort-Terminen, digital oder nach Aktenlage durchgeführt werden. In Pandemiezeiten hat sich die digitale Prüfung bewährt und das Mittel der Querschnittsprüfung wurde etabliert. Diese war im Berichtzeitraum die vorherrschende Methode zur Erfüllung der oben genannten Verpflichtung.

Die Ergebnisse der Querschnittsprüfungen der Kindertagesstätten sowie die Vorbereitung und der Start der Querschnittsprüfung der Caritas-Verbände werden nachstehend beschrieben.

3.4.1. Querschnittsprüfung Kindertagesstätten

Bereits im 7. Jahresbericht ist berichtet worden, dass eine Online-Prüfung bei den Kindertagesstätten im Zuständigkeitsbereich der KDSA Nord durchgeführt wurde. Im Berichtszeitraum konnte diese Online-Prüfung nun erfolgreich abgeschlossen werden.

Anlass für die Durchführung der Querschnittsprüfung war die Zunahme der Meldungen über Datenverluste bedingt durch gestohlene Laptops und Datenträger in Kindertageseinrichtungen. Bereits im August 2019 erfolgte diesbezüglich zunächst eine Sensibilisierung der Einrichtungen über die (Erz-)Bischöflichen Generalvikariate sowie das Bischöflich Münstersche Offizialat. Anschließend wurde die Umsetzung der datenschutzrechtlichen Vorgaben sowie der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten in zufällig ausgewählten Einrichtungen im Rahmen einer Querschnittsprüfung stichprobenartig geprüft. Das Ergebnis der Online-Prüfung soll im Folgendem dargestellt und erläutert werden.

Die Querschnittsprüfung in ausgewählten Kindertageseinrichtungen in den norddeutschen (Erz-)Diözesen sowie im Bischöflich Münsterschen Offizialat Vechta zur Prüfung der Umsetzung datenschutzrechtlicher Vorgaben sowie der technischen und organisatorischen Maßnahmen konnte Anfang Juli 2021 abgeschlossen werden. Es wurden sowohl die Ergebnisdokumentationen als auch ggf. die Hinweise für eine Verbesserung des Datenschutzes und/oder eine Auflistung von Nachbesserungsbedarfen an die verantwortlichen Stellen gesendet.

Die Überprüfung der Einhaltung datenschutzrechtlicher Vorgaben ist über das Ausfüllen eines allgemeinen elektronischen Fragebogens sowie über die Beantwortung einrichtungsspezifischer Nachfragen rein digital erfolgt; Vor-Ort-Termine haben in diesem Zusammenhang nicht stattgefunden.

Auch wenn sich Ablauf und Stichprobennahme von einer Prüfung vor Ort unterscheiden, so war es doch möglich, Hinweise für eine Verbesserung des Datenschutzes auszusprechen und/oder Nachbesserungsbedarfe zu identifizieren – und auch grundsätzlich für das Thema Datenschutz zu sensibilisieren.

Behandelt wurden folgende Themenbereiche:

- Betrieblicher Datenschutzbeauftragter
- Grundlagen zur Datenverarbeitung
- Organisatorischer Datenschutz
- Löschen und Verschlüsseln von Daten
- allgemeine technische und organisatorische Maßnahmen

Die Antworten auf Prüffragen ergeben einen umfassenden Eindruck über die Berücksichtigung datenschutzrechtlicher Vorgaben innerhalb der kirchlichen Einrichtung. Prüffragen konnten entweder durch eine ja/nein-Antwort, vorgegebene Auswahlmöglichkeiten oder eine Freitexteingabe beantwortet werden. In den Fällen, in denen sich aus den übermittelten Angaben Nachfragen ergeben, wurden der Einrichtung in einer zweiten Runde spezifische Nachfragen zugesandt, die als Freitext zu beantworten waren. Die Prüffragen sind als Anlage 2 diesem Bericht auszugsweise beigefügt.

Die einzelnen Prüfpunkte wurden dahingehend bewertet, ob bei den abgefragten Sachverhalten eine Abweichung von den datenschutzrechtlichen Vorgaben in Form eines Verbesserungspotenzials (Hinweises) vorliegt oder Nachbesserungsbedarf bestand.

- „Hinweis“ bedeutet, dass die Erfüllung datenschutzrechtlicher Vorgaben möglicherweise noch verbessert werden kann. Eine Umsetzung ist nicht zwingend vorgeschrieben, sollte jedoch geprüft werden. Ggf. wurden die Hinweise auch für eine Sensibilisierung zu einem bestimmten Sachverhalt genutzt.

– „Nachbesserungsbedarf“ bedeutet, dass auf Grundlage der übermittelten Antworten die Erfüllung der gesetzlichen Anforderungen nicht festgestellt werden konnte und Veränderungen vorgenommen werden müssen.

Insgesamt hat die Querschnittsprüfung ergeben, dass die Einrichtungen auf einem guten Weg im Hinblick auf die Umsetzung datenschutzrechtlicher Vorgaben sind und dieses Thema Gegenstand weiterer und laufender Aktivitäten ist. Einrichtungsübergreifend kann festgestellt werden, dass die meisten Nachbesserungsbedarfe im Bereich der Vermeidung unberechtigter Nutzung von IT-Systemen und dort speziell in der Sicherstellung der Aktualität vergebener Berechtigungen identifiziert worden sind. Die meisten Hinweise für eine mögliche Verbesserung des Datenschutzes wurden im Themenbereich Löschen von Daten formuliert.

Insgesamt wurden in 22 Einrichtungen Nachbesserungsbedarfe festgestellt und Bescheide in Form einer Verwarnung zugestellt. In 16 Einrichtungen wurden lediglich Hinweise ausgesprochen und entsprechende Informationsschreiben versandt (s. Abbildung 1). In Abbildung 2 ist dargestellt, wie viele Hinweise und Nachbesserungsbedarfe für die Einrichtungen im Mittel und maximal/minimal formuliert worden sind.

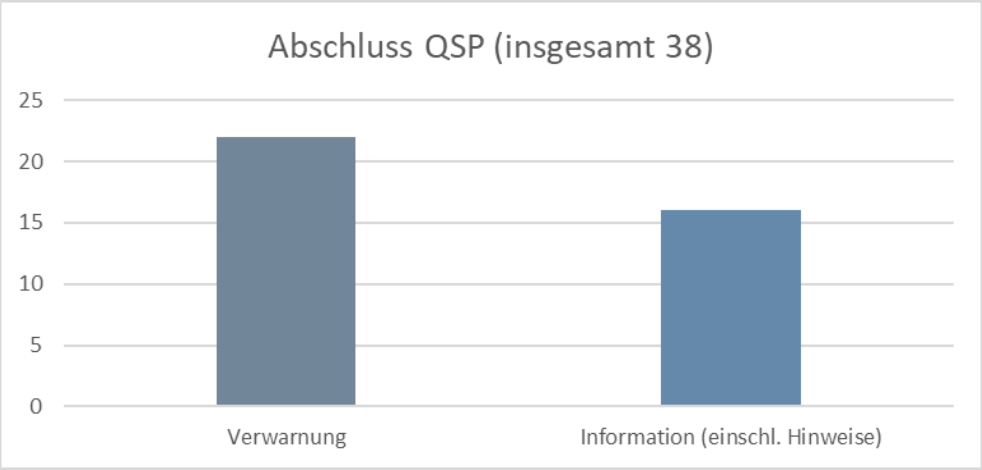

Abbildung 1 Ergebnis der Querschnittsprüfung im Hinblick auf die versandten Bescheide (Verwarnung) und Informationsschreiben

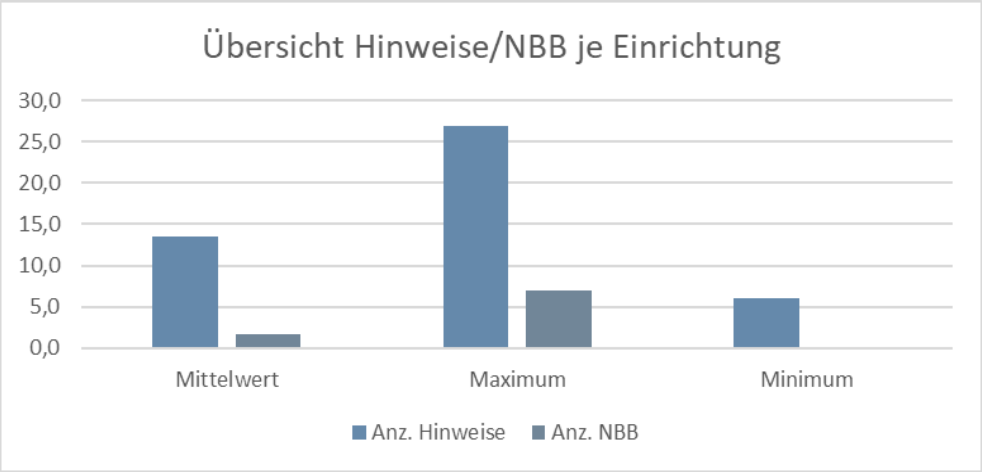

Abbildung 2 Ergebnisse der formulierten Hinweise und identifizierten Nachbesserungsbedarfe (NBB) für die Einrichtungen im Mittel, sowie die minimalen und maximalen Werte, die in den Einrichtungen vorgekommen sind.

Tabelle 1 beinhaltet die Top 10 der Prüfpunkte über alle Einrichtungen, die zur Formulierung eines Hinweises geführt haben. Angegeben sind die Diözesen-übergreifenden Zahlen. Sofern mehr als zehn Prüfpunkte die zehnhäufigsten Anzahlen aufweisen, sind diese alle in der Tabelle aufgeführt.

Die Prüfung hat rein online-basiert und nicht vor Ort stattgefunden. Im Zweifelsfall, ob es sich bei einer Feststellung – auch nach einer Nachfragerunde – um einen Nachbesserungsbedarf oder um einen Hinweis handelt, wurde diese zugunsten der Einrichtung als Hinweis eingestuft.

Tabelle 1 Top 10 der Prüfpunkte, bei denen Diözesen-übergreifend die meisten Hinweise ausgesprochen worden sind. Ausgewertet wurden 38 Fragebögen.

Rang	Themenbereich	Prüfpunkt	Anzahl
1	Löschen von Daten	Löschen (ext. (kirchl.) Archiv)	29
2	Löschen von Daten	Datenträgervernichtung	26
3	Virenscanner	Aktualität Virenscanner	25
3	Löschen von Daten	Ausmusterung Datenträger	25
5	TOM	Überprüfung Zugang/Zugriff (regelm.)	23
6	TOM	Überprüfung Zutritt (regelm.)	22
7	Zugangsschutz	Gruppenaccount	21
8	Informationspflicht	Informationspflicht (Aushang)	17
8	Datensicherheit	Verschlüsselung Datenträger	17
9	Informationspflicht	Informationspflicht (Webseite)	15
9	Informationspflicht	Informationspflicht (Schulung/Sensibilisierung)	15

Wie oben beschrieben, wurden die formulierten Hinweise auch für die Sensibilisierung für bestimmte Sachverhalte genutzt. Als Beispiele seien auf Rang 1 das Auslagern der Daten in externes (kirchliches) Archiv, auf Rang 2 der Hinweis auf eine entsprechende Norm für die Entsorgung von Datenträgern und auf Rang 7 Hinweise zum Einsatz von Gruppenaccounts genannt.

Nachbesserungsbedarfe sind dort formuliert, wo anhand der übermittelten Antworten die Erfüllung der rechtlichen Anforderungen nicht gegeben scheint und Änderungen vorgenommen werden müssen.

Tabelle 2 beinhaltet die Top 5 der Prüfpunkte über alle Einrichtungen, die zur Feststellung eines Nachbesserungsbedarfes geführt haben. Angegeben sind die Diözesen-übergreifenden Zahlen. Sofern mehr als fünf Prüfpunkte die fünf häufigsten Anzahlen aufweisen, sind diese alle in der Tabelle aufgeführt.

Tabelle 2 Top 5 der Prüfpunkte, bei denen Diözesen-übergreifend die meisten Nachbesserungsbedarfe identifiziert worden sind. Ausgewertet wurden 38 Fragebögen.

Rang	Themenbereich	Prüfpunkt	Anzahl
1	TOM	Überprüfung Zugang/Zugriff (gelegtl.)	12
2	TOM	Überprüfung Zutritt (gelegtl.)	11
3	TOM	Protokollierung (Eingabe)	5
3	TOM	Eingabekontrolle (allg.)	5
5	TOM	Boot-Schutz	4
5	TOM	Protokollierung (Vorhaltezeit)	4

Die Einrichtungen sind aufgefordert, festgestellte Nachbesserungsbedarfe innerhalb einer vorgegebenen Frist zu beheben und nachweisen zu können.

3.4.2. Querschnittsprüfung Caritas

Im Berichtszeitraum hat die KDSA Nord nach erfolgreichem Abschluss der Querschnittsprüfung der Umsetzung datenschutzrechtlicher Vorgaben in ausgewählten Kindertagesstätten in ihrem Zuständigkeitsbereich eine weitere Querschnittsprüfung gestartet. Die Prüfung wurde wiederum als Online-Prüfung konzipiert und erfolgt auf der Ebene der Caritas-Verbände.

Gegenstand der Prüfung sind die Themenbereiche:

- Datengeheimnis
- Auskunftsersuchen und Informationspflichten
- Verzeichnis von Verarbeitungstätigkeiten
- Meldungen an die Aufsicht
- Technik und Organisation

Gegebenenfalls werden die aus unterschiedlichen Kapiteln und Abschnitten des KDG stammenden Themenbereiche anhand von vorgegebenen Verarbeitungstätigkeiten konkretisiert.

Ziel ist es auch hier sicherzustellen, dass die datenschutzrechtlichen Vorgaben eingehalten werden und ggf. notwendige Prozesse etabliert sind.

4. Über die Dienststelle des DDSB/KDSA Nord-Bremen

4.1. Infrastruktur

Das Büro der KDSA Nord ist in der zentralen Innenstadt von Bremen eingerichtet. Die Anschrift lautet:

Unser Lieben Frauen Kirchhof 20, 28195 Bremen.

Das Büro ist regelmäßig von Montag bis Donnerstag in der Zeit von 09:00 bis 16:00 Uhr und am Freitag von 09:00 bis 12:00 Uhr zu erreichen.

Telefon: 0421 330056-0

E-Mail: info@kdsa-nord.de

4.2. Finanzen

Die Personal- und Sachkosten der KDSA Nord werden durch eine Finanzumlage der beteiligten (Erz-)Bistümer und des Bischöflich Münsterschen Offizialats in Vechta nach einem vereinbarten Schlüssel getragen.

Die Finanz- und Budgethoheit liegt beim Diözesandatenschutzbeauftragten. Die Abwicklung des Haushaltes erfolgt über die Finanzabteilung des bischöflichen Generalvikariates Osnabrück als Belegenheitsbistum für die Stadt Bremen.

Für das Kalenderjahr 2021 standen Haushaltsmittel in Höhe von 424.500 EUR zur Verfügung.

4.3. Vertretung in Konferenzen und Arbeitsgruppen

Der Leiter der KDSA Nord ist persönlich in einer Reihe von ständigen oder temporären Konferenzen oder Arbeitsgruppen vertreten.

- Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche
- IT-Tagung für die Leiter der IT-Abteilungen der (Erz-)Diözesen und des Bischöflich Münsterschen Offizialats in Vechta und die Datenschutzreferenten
- Konferenz der Diözesanjuristen der norddeutschen (Erz-)Diözesen und des Bischöflich Münsterschen Offizialats in Vechta
- Regelmäßige virtuelle Treffen mit den betrieblichen Datenschutzbeauftragten

Überwiegend sind die Termine virtuell durchgeführt worden.

4.4. Vernetzung

Im Berichtszeitraum sind Kontakte aufgebaut und Gespräche mit den Landesbeauftragten für den Datenschutz und Informationsfreiheit geführt worden.

Darüber hinaus besteht ein guter Kontakt zum Beauftragten für den Datenschutz in der evangelischen Kirche Deutschlands und anderen kirchlichen Datenschutzbeauftragten oder Datenschutzreferenten.

5. Schlussbemerkung

Im Rahmen der Möglichkeit der uns alle betreffenden pandemischen Lage sind wir verlässlich und kompetent unseren Aufgaben nachgekommen. In dem Bewusstsein, dass das Recht auf informationelle Selbstbestimmung als das Recht des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, nicht disponibel ist, sind wir angetreten, die Rechte der Betroffenen umfassend zu schützen.

Der vorstehende Bericht kann insoweit natürlich nur einen kleinen Teil der Arbeit des Diözesandatenschutzbeauftragten mit seinem Team wiedergeben. Die Aufnahme sämtlicher Anfragen, Beschwerden sowie die Auflistung der gesamten Beratungsarbeit würden den Rahmen eines solchen Berichts bei weitem sprengen. Es kommt dem Verfasser vielmehr darauf an, wesentliche Schwerpunkte herauszuarbeiten und damit auch Hinweise für die Zukunft zu geben.

Wir leben nicht nur unter Datenschutzgesichtspunkten in schwierigen Zeiten. Umso wichtiger erscheint es uns insoweit zumindest in unserem Zuständigkeitsbereich für eine verlässliche und den Betroffenen zugewandte behördliche Institution Sorge zu tragen.

Bremen, im März 2022

6. Anlagen

6.1. Betriebliche Datenschutzbeauftragte

Liste der betrieblichen Datenschutzbeauftragten auf der Ebene der (Erz-)Bistümer und des Offizialatsbezirks Vechta

Einrichtung	Datenschutzbeauftragte	Anschrift
Bischöfliches Generalvikariat Osnabrück	Herr Thomas Marien datenschutz@bistum-os.de	Hasestraße 40a 49074 Osnabrück
Ehe-/Familien-/Lebens-/Erziehungs-Beratungsstelle	Herr Ludger Lüken l.lueken@bistum-os.de	Domhof 2 49074 Osnabrück
Kirchliche Einrichtungen im Bistum Osnabrück	Itebo GmbH Herr Kim Schoen datenschutz@bistum-os.de Aktuell: pco GmbH & Co. KG Herr Philipp Wachhorst datenschutz@bistum-os.de	Dielinger Straße 40 49074 Osnabrück Hafenstraße 11 49090 Osnabrück
Offizialat Vechta	datenschutz nord GmbH Herr Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Schmidt-Straße 88 28217 Bremen
Kirchliche Einrichtung im Offizialat Vechta	Intersoft consulting services AG Herr Stefan Winkel	Beim Strohause 17 20097 Hamburg
Bischöfliches Generalvikariat Hildesheim	datenschutz nord GmbH Herr Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Kirchliche Einrichtungen im Bistum Hildesheim	datenschutz nord GmbH Herr Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Erzbischöfliches Generalvikariat Hamburg	Itebo GmbH Herr Kim Schoen dsb@itebo.de	Dielinger Straße 40 49074 Osnabrück
Kirchliche Einrichtungen im Erzbistum Hamburg	datenschutz nord GmbH Herr Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen

6.2. Auszug Querschnittsprüfung Kindertagesstätten

Allgemeine Infos

1. Wie lautet die genaue Bezeichnung der Einrichtung? Bitte – wenn nötig – ergänzen oder korrigieren!
2. Geben Sie bitte – falls vorhanden – die Homepage der Einrichtung an.
3. Zu welchem (Erz-)Bistum gehört die Einrichtung?
4. Wer steht als Ansprechpartner für Rückfragen zur Verfügung?
5. Welche Organisation ist Träger der Einrichtung? Bitte – wenn nötig – ergänzen oder korrigieren!
6. Wie viele Mitarbeiter hat die Einrichtung? Bitte geben Sie die Zahl aller mitarbeitenden Personen inklusive Ehrenamtlicher, BufDi, FSJ, Praktikanten usw. an.
7. Wie viele Kinder werden in der Einrichtung betreut?
8. Werden Kinder im Rahmen von Inklusionsmaßnahmen betreut?
9. Wo liegt die Einrichtung

Betrieblicher DSB

10. Wurde für Ihre Einrichtung ein betrieblicher Datenschutzbeauftragter benannt?
11. Warum wurde ggf. kein betrieblicher Datenschutzbeauftragter benannt?
12. Bitte geben Sie die dienstlichen Kontaktdaten des betrieblichen Datenschutzbeauftragten an:
13. Wurde der betriebliche Datenschutzbeauftragte der zuständigen Datenschutzaufsicht gemeldet?
14. Art des betrieblichen Datenschutzbeauftragten: (intern/extern)
15. Welche Aufgaben übernimmt Ihr betrieblicher Datenschutzbeauftragter? (Mehrfachauswahlmöglich)

Datensicherung

16. Wie viele Endgeräte haben Sie in Betrieb? Um die Erfüllung datenschutzrechtlicher Anforderungen in Bezug auf Endgeräte wie Desktop-PCs, Laptops, Smartphones usw. nachweisen zu können (z.B. Zugangskontrolle und

Patchmanagement), ist es zunächst erforderlich, diese aufzulisten.

17. Welche Speichermedien nutzen Sie im Alltagsbetrieb für die Speicherung personenbezogener Daten? Die Art der Speichermedien kann Einfluss auf die zu treffenden Maßnahmen zum Schutz dieser Medien (z.B. Aufbewahrung) haben. (Mehrfachauswahl möglich)
18. Führen Sie regelmäßig Datensicherungen durch?
19. Wie oft führen Sie Datensicherungen durch?
20. Warum führen Sie ggf. keine Datensicherung durch?
21. Auf welchen Speichermedien werden Ihre Datensicherungen gespeichert? Die Art der Speichermedien kann Einfluss auf die zu treffenden Maßnahmen zum Schutz dieser Medien (z.B. Lagerung) haben. (Mehrfachauswahl möglich)

Virenscanner

22. Setzen Sie Virenscanner ein?
23. Wie oft wird der Virenscanner aktualisiert?
24. Welche(n) Virenscanner setzen Sie ein?

Datenspeicher

25. Wie viele externe/mobile Datenspeicher nutzen Sie?
26. Wo und wie werden die Endgeräte und die externen Datenspeicher aufbewahrt, wenn diese nicht benutzt oder beaufsichtigt werden (insb. außerhalb der Dienstzeiten)?
27. Nutzen Sie einen Server (intern oder extern) als zentrales System (z.B. zur Datenspeicherung oder für Anwendungen)? Werden z.B. Daten zentral auf einem Server gespeichert oder sind diese auf die eingesetzten Geräte „verteilt“?
28. Durch wen wird der Server betrieben? (Mehrfachauswahl möglich)
29. Durch wen wird der Server gewartet? (Mehrfachauswahl möglich)

Zugangsschutz

30. Wie ist der Zugang zu den Betriebssystemen geschützt? (Mehrfachauswahl möglich)
31. Gibt es eine systemseitige Automatik für die Änderung der Passwörter für den Zugang zum Betriebssystem?

32. Wie oft wird ggf. das Passwort geändert?

Verzeichnis von Verarbeitungstätigkeiten

33. Ist für Ihre Einrichtung ein Verzeichnis von Verarbeitungstätigkeiten vorhanden?

34. Wie stellen Sie die Aktualität des Verzeichnisses sicher?

35. Wer führt das Verzeichnis von Verarbeitungstätigkeiten

36. Sofern eine Verarbeitung auf die Rechtsgrundlage der "Einwilligung" gestützt wird, wie wird die Einwilligungserklärung erteilt? (Mehrfachauswahl möglich)

37. Wie werden eingeholte Einwilligungen dokumentiert? (Mehrfachauswahl möglich)

Informationspflicht

38. Wie kommen Sie Ihren Informationspflichten in Bezug auf Ihre Verarbeitungstätigkeiten nach? (Mehrfachauswahl möglich)

39. Sind die Mitarbeiter zur datenschutzkonformen Verarbeitung personenbezogener Daten in Ihrem Arbeitsbereich sensibilisiert, geschult und verpflichtet worden?

40. Zu welchem Zeitpunkt führen Sie die Verpflichtung durch?

41. Wie oft werden die Mitarbeiter auf die Verarbeitung von personenbezogenen Daten hin sensibilisiert/geschult?

Datenschutzverletzungen

42. Wenn bei uns Datenschutzverletzungen festgestellt werden, ... Unter Datenschutzverletzungen im Sinne dieser Frage sind sämtliche "Datenpannen" (z.B. Versand von Unterlagen an den falschen Empfänger, Veröffentlichung vertrauenswürdiger Informationen, Veröffentlichung von Fotos ohne Einwilligung, Schadsoftwarebefall mit nachfolgendem Verlust personenbezogener Daten, etc.) zu verstehen, unabhängig von einer Meldepflicht an die Datenschutzaufsicht. (Mehrfachauswahl möglich)

Private Endgeräte

43. Benutzen Mitarbeiter private Endgeräte zu dienstlichen Zwecken?

44. Welche Regelungen haben Sie zur Nutzung von privaten Endgeräten zu

dienstlichen Zwecken getroffen? Regelungen könnten z.B. in Form von Dienstanweisungen oder Dienstvereinbarungen bestehen. Bitte fassen Sie den Inhalt eventueller Bestimmungen/Vereinbarungen stichwortartig zusammen.

Löschen von Daten

45. Haben Sie für alle Datenarten festgelegt, wie lange diese aufbewahrt werden müssen (gesetzliche oder betriebliche Gründe)?

46. Haben Sie Regeln und Verfahren, wie Sie mit zu löschenden Daten umgehen? Daten sind zu löschen, wenn ihre Verarbeitung durch den Fristablauf der Zweckbestimmung nicht mehr rechtmäßig ist. (Mehrfachauswahl möglich)

47. Existiert ein Löschkonzept, das auch das Löschen aus dem Langzeitregister (internes Archiv) und von Datensicherungen regelt?

48. Wie stellen Sie sicher, dass auf ausgemusterten Endgeräten keine personenbezogenen Daten mehr gespeichert sind?

Datensicherheit

49. Sind alle Festplatten (interne und externe) Ihrer Einrichtung verschlüsselt?

50. Mit welcher Software führen Sie die Festplattenverschlüsselung durch?

51. Sind alle weiteren digitalen Datenträger (z.B. USB-Sticks, SD-Karten) mit personenbezogenen Daten verschlüsselt?

52. Warum sind die digitalen Datenträger mit personenbezogenen Daten ggf. nicht verschlüsselt? (Mehrfachauswahl möglich)

53. Kopieren Sie personenbezogene Daten auf externe Datenspeicher? (Festplatten, USB Sticks, SD-Karten)

Technische und Organisatorische Maßnahmen

54. Welche Vorkehrungen sind zur Zutrittskontrolle zum Gebäude getroffen? Hierunter versteht man Maßnahmen, die den Zutritt zu den Räumlichkeiten der Datenverarbeitung beschränken und kontrollieren. (Mehrfachauswahl möglich, bitte geben Sie nur die bereits umgesetzten Maßnahmen an.)

55. Welche Vorkehrungen sind zur Zugangskontrolle zu den Rechnern/Endgeräten (Anmeldung) bzw. zur Zugriffskontrolle auf die Anwendungsdaten (Berechtigungen) getroffen? Dies sind Maßnahmen, die auf der zweiten

Stufe den Zugang zu Datenverarbeitungssystemen verhindern, nachdem die erste Stufe der Zutrittskontrolle überwunden wurde, sowie Maßnahmen, die Nutzern den Zugriff auf oder die Löschung von bestimmten Daten erlauben. (Mehrfachauswahl möglich, bitte geben Sie nur die bereits umgesetzten Maßnahmen an.)

56. Wie wird die Weitergabe von Daten kontrolliert? Gemeint sind Maßnahmen, die die Integrität und Vertraulichkeit personenbezogener Daten sowohl bei elektronischen Übermittlungsvorgängen als auch beim Transport der Datenträger sicherstellen. (Mehrfachauswahl möglich, bitte geben Sie nur die bereits umgesetzten Maßnahmen an.)

57. Wird die Tätigkeit von Auftragsverarbeitern kontrolliert? (Bitte nennen Sie nur bereits umgesetzte Maßnahmen.)

58. Wie kontrollieren Sie die Eingabe und das Löschen von personenbezogenen Daten? Dies sind Maßnahmen, die nachträgliche Feststellungen ermöglichen, ob und durch wen personenbezogene Daten in Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind. (Mehrfachauswahl möglich, bitte nennen Sie nur bereits umgesetzte Maßnahmen.)

59. Wie werden die permanente Verfügbarkeit bzw. die Wiederherstellung der Daten sichergestellt? Gemeint sind Maßnahmen zur Verhinderung eines ungewollten Datenverlustes sowie zur Wiederherstellung von Daten. (Mehrfachauswahl möglich, bitte nennen Sie nur bereits umgesetzte Maßnahmen.)