Katholische
Datenschutzaufsicht Nord

7. Jahresbericht

2020

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/

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

Wer hätte, außer den entsprechenden Fachleuten, gedacht, dass unser aller Leben einmal durch eine weltweite Pandemie so eingeschränkt und verändert wird, wie es seit Beginn des Jahres 2020, und ein Ende ist bis heute nicht in Sicht, der Fall ist. Das Coronavirus hat alle Lebensbereiche beeinflusst und natürlich auch die Arbeit im Bereich der Katholischen Datenschutzaufsicht Nord maßgeblich geprägt.

Nicht nur die Fragen zu Homeoffice, Hygienekonzepten oder die Beschaffung von Masken und Desinfektionsmitteln waren relevant, sondern auch der persönliche Umgang mit den Kolleginnen und Kollegen, die bis dato „notwendige“ Präsenz bei Gesprächen und Sitzungen, die kollegial freundschaftliche Gestaltung der Pausen und das soziale Miteinander sind nachhaltigen Veränderungen unterzogen worden. Wir verabschieden uns nicht mehr mit „freundlichen Grüßen“, sondern fordern den Anderen auf „gesund zu bleiben“. Im Übrigen versuchen wir, wie alle anderen, Abstand zu halten, ohne eine soziale Distanz zu bewirken, und uns den Aufgaben zu widmen, für die wir als kirchliche Datenschutzaufsicht zuständig sind.

Der Schwerpunkt unserer Tätigkeit war pandemiebedingt „Bremen“-orientiert, denn mit wenigen Ausnahmen hat es keine auswärtigen Vor-Ort-Termine gegeben. Das heißt nicht, dass es keine Prüfungen gegeben hat, aber es bedeutet, dass die erforderlichen Prüfungen im Wesentlichen anhand von Aktenlagen durchgeführt worden sind.

Die im Zusammenhang mit der Corona Pandemie entstandenen Fragen nach „mobilen“ Arbeitsplätzen, Homeoffice, Kommunikationstools, Verarbeitung von personenbezogenen Daten (Gesundheitsdaten) beim Umgang mit der Pandemie, bis hin zur Verarbeitung von personenbezogenen Daten im Rahmen von Gottesdiensten und Beerdigungen oder etwa Anfragen aus der Mitarbeitervertretung, waren mehrheitlich Gegenstand der Fragen, Beratungen und Beschwerden, die im Laufe des Berichtzeitraums zu bearbeiten waren. Daneben war ein deutlicher Anstieg der auf die verstärkte Nutzung von digitaler Kommunikation zurückzuführender Datenschutzverletzungen wahrzunehmen. Das vermehrte Offenlegen von personenbezogenen Daten, etwa durch falsche Zuordnung von E-Mail-Anschriften macht dies deutlich.

Aber auch jenseits von Corona hat es Vorgänge gegeben, die für die Arbeit der Katholischen Datenschutzaufsicht Nord von Bedeutung waren, und dies meint nicht nur die Umbenennung der Behörde in „Katholische Datenschutzaufsicht Nord“. Letzteres ist auch der Vereinheitlichung der Bezeichnungen der katholischen Aufsichtsbehörden geschuldet und dient damit der Orientierung der Betroffenen im Hinblick auf die Wahrnehmung Ihrer Rechte. Gemeint ist, dass sich im staatlichen und kirchlichen Bereich wesentliche Veränderungen ergeben haben, die Auswirkungen auf das kirchliche Datenschutzrecht, und damit auf die Grundlage unserer Arbeit hatten.

Die Grundlage für die Datenübermittlung in die Vereinigten Staaten von Amerika, das Privacy Shield, ist am 16. Juli 2020, durch ein Urteil des EuGHs („Schrems II“) für ungültig erklärt worden. Zusätzlich müssen die Einrichtungen bei der Verwendung von Standarddatenschutzklauseln künftig bei der Übermittlung personenbezogener Daten in ein Drittland überprüfen, ob dort - evtl. auch durch zusätzliche vertragliche Vereinbarungen - ein angemessenes Datenschutzniveau herrscht oder hergestellt werden kann.

Die Europäische Union (EU) und Großbritannien haben sich auf ein Handelsabkommen geeinigt, das den „Brexit“ regeln soll. Dieses Abkommen, welches offiziell als "Handels- und Kooperationsabkommen zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits" bezeichnet wird, sieht u.a. eine Übergangsfrist in Bezug auf den Transfer von personenbezogenen Daten von der EU nach Großbritannien vor. Hinsichtlich der Verarbeitung von personenbezogenen Daten kirchlicher Einrichtungen in Großbritannien und Nordirland besteht zukünftiger Handlungsbedarf.

Im kirchlichen Bereich wurde eine Verfahrensregelung für die katholischen Datenschutzaufsichten verkündet. Mit dem Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG) steht den Aufsichten nunmehr eine ergänzende gesetzliche Grundlage für ihr behördliches Handeln zur Erfüllung ihrer Aufgaben aus Kapitel 6 und Kapitel 7 des KDG zur Verfügung.

Die Katholische Datenschutzaufsicht Nord ist zuständig für die Gebiete des Erzbistums Hamburg, der Bistümer Osnabrück und Hildesheim und des Offizialatsbezirks

Vechta in Oldenburg. Die Leitung der Datenschutzaufsicht obliegt dem Diözesandatenschutzbeauftragten.

Die Aufgaben der Datenschutzaufsicht sind dabei gesetzlich in § 44 KDG geregelt und entsprechen damit den Bestimmungen des Kapitel VI DS-GVO. Die im Rahmen der gemeinsamen Datenschutzaufsicht für den norddeutschen Bereich zuständigen Institutionen sind gehalten, die Aufsichtsbehörde mit den dafür erforderlichen Ressourcen auszustatten.

Auch im fünften Jahr komme ich gerne der mir durch die (Erz-)Bischöfe von Hamburg, Osnabrück und Hildesheim und dem Leiter des Bischöflich Münsterschen Offizialats in Vechta erneut 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 2020 lege ich nachstehend vor. Wie üblich werde ich neben einer zusammenfassenden Darstellung der Entwicklung des Datenschutzrechtes auf europäischer, deutscher und kirchlicher Ebene auch exemplarisch auf wesentliche Vorkommnisse in dem Berichtszeitraum hinweisen, die von allgemeiner Bedeutung für die Dienststellen in meinem Tätigkeitsbereich sein können.

Bremen, im Juli 2021

Andreas Mündelein
Diözesandatenschutzbeauftragter

1. Die Entwicklung des Datenschutzrechts

1.1. Europarecht

1.1.1. Evaluation der Europäische Datenschutz-Grundverordnung (DS-GVO)

Die DS-GVO wird regelmäßig bewertet und überprüft. Dafür soll die Regelung in einem Zeitraum von vier Jahren regelmäßig evaluiert werden. Erstmalig erfolgte dies im Mai 2020. Die EU-Kommission hat im Juni 2020 dem Europäischen Rat einen ersten umfassenden Bericht vorgelegt, der veröffentlicht worden ist. Darin wird die Regelung grundsätzlich positiv bewertet, auch wenn eine europaeinheitliche Umsetzung noch nicht vollständig in allen Bereichen abgeschlossen ist.

1.1.2. Datentransfers in Drittländer (EU-U.S. Privacy Shield)

Am 16. Juli 2020 verkündeten der Europäische Gerichtshof das Urteil in der Sache „Schrems II“ und erklärte den „EU-U.S. Privacy Shield“ für ungültig. Zur Urteilsbegründung führt der Gerichtshof aus, dass das Datenschutzniveau der EU und damit der durch die DS-GVO festgelegte und geforderte Schutz für personenbezogene Daten bei einer Übermittlung in die USA durch das Datenschutzabkommen („Privacy Shield“) nicht gewährt werden kann.

In den Fällen, in denen Verantwortliche die Datenübermittlungen in die USA auf das nun nicht mehr gültige Datenschutzabkommen zwischen der EU und den USA gestützt haben, müssen diese nun handeln, da sie andernfalls personenbezogene Daten ohne Rechtsgrundlage in ein Drittland transferieren.

Hinsichtlich eines Drittlandtransfers wurden die Standarddatenschutzklauseln der EU-Kommission nach Art. 46 Abs. 2 lit. c) und d) DS-GVO nicht für ungültig erklärt. 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. Nur in diesem Fall können die Standarddatenschutzklauseln eine Rechtsgrundlage für die Übermittlung personenbezogener Daten in ein Drittland darstellen. Daher obliegt den Verantwortlichen eine Rechtsprüfung, in-

wiefern das Datenschutzniveau im jeweiligen Drittland dem der DS-GVO entspricht bzw. dort von den Vertragspartnern eingehalten werden kann.

Das Urteil betrifft für die Anwendung der Standarddatenschutzklauseln alle Datenübertragungen in Drittländer, die keinem Angemessenheitsbeschluss nach Art. 45 DS-GVO unterfallen. Durch den Wegfall des „Privacy Shield“ fehlt ein solcher Beschluss jetzt auch für die USA. Nach den Ausführungen des EuGHs ist für die USA auch der Einsatz von Standarddatenschutzklauseln nicht mehr möglich.

1.1.3. Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)

Zu der vorgenannten Verordnung hatte ich schon mehrfach berichtet und auf die Notwendigkeit einer Regelung hingewiesen. Mit der Übernahme der EU-Ratspräsidentschaft durch die Bundesregierung im Juli des letzten Jahres sollte die ePrivacy Verordnung nun endgültig auf den Weg gebracht werden. Streitigkeiten um die Nutzung von Cookies und Metadaten sollten beendet und eine gemeinsame Entscheidungsgrundlage für die EU-Mitgliedstaaten geschaffen werden. Dies ist allerdings nicht gelungen und wann die ePrivacy Verordnung in Kraft treten wird, ist weiterhin unklar.

1.1.4. Brexit

Am 24. Dezember 2020 haben sich die Europäische Union (EU) und Großbritannien auf ein Handelsabkommen geeinigt. In dem am 26. Dezember 2020 veröffentlichten und noch vorläufigen Handelsabkommen findet sich auch eine Übergangslösung in Bezug auf den Transfer von personenbezogenen Daten von der EU nach Großbritannien. Im Artikel FINPROV.10A Abs. 1 des „Handels- und Kooperationsabkommen zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einer-seits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits“ heißt es hierzu, dass der Transfer von personenbezogenen Daten von der EU nach Großbritannien für einen bestimmten Zeitraum nicht als Übermittlung in ein Drittland gelten soll. Dieser bestimmte Zeitraum soll am 1. Januar 2021 beginnen und gemäß Artikel FINPROV.10A Abs. 4 dann enden, wenn entweder ein Angemessenheiten Beschluss der Europäischen Kommission vorliegt oder vier Monate

nach Beginn der Übergangsphase bzw. sechs Monate nach Beginn der Übergangsphase, sofern keine der Vertragsparteien widerspricht.

1.1.5. Nutzung von Microsoft-Produkten und -Services

Im vorausgegangenen Tätigkeitsbericht war berichtet worden, dass der European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski im April 2019 Untersuchungen begonnen hatte, ob die vertraglichen Verhältnisse, die zwischen den EU-Einrichtungen und Microsoft bezgl. der von den EU-Einrichtungen (EUIs) eingesetzten Software geschlossen worden sind, den (datenschutz-) rechtlichen Anforderunggen genügen.

Am 2. Juli 2020 hat das The Hague Forum zum zweiten Mal getagt. Im Zuge dessen hat der EDPS ein Papier[1] vorgestellt und veröffentlicht, in dem die Ergebnisse dieser Untersuchung publiziert worden sind und in den Feststellungen und Empfehlungen zur Nutzung von Microsoft-Produkten und -Services durch EUIs gegeben werden; Gegenstand waren die Inter-Institutional Licensing Agreement (ILA).

Im Ergebnis hat die Datenschutzbehörde der europäischen Union die Nutzung von Microsoft-Produkten und -Diensten unter den gegebenen Voraussetzungen als nicht unproblematisch angesehen[2].

1.2. Bundesrecht

Neben den im Zusammenhang mit der Pandemie relevanten Veränderungen des Bundesinfektionsschutzgesetzes waren auf der Bundesebene der Brexit und dessen Auswirkungen auf den Datenaustausch mit Großbritannien ebenso relevant wie die Umsetzung des Schrems II Urteils des Europäischen Gerichtshofs. Daneben sind die Digitalisierung des Gesundheitswesens und das neue Patientendaten-Schutz-Gesetz zu erwähnen.

Von besonderer Bedeutung waren gleichwohl die im Zusammenhang mit der Bekämpfung der Pandemie getroffenen gesetzlichen Bestimmungen, weil diese unmittelbaren Auswirkungen auf die kirchlichen Einrichtungen hatten.

[1] https://edps.europa.eu/sites/default/files/publication/20-07-02_edps_paper_euis_ microsoft_ contract_investigation_en.pdf
[2] https://www.kdsa-nord.de/20200714

1.2.1. Gesetze zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite

Das Gesetz vom 27. März 2020 ist ein Artikelgesetz, das anlässlich des Ausbruchs der durch das neuartige Coronavirus SARS-CoV-2 verursachten COVID-19-Pandemie in Deutschland erlassen wurde.

In Ausführung des Infektionsschutzgesetzes, das im Rahmen einer Gefahrenabwehr dem Schutz vor Ansteckung mit einer infektiösen Krankheit dient, ist das Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite im Bundestag am 25. März 2020 beschlossen worden und nach Zustimmung des Bundesrates am 27. März am 28. März 2020 in Kraft getreten. Mit dem Gesetz sind weitreichende Eingriffs- und Verordnungsbefugnisse, bis hin zu Einschränkungen der Grundrechte der Bürgerinnen und Bürger, für das Bundesministerium für Gesundheit (BMG) geregelt worden. Erweitert wurde das Gesetz durch das Zweite Änderungsgesetz, das am 23. Mai 2020 in Kraft getreten ist und weitere Anpassungen des Infektionsschutzgesetzes enthalten hat und das dritte Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite vom 18. November 2020, mit dem u.a. weitere Meldepflichten und Übermittlungen von personenbezogenem Daten geregelt worden sind.

1.2.2. Landesrechtliche Regelungen

Die nachstehenden Regelungen waren (sind) die Grundlagen für den Umgang mit der Pandemie mit unmittelbaren Auswirkungen auf die kirchlichen Bereiche in den norddeutschen Diözesen.

Auf der Grundlage des § 32 des Infektionsschutzgesetzes sind die Länder ermächtigt, Maßnahmen zur Bekämpfung von übertragbaren Krankheiten zu treffen. Im Rahmen der Pandemie haben die im Bereich der Katholischen Datenschutzaufsicht Nord liegenden Bundesländer davon Gebrauch gemacht. Diese waren für den kirchlichen Bereich als Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten von besonderer Bedeutung.

Die Regelungen sind entsprechend des Pandemieverlaufs jeweils aktualisiert worden und zeigen insoweit nur einen Zwischenstand.

Hamburg: Verordnung zur Eindämmung der Ausbreitung des Coronavirus SARS-CoV-2 in der Freien und Hansestadt Hamburg (Hamburgische SARS-CoV-2-

Eindämmungsverordnung – HmbSARS-CoV-2-EindämmungsVO (gültig ab 7. August 2020)

Niedersachsen: Niedersächsische Verordnung zur Neuordnung der Maßnahmen gegen die Ausbreitung des Corona-Virus SARS-CoV-2 (Niedersächsische Corona-Verordnung) vom 10. Juli 2020

Mecklenburg-Vorpommern: Änderung der Verordnung der Landesregierung zum dauerhaften Schutz gegen das neuartige Coronavirus in Mecklenburg-Vorpommern vom 12. Juni 2020

Schleswig-Holstein: Landesverordnung zur Bekämpfung des Coronavirus SARS-CoV-2 (Corona-Bekämpfungsverordnung – Corona-BekämpfVO) vom 26. Juni 2020 (Konsolidierte Lesefassung einschließlich der ab dem 10. August 2020 gelten-den Änderungen)

Bremen: Dreizehnte Verordnung zum Schutz vor Neuinfektionen mit dem Coronavirus SARS-CoV-2 (Dreizehnte Coronaverordnung) (gültig ab 11 August 2020)

1.3. Datenschutzrecht der Kirche

1.3.1. Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG)[3]

Nach dem kirchlichen Datenschutzgesetz (§ 42 ff. KDG) sind unabhängige Datenschutzaufsichten einzurichten. Zur Erfüllung ihrer Aufgaben können sie in die Verarbeitung personenbezogener Daten durch kirchliche Stellen eingreifen. Das Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG) regelt nun das Verwaltungsverfahren im Bereich des kirchlichen Datenschutzes und bietet damit die erforderliche, mit dem kanonischen Recht vereinbarte Rechtsgrundlage für die Tätigkeit der kirchlichen Datenschutzaufsichten.

In Anlehnung an das Verwaltungsverfahrensgesetz (VwVfG) des Bundes und der Länder enthält das KDS-VwVfG Regelungen, die eine allgemeine Arbeitsgrundlage für die Tätigkeit der Datenschutzaufsichten darstellen (Verfahrensgrundsätze, Zu-

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

standekommen und Bestandskraft von Verwaltungsakten, Verwaltungszustellung), Regelungen zur Anwendung des Gesetzes über Ordnungswidrigkeiten (OWiG) als Verfahrensgrundlage für den Erlass von Bußgeldern sowie Regelungen zur Durchsetzung und Vollstreckung von Bußgeldbescheiden und anderen Anordnungen der kirchlichen Datenschutzaufsichten.

1.3.2. Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft im Bistum Hildesheim

Am 15. Februar 2020 ist die Anordnung zum Schutz personenbezogener Daten in katholischen Schulen (SchulDSO) im Bistum Hildesheim in Kraft getreten. 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.

Durch die Regelung wird unter anderem der Bereich des Homeoffice für die Lehrkräfte und die Mitnahme von Daten aus der Schule (vgl. § 7 d. O) sowie die Weitergabe von Daten im Bereich der Ganztagsbetreuung (vgl. § 6 Abs. 8 d.O) auf eine rechtssichere Basis gestellt. Eher unglücklich ist dagegen die Formulierung des § 6 Abs. 7 d. O. „an sonstige öffentliche und nichtöffentliche Stellen können Daten übermittelt werden, sofern dies zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist“. Die Formulierung ist sehr weit und birgt das Risiko der Weitergabe von Daten aus dem Schulbereich (Bsp. Bankdaten der Eltern gegenüber einem Inkassounternehmen) an nichtöffentliche Stellen zur Erfüllung deren Aufgaben, die gegebenenfalls mit dem Zweck der unmittelbaren Regelung nicht im Zusammenhang steht.

1.3.3. Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens« (Seelsorge-PatDSG)

Die Diözesandatenschutzbeauftragten haben die Krankenhausseelsorge schon immer als eine wichtige Aufgabe der Kirche angesehen. Schon deshalb ist es zu begrüßen, dass die Erfüllung dieser Aufgabe auf einer gesetzlichen Grundlage erfolgt, auch wenn das Ergebnis des Gesetzes nicht in allen Fällen auf die uneingeschränkte Zustimmung auch meiner Behörde gestoßen ist.

Das Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens (Seelsorge-PatDSG) ist eine auf die Seelsorge beschränkte Nachfolgeregelung zu den mit der Einführung des KDG ausgelaufenen Patientendatenschutzordnungen.

Das Gesetz nimmt die veränderten Formen der Krankenhausseelsorge zum Anlass und unterscheidet zwischen verschiedenen Seelsorgekonzepten: der implementierten Krankenhausseelsorge, der nicht implementierten Krankenhausseelsorge durch eine mit Seelsorgeauftrag der zuständigen kirchlichen Stelle ausgestattete Person sowie der Seelsorge durch einen (ehrenamtlichen) Besuchsdienst der Kirchengemeinde des Patienten.

Für den kirchlichen Datenschutz bedeutet das eine wesentliche Veränderung. Der bisherige Grundsatz der seelsorglichen Zuwendung, vordergründig auf Wunsch des Patienten, und damit verbunden die Verarbeitung seiner personenbezogenen Daten nur mit dessen Einwilligung, ist dem veränderten Verständnis der Seelsorge im Krankenhaus im Sinne einer ganzheitlichen Behandlung des Patienten gewichen. Die Seelsorge versteht sich nunmehr als Ergänzung zur medizinischen, pflegerischen und sozialen Behandlung, und will einen spirituellen und ethischen Beitrag bei der Behandlung leisten (sog. spiritual care).

Die personenbezogenen Daten der Patienten, z.B. der Name, die Konfession, die Station oder das Aufnahmedatum, dürfen daher, zumindest dann, wenn die Seelsorge als „konzeptionell integrierte Seelsorge“ im Krankenhausalltag organisiert ist, ohne ausdrückliche Einwilligung an die Krankenhausseelsorge weitergegeben werden.

Aber auch bei der anderen Variante, die keine konzeptionell integrierte Seelsorge vorsieht (was auch immer das bedeutet), kann ohne Einwilligung des Patienten eine Offenlegung seiner Daten gegenüber der mit einem Seelsorgeauftrag ausgestatteten Person erfolgen. Es sei denn, der Patient widerspricht aktiv der Inanspruchnahme der Seelsorge.

Nur noch die Weitergabe der Patientendaten an die Heimatgemeinde erfordert die Zustimmung des Betroffenen.

Bisher galten für die Weitergabe der Religionszugehörigkeit und die „Einwilligung“ für den Besuch der Krankenhausseelsorge grundsätzlich die verfassungsrechtlichen Bestimmungen des Grundgesetzes in Verbindung mit den entsprechenden Ordnungen.

„Soweit das Bedürfnis nach Gottesdienst und Seelsorge im Heer, in Krankenhäusern, Strafanstalten oder sonstigen öffentlichen Anstalten besteht, sind die Religionsgesellschaften zur Vornahme religiöser Handlungen zuzulassen, wobei jeder Zwang fernzuhalten ist (vgl. Art. 140 GG i.V.m. Art. 141 WRV)“.

Die Folge daraus war, dass das Krankenhaus die Religionszugehörigkeit der Patienten abfragen darf (muss), wobei auf die Freiwilligkeit der Angabe hinzuweisen war. Darüber hinaus war bei dem Patienten eine Einwilligungserklärung einzuholen für die Weiterleitung an den zuständigen Krankenhausseelsorger. Hierdurch wurde die Verpflichtung des Grundgesetzes „jeden Zwang fernzuhalten“ gewährleistet.

Durch die Integration der Seelsorge im Sinne einer ganzheitlichen Behandlung des Patienten in den Krankenhausalltag, mit der Folge der Weitergabe u.a. der Konfessionszugehörigkeit, ohne die Einwilligung des Patienten, wird der Grundsatz, „jeden Zwang zur Seelsorge“ fernzuhalten konterkariert.

Man könnte zwar daran denken, dass ein Patient bei einer bewussten Entscheidung für ein katholisches Krankenhaus und unter Berücksichtigung der abzuschließenden vertraglichen Vereinbarungen eine entsprechende Entscheidung auch für die Seelsorge treffen will. Die Frage ist nur was mit den Patienten geschieht, die im Rahmen eines Versorgungsauftrages der Einrichtung schlicht eingeliefert werden.

In der anderen Variante wird der Patient „gezwungen“, sich mit der Wahrnehmung der Seelsorge aktiv auseinanderzusetzen. Der Patient muss reagieren, wenn er keine Seelsorge in Anspruch nehmen möchte. Das ist aber nach diesseitigem Verständnis mit dem kirchlichen Datenschutzrecht nicht kompatibel. Der Betroffene muss nicht erklären, dass er im Hinblick auf die Verarbeitung seiner Daten etwas nicht will, sondern derjenige, der die Daten verarbeiten möchte, braucht eine freiwillige und informierte Einwilligung des Patienten.

Ob das Seelsorge-PatDSG insoweit geeignet ist, „ohne jeden Zwang“ (s.o. Art 141 WRV) die Seelsorge in einem katholischen Krankenhaus zu organisieren, ist auch im Rahmen des Gesetzgebungsverfahrens durch die Datenschutzaufsichten mehrfach problematisiert worden.

Bisher hat in meinem Bereich allein das Erzbistum Hamburg das Gesetz umgesetzt.

1.3.4. Pandemieregelungen der Diözesen

Im Wesentlichen haben die (Erz-)Bistümer im Norden durch Verlautbarungen der Bischöfe oder durch Anordnung und Handlungsempfehlungen der Generalvikare auf die Pandemie reagiert und unter Berücksichtigung der jeweiligen Landesverordnungen die notwendigen Schritte gegen die Weiterverbreitung des Coronavirus in den Bistümern unternommen.
Mit Videokonferenzsystemen konnte in der Pandemiesituation ein persönlicher Kontakt und damit eine Gefährdung vermieden werden, wenn die Mitarbeiter vermehrt aus einer mobilen - oder aus der Homeoffice Situation gearbeitet haben, und die notwendige Kommunikation mithilfe der technischen Mittel erfolgte. Darüber hinaus waren auf Anordnung der Bistümer die Dienstreisen und die Vor-Ort-Terminen zu reduzieren oder einzustellen.

Uns erreichten insoweit zunehmend Anfragen im Hinblick auf ein mit dem kirchlichen Datenschutzrecht kompatibles Videosystem.

Aufgrund der Menge an Online Meeting Services war es nicht möglich, eine allgemeinverbindliche Lösung anzubieten, und aus Praktikabilitätserwägungen zudem auch nicht immer zielführend. Es wurde daher eine Hilfestellung formuliert, die auf unserer Homepage verlinkt war. Dieses Dokument soll als Entscheidungshilfe dienen, sich – in Abhängigkeit der jeweils vorliegenden Situation – für einen passenden Anbieter zu entscheiden zu können.

Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben ähnlich reagiert und eine Orientierungshilfe zum Einsatz von Videokonferenzsystemen erarbeitet, die im Oktober 2020 veröffentlicht wurde.

Mit der Verbreitung des Corona-Virus und der dadurch ausgelösten Sars-Cov-2-Infektion waren nahezu zeitglich auch die Anzahl der Betrugsversuche über elektronische Medien stark angestiegen. Zu nennen sind exemplarisch dubiose E-Mail-Kampagnen mit Spendenaufrufen, aber auch die Einrichtung ebensolcher Webpräsenzen, wie z. B. die Nachahmung der Internetseiten des Wirtschaftsministeriums in Nordrhein-Westfalen, über die die Soforthilfe beantragt werden kann.

Die Corona-Pandemie hat zu Einschränkungen und Änderungen nicht zuletzt im Berufsalltag geführt. Geänderte Arbeitsbedingungen, Homeoffice (z. T. mit gleichzeitiger Kinderbetreuung) und nicht zuletzt die allgemeine Unsicherheit haben zu Ausnahmesituationen und Verunsicherung geführt; die bspw. im Rahmen von Phishing-Kampagnen ausgenutzt worden sind. [4]

Doch das durfte nicht dazu führen, dass deshalb der erforderliche Datenschutz vernachlässigt wird. Wir haben uns von dem Gedanken leiten lassen, dass situativ und ohne Aufgabe unserer datenschutzrechtlichen Überzeugungen der Grundsatz der Praktikabilität bei der Lösung der mit der Pandemie entstandenen Herausforderungen nicht in Vergessenheit geraten ist.

Dabei konnte aber nicht jede Hürde übersprungen werden. Beispielsweise die Verwendung des Messengers WhatsApp. Auch wenn deren Gebrauch im privaten Bereich nach wie vor hoch ist, ist er für die dienstliche Kommunikation ungeeignet und datenschutzrechtlich unzulässig. Das hat auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) noch einmal in einem Schreiben an alle Bundesministerien und oberste Bundesbehörden ausdrücklich festgestellt. Das gilt sowohl für die Kommunikation innerhalb der Behörde als auch für die Kommunikation zwischen Behörde und Bürgern.

[4] https://www.kdsa-nord.de/20200416

2. Die Entwicklung des kirchlichen Datenschutzes

2.1. Betriebliche Datenschutzbeauftragte in den Einrichtungen

Wie bereits mehrfach dargestellt, ergibt sich die Verpflichtung der Diözesen, Kirchengemeinden, Kirchenstiftungen und der Kirchengemeindeverbände, ebenso wie die Diözesancaritasverbände und ihre Untergliederungen, einen betrieblichen Datenschutzbeauftragten zu bestellen, aus § 36 Abs. 1 KDG. Dasselbe gilt für Fachverbände, kirchliche Körperschaften und Stiftungen, Anstalten, Werke, Einrichtungen und sonstige kirchliche Rechtsträger (Einrichtungen nach § 3 Abs. 1 lit. b) und c) KDG).

Die gesetzliche Verpflichtung haben die Diözesen und die kirchlichen und caritativen Einrichtungen erfüllt. Die Einrichtungen werden zum überwiegenden Teil im Auftrag der Diözesen und des Offizialats durch professionelle externe Datenschutzbeauftragte betreut.

Die institutionalisierte Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten hat sich bewährt. Die zu diesem Zweck eingerichteten regelmäßigen Treffen haben zur effektiven Umsetzung der datenschutzrechtlichen Belange in den Einrichtungen erheblich beigetragen.

2.2. Kirchliche Datenschutzaufsicht

2.2.1. Die Struktur der Datenschutzaufsicht für die norddeutschen Diözesen

Bekanntermaßen hat die kirchliche Datenschutzaufsicht die in Kapitel VI der DS-GVO niedergelegten Bedingungen zu erfüllen (Art. 91 Abs. 2 DS-GVO (Art. 51, Art. 59 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 Katholische Datenschutzaufsicht Nord ist rechtlich als unabhängige Stelle eigener Art konfiguriert.

Die geplante Umsetzung der rechtlichen Neustrukturierung der Aufsichtsbehörde in eine Körperschaft des öffentlichen Rechts (s. Bericht 2019), die dem Grunde nach

beschlossen ist, ist in der Konkretisierung an der Pandemie gescheitert. Die notwendigen Treffen und Absprachen, die für das späte Frühjahr vereinbart waren, sind ausgefallen und konnten auch nicht über eine andere Form der Kommunikation realisiert werden. Ein neuer Anlauf erfolgt im laufenden Jahr.

Zum Ende des Berichtszeitraums ist die personelle Ausstattung der Aufsichtsbehörde angepasst worden. Das Stellentableau umfasst nunmehr 4 Vollzeitstellen, das Sekretariat inbegriffen.

2.2.2. Statistik und Zahlen

Im Laufe des Berichtszeitraums waren die Anfragen zum kirchlichen Datenschutzgesetz um 38% rückläufig. Das ist nach hiesiger Auffassung nicht zuletzt dem Umstand geschuldet, dass die Professionalisierung der Beratung der Einrichtungen durch entsprechende betriebliche Datenschutzbeauftragte ausgebaut werden konnte. Darüber hinaus hat sich das Gesetz und die zugehörigen Ordnungen nach diesseitiger Wahrnehmung im Bewusstsein der Verantwortlichen etabliert. Dies mag auch ein Grund dafür sein, dass die Meldung von Datenpannen mit 83% erheblich gestiegen ist, während die Anzahl der Beschwerdevorgänge annähernd dem Niveau des Vorjahres entsprach.

Die Anzahl der Prüfungen vor Ort ist pandemiebedingt rückläufig gewesen, weil geplante Termine in den Einrichtungen aus Schutzgesichtspunkten für die Beteiligten größtenteils nicht durchgeführt werden konnten. Demgegenüber ist die Anzahl der „Prüfungen nach Aktenlage“ gestiegen. Aber auch unter Berücksichtigung der im Rahmen der Querschnittsprüfung (s.u.) notwendigen Erhebungen ist insgesamt ein Rückgang um ca. 25% festzustellen. Es bleibt zu hoffen, dass die Pandemie es im nächsten Jahr zulässt, Prüfungstermine vor Ort in den Einrichtungen wieder durchzuführen.

Die Mitarbeiter der Datenschutzaufsicht haben im Berichtszeitraum an 31 Arbeitsgruppen (extern und intern) teilgenommen, die im Wesentlichen als Videokonferenzen durchgeführt wurden.

2.2.3. Konferenz der Diözesandatenschutzbeauftragten

Die kirchlichen Datenschutzaufsichten haben sich im Rahmen einer „Konferenz der Diözesandatenschutzbeauftragten“ mit dem Ziel zusammengeschlossen, eine mög-

lichst einheitliche Anwendung der kirchlichen Datenschutzbestimmungen zu gewährleisten. Sie entsprechen damit den gesetzlichen Vorgaben nach § 46 KDG. Die Konferenz tagt mehrfach im Jahr nach einem abgestimmten Verfahrensablauf. Dazu hat sich die Konferenz eine Geschäftsordnung gegeben, die im Berichtszeitraum noch einmal aktualisiert worden ist (Geschäftsordnung/ 2020).

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, aber ohne eine Entscheidungskompetenz für die Konferenz. Damit ist sichergestellt, dass die gesetzlich normierte Unabhängigkeit der Diözesandatenschutzbeauftragten gewährleistet ist.

In jeweiliger Abstimmung mit der Konferenz sind die nachstehend genannten Informationen auf der Homepage der KDSA – Nord veröffentlicht worden.

- Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Dienstgeber im Bereich der norddeutschen Bistümer im Zusammenhang mit der Corona-Pandemie
- Betrugsversuche zu Zeiten von Corona
- Einsatz neuer Informations- und Kommunikationstechnologien bei Sitzungen der Mitarbeitervertretungen in Zeiten der Corona-Pandemie
- Hinweise zu Online-Meeting Tools
- Best Practices für medizinische Einrichtungen
- EuGH erklärt den Beschluss über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig
- EuGH-Urteil vom 16. Juli 2020 (C-311/18)
- Brexit Handelsabkommen
- Brexit Handelsabkommen II

2.2.4. Kirchliches Datenschutz Modell (KDM)

Der Beschluss der Datenschutzaufsichten der katholischen und evangelischen Kirche, das Standard-Datenschutzmodell (SDM) an die kirchlichen Gegebenheiten und

für die konkrete Anwendung in Form des Kirchlichen Datenschutz Modells anzupassen, wurde im Berichtszeitraum durch eine Projektgruppe weiterverfolgt (s. 6. Tätigkeitsbericht); die Teilnahme der KDSA Nord an dieser Projektgruppe bestand fort.

3. Exemplarische Darstellung von Einzelfragen und Einzelfällen

3.1. Beratung

3.1.1. Temperaturmessungen Krankenhaus Corona

Bereits früh zu Beginn der Corona-Krise erreichte uns die Anfrage, ob es datenschutzrechtlich zulässig sei, an den Haupteingängen von Krankenhäusern eine Echtzeittemperaturmessung zu installieren. Zum Zeitpunkt der Anfrage ging das RKI davon aus, dass lediglich 42 Prozent der betroffenen Personen Fieber als Symptom der COVID-19-Erkrankung entwickeln würden. Zudem wurde geschätzt, dass Patienten bereits 2,5 Tage vor den ersten Symptomen infektiös sind.

Dies führte uns zu dem Ergebnis, dass die Temperaturmessung weder geeignet noch erforderlich ist, um zuverlässige Ergebnisse im Rahmen der Zugangskontrolle zu erhalten. Denn nicht jede erhöhte Körpertemperatur ist, sofern diese denn gegeben ist, auf eine mögliche COVID-19-Erkrankung zurückzuführen. Auch kann nicht zuverlässig ausgeschlossen werden, dass eine Normaltemperatur gleichzeitig auch bedeutet, dass die betroffene Person nicht infektiös ist.

3.1.2. Namenschilder im Krankenhaus

Uns erreichte eine Anfrage zum Tragen von Namensschildern im Krankenhaus. Häufig verlangen Arbeitgeber von den Mitarbeitern, Namensschilder zu tragen, welche den Vor- und Nachnamen der betroffenen Person ausweisen. Insbesondere in Krankenhäusern ist das Tragen von Namensschildern üblich. Durch die Darstellung sowohl des Vor- als auch des Nachnamens besteht jedoch für die betroffenen Personen die oft nicht unbegründete Sorge, dass anhand von Suchmaschinen im Internet weitere Daten, z. B. die Privatanschrift, ermittelt und die betroffenen Personen durch Patienten und/oder Besucher belästigt werden. Die Benennung sowohl des Vor- als auch des Nachnamens ist aus datenschutzrechtlicher Sicht nicht erforderlich und damit unzulässig.

3.1.3. Nutzung von Videokonferenzsystemen

Noch vor Bekanntwerden des sogenannten Urteils „Schrems II“ (EuGH-Urteil vom 16. Juli 2020 (C-311/18) vom 16. Juli 2020 sind wir angefragt worden, welche Videokonferenzsysteme in kirchlichen Einrichtungen genutzt werden können.

Konkret hängt die Wahl des Videokonferenzsystems davon ab, welche personenbezogenen Daten im jeweiligen Szenario verarbeitet werden sollen und ob diese dann durch technische und organisatorische Maßnahmen des eingesetzten Produkts angemessen geschützt sind. Dies hängt zum Teil auch von der eingesetzten Produktversion ab. So sind bspw. an eine Videosprechstunde einer Beratungsstelle aus technischer Sicht andere Ansprüche im Hinblick auf die Sicherstellung der Vertraulichkeit der verarbeiteten Inhalte zu stellen als z.B. bei einer allmorgendlichen Team-besprechung, bei der es um die Verteilung von Arbeitsaufgaben geht.

Grundsätzlich ist bei Videokonferenzsystemen oder auch nur bei Chatsystemen auf den Standort der Datenspeicherung und -verarbeitung sowie auf die Zugriffmöglichkeiten des Anbieters zu achten. Um diese kritischen Punkte zu umgehen, kann auch - je nach den gegebenen Voraussetzungen - über eine selbst gehostete Software-Lösung nachgedacht werden.

Sofern die selbst gehostete Lösung nicht in Betracht kommt, ist es erforderlich, mit dem Dienstleister einen Auftragsverarbeitungsvertrag abzuschließen.

Im Berichtszeitraum haben Videokonferenzsysteme einen regelrechten Boom erfahren. Um die mit dem Urteil „Schrems II“ verbundenen Schwierigkeiten beim internationalen Datenverkehr zu umgehen, empfehlen wir grundsätzlich den Einsatz von Videokonferenzsystemen, welche die für den Betrieb erforderlichen personenbezogenen Daten innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums verarbeiten.

3.1.4. Aufbewahrungsfristen für Einwilligungserklärungen

Eine Schule aus unserem Zuständigkeitsbereich hat uns angefragt, wie lange Einwilligungserklärungen für die Veröffentlichung von Bildern auf der Homepage aufbewahrt werden müssen.

Eine aus gesetzlichen Regelungen ersichtliche Mindestspeicherdauer für Einwilligungserklärungen gibt es bis auf wenige Ausnahmen nicht. Grundsätzlich müssen die Einwilligungserklärungen vorliegen, solange die Verarbeitung noch andauert. Das heißt, solange Bilder der Schülerinnen und Schüler auf der Homepage abrufbar sind, müssen die Einwilligungserklärungen auch vorliegen. Es kommt somit darauf an, ob und wann die Bilder der Schülerinnen und Schüler von der Homepage entfernt werden. Ab diesem Zeitpunkt kann auch erst die Berechnung einer etwaigen Aufbewahrungsfrist beginnen.

Mangels anderweitiger Vorgaben haben wir empfohlen, die Einwilligungserklärungen für eine Frist von drei Jahren nach Entfernung der Bilder auf der Homepage aufzubewahren. Diese Frist orientiert sich an der Regelverjährungsfrist gemäß § 195 BGB.

3.1.5. Einwilligung bei der Analyse von Webseitenbesuchern

Uns erreichten Anfragen, ob bei der Verhaltensanalyse von Webseitenbesuchern die Zustimmung des Nutzers erforderlich ist, auch wenn diese ohne den Einsatz von Cookies erfolgt. (Für den Fall, dass Cookies eingesetzt werden siehe „Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland: Hinweise zur Verwendung von Cookies“ vom 26. Juli 2018) [5]

Wird das Verhalten von Webseitenbesuchern anhand eines personenbeziehbaren Datums verfolgt, unterliegt diese Analyse dem KDG und bedarf einer Rechtsgrundlage; sie kann dabei auf eine Einwilligung oder auf berechtigtes Interesse gemäß § 6 Abs. 1 lit. g) KDG gestützt werden. Es gilt:

a) Basiert die Verarbeitung auf der Einwilligung der betroffenen Person gemäß § 6 Abs. 2 lit. b) KDG, so ist die Nennung des Zwecks der Verarbeitung erforderlich und die Einwilligung muss vorab erfolgen.

b) Wird die Webanalyse hingegen auf Grundlage des berechtigten Interesses durchgeführt, erfordert dies gemäß § 23 Abs. 1 KDG die Möglichkeit des Widerspruchs.

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

Eine Möglichkeit, diesbezüglich Rechtssicherheit herzustellen, ist ein dem eigentlichen Webseitenbesuch vorgeschalteter sog. "Cookie-Banner", der für den Fall a) die Einwilligung einholt und in b) eine Widerspruchsmöglichkeit bietet. Dabei ist das Erfordernis, die Einwilligung einzuholen oder Widerspruchsmöglichkeit einzuräumen, unabhängig von der Nutzung eines Cookies.

3.2. Beschwerden

3.2.1. Grenzen des Auskunftsrechts im Hinblick auf die Verarbeitung der personenbezogenen Daten eines Kindes durch eine Kirchgemeinde

Die Beschwerde richtete sich gegen eine Kirchengemeinde. Der Beschwerdeführer machte geltend, dass seinem Auskunftsrecht im Hinblick auf die Verarbeitung der personenbezogenen Daten seines Kindes nicht hinreichend Rechnung getragen worden ist. Das evangelische Kind des Beschwerdeführers wurde fehlerhaft von der Pfarrei angeschrieben und zum Kommunionsunterricht eingeladen.

Im laufenden Verfahren trug der Beschwerdeführer vor, dass er zusätzliche Informationen nicht erhalten hätte, auf die er neben solchen über die Verarbeitung der personenbezogenen Daten seines Kindes hinaus, einen Anspruch habe. Dies betraf grundsätzliche Fragen zur Datenlöschung in dem für die Verwaltung genutzten e-mip Programm, Auskünfte darüber, wer Data Controller und wer Data Processor im e-mip ist, die mögliche Nichteinhaltung ordnungsgemäßer technischer und organisatorischen Maßnahmen und letztlich den Zweck der Datenspeicherung und Verarbeitung durch eine Kirchengemeinde.

Der Auskunftsanspruch des Beschwerdeführers gegenüber der Kirchengemeinde richtet sich nach § 17 Abs. 1 Gesetz über den Kirchlichen Datenschutz (KDG) und betrifft grundsätzlich zwei Bereiche. Zum einen den Bereich, ob eine Verarbeitung vorliegt und zum zweiten, falls eine Verarbeitung vorliegt, ein Recht auf Auskunft über die personenbezogenen Daten, die verarbeitet werden.

Neben den personenbezogenen Daten hat der Verantwortliche der betroffenen Person auch Auskunft über zusätzliche Informationen zu erteilen. Die insoweit mitzuteilenden Informationen bestimmen sich anhand des in § 17 Abs. 1 lit. a) bis h) KDG

aufgeführten Kataloges von Informationen abschließend. (vgl. Paal/Pauly/Paal, 2 Aufl. 2018, DS-GVO Art. 15 Rn. 23)

Über den Katalog hinausgehende zusätzliche Informationen waren und sind nicht Teil des Auskunftsanspruches.

3.2.2. Die listenmäßige Erfassung der Besucher eines Kolumbariums

Die Beschwerde richtete sich gegen den kirchlichen Träger eines Kolumbariums.

Der Beschwerdeführer hatte vorgetragen, dass die listenmäßige Erfassung der Besucher der Einrichtung ohne eine Rechtsgrundlage erfolgt und daher nicht zulässig sei. Die in Rede stehende Liste umfasste neben dem Namen, der Telefonnummer und dem Namen des Verstorbenen auch die Ankunfts- und Weggangzeit des Besuchers. Ein Hinweis auf die datenschutzrechtlichen Informationspflichten war nicht erkennbar. Als Datenschutzhinweis erfolgt ausschließlich eine aufgedruckte Mitteilung, dass die Liste nach 21 Tagen vernichtet wird.

Mit einem Schreiben des zuständigen Bistums wurde der Beschwerdeführer darüber informiert, dass die Verarbeitung seiner personenbezogenen Daten auf der Rechtsgrundlage eines berechtigten Interesses (gem. § 6 Abs. 1 lit. g) KDG) erfolgt und darüber hinaus zukünftig eine andere Art der Datenverarbeitung erfolgen soll (einzelne Meldezettel).

Die listenmäßige Erfassung der personenbezogenen Daten der Besucher des Kolumbariums war in der dargestellten Form unzulässig.

Die Verarbeitung personenbezogener Daten hat rechtmäßig zu erfolgen (vgl. § 7 Abs.1 KDG). Bei der listenmäßigen Verarbeitung sind die personenbezogenen Daten unmittelbar bei der betroffenen Person erhoben worden. Insoweit ist die betroffene Person über die in § 15 KDG geregelten Vorgaben schon bei der Datenerhebung zu informieren.

Unabhängig davon war auf folgendes hinzuweisen:

Die Verarbeitung personenbezogener Daten im Rahmen der Umstellung der Datenerhebung durch Meldezettel ist u. a. dann zulässig, wenn das kirchliche Daten-

schutzgesetz oder eine staatliche Rechtsvorschrift, alternativ eine andere kirchliche Regelung, sie erlaubt oder anordnet (vgl. § 6 Abs. 1lit a) KDG).

Eine staatliche Rechtsvorschrift bestand nicht; insbesondere sieht die niedersächsische Corona-Verordnung gerade keine Verpflichtung zur Erhebung von personenbezogenen Daten im Rahmen der für die Religionsausübung getroffenen Regelungen vor (vgl. § 23 Niedersächsische Corona-Verordnung (NDS. GVBL S. 226,257)), sondern verweist auf ein Hygienekonzept (vgl. § 3 Niedersächsische Corona-Verordnung).

Eine andere kirchliche Regelung außerhalb des kirchlichen Datenschutzrechts liegt ebenfalls nicht vor.

Die aus § 6 Abs. 1 lit. g) KDG herangezogene Rechtsgrundlage des berechtigten Interesses zur Verarbeitung der personenbezogenen Daten ist zumindest nicht frei von rechtlichen Bedenken. Fragen stellen sich bereits im Rahmen der Erforderlichkeit der Verarbeitung. Gegebenenfalls könnte auch eine Begrenzung der Besucherzahl, Maske und Abstand den Zweck erfüllen die Besucher und Mitarbeiter zu schützen (Hygienekonzept). Letztlich sind die Interessen, Grundrechte und Grundfreiheiten des Betroffenen mit den Interessen des Verarbeiters abzuwägen.

Im Ergebnis hat der Träger mitgeteilt, dass keine Besucherdaten mehr erhoben werden - weder zu den Öffnungszeiten, noch zu den Gottesdiensten -, sondern ein Hygienekonzept entwickelt worden ist, dass dem Besuchsanlass entsprechend für die notwendig Sicherheit sorgt.

3.2.3. Datenschutzhinweise Homepage

Eine weitere Beschwerde hatte die Datenschutzhinweise einer Webseite zum Gegenstand. Vorgetragen worden ist, dass der Beschwerdegegner keine Rechtsgrundlagen für die jeweiligen Verarbeitungsvorgänge aufgeführt hatte. Im Ergebnis war die Beschwerde des Beschwerdeführers begründet. Die Datenschutzhinweise der Webseite enthielt nicht sämtliche nach § 15 Abs. 1 KDG erforderlichen Informationen. In diesem konkreten Fall waren nicht die in § 6 KDG benannten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten aufgeführt.

3.3. Datenpannen

3.3.1. Fehlerhafter Zugriff auf ein sogenanntes Transferverzeichnis

Von einem externen betrieblichen Datenschutzbeauftragten wurde mitgeteilt, dass es durch einen fehlerhaften Zugriff auf ein sogenanntes Transferverzeichnis zu einer Offenlegung auf die in einem Rechenzentrum gespeicherten Daten von vierzig Kirchengemeinden gekommen ist. Ursächlich war eine fehlerhafte Konfiguration. Dadurch wäre eine missbräuchliche Nutzung der einsehbaren Daten aus einer anderen kirchengemeindlichen Einrichtung des betreffenden Bistums möglich gewesen.

Nach Angaben des Dienstleisters (Rechenzentrum) waren insgesamt - alle Ordner zusammengefasst -1.332 Dokumente betroffen. Die Anzahl der möglichen Nutzer wurde mit 1.159 beziffert. Neben einigen datenschutzrechtlich völlig unkritischen Dokumenten handelte es sich zumindest teilweise um besondere personenbezogene Daten. Die Verantwortlichkeit für die fehlerhafte Konfiguration ließ sich nach Angaben des Dienstleisters (Rechenzentrum) nicht feststellen. Die Möglichkeit, den jeweiligen Nutzern entsprechende Rechte einzuräumen wäre sowohl auf Seiten der Kirche als auch von Seiten des Dienstleisters her möglich gewesen.

Bei den Recherchen zur Sachverhaltsaufklärung wurde festgestellt, dass ein Berechtigungskonzept, unter welchen Voraussetzungen und von wem Rechte vergeben oder entzogen bzw. geändert werden durften, nicht vorhanden war. Entsprechende Vergaben sind zudem nicht dokumentiert worden. Zudem mangelte es an einer rechtssicheren Grundlage für die Verarbeitung von personenbezogenen Daten im Sinne des § 29 Abs. 3 KDG zwischen den betroffenen Kirchengemeinden und dem Dienstleister.

Nach den eigenen Feststellungen des Dienstleisters für die Datenverarbeitung ist letztlich davon auszugehen, dass unzureichende organisatorische Maßnahmen als Ursache der Datenschutzverletzung anzunehmen sind.

Die Verpflichtung zur Umsetzung eines angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten durch entsprechende technische und organisatorische Maßnahmen trifft den Verantwortlichen und gegebenenfalls den Auf-

tragsverarbeiter (vgl. § 26 Abs. 1 KDG). Ein Auftragsverarbeitungsverhältnis im Sinne des § 29 Abs. 3 KDG war für die Verarbeitung von personenbezogenen Daten zwischen der betroffenen Kirchengemeinde und dem Dienstleister allerdings nicht vorhanden. Die Nichtberücksichtigung der erforderlichen organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten vor einer unbefugten Offenlegung durch den Dienstleister ist daher allein der verantwortlichen Stelle zuzuschreiben, wenn diese es verabsäumt hat sicherzustellen, dass die Verarbeitung im Einklang mit den Anforderungen des kirchlichen Datenschutzrechts erfolgt (vgl. § 29 Abs. 1 KDG).

Die Nichtbeachtung der sich aus dem kirchlichen Datenschutzrecht für den Verantwortlichen ergebenden Verpflichtungen bei der Verarbeitung von personenbezogenen Daten war daher datenschutzrechtlich zu sanktionieren.

3.3.2. Fehlerhafter Versand von E-Mail Befunddaten

Ein Krankenhaus teilte mit, dass es durch einen Schreibfehler bei einer E-Mail-Adresse zu einem fehlerhaften Versand und damit zu einer unrechtmäßigen Offenlegung von Befunden gekommen sei. Die Befunde sollten nach Rücksprache mit dem betroffenen Patienten per E-Mail unverschlüsselt an diesen verschickt werden. Durch den fehlerhaften Versand der E-Mail hatte der unbefugte Dritte zumindest die Möglichkeit, von den Befunden Kenntnis zu nehmen. Bereits in der Meldung der Datenschutzverletzung hat das Krankenhaus als sofort ergriffene Maßnahme mitgeteilt, dass fortan Postausgänge stets nach dem 4-Augen-Prinzip geprüft werden sollen.

Durch den Versand der unverschlüsselten E-Mail an den unbefugten Dritten hat das Krankenhaus gegen datenschutzrechtliche Vorschriften verstoßen. In der das Verfahren abschließenden Verwarnung ist zum einen ein Verstoß gegen § 25 Abs. 1 KDG-DVO festgestellt worden. Hiernach dürfen E-Mails, welche personenbezogene Daten der Datenschutzklasse III enthalten, „ausschließlich im Rahmen eines geschlossenen und gesicherten Netzwerks oder in verschlüsselter Form mit geeignetem Verschlüsselungsverfahren übermittelt werden“. Dies ist vorliegend nicht erfolgt.

Zum anderen entspricht das Vorgehen nicht den Vorgaben aus dem Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 19. September 2019.[6] Sofern in der „Rücksprache mit dem Patienten“ überhaupt eine Einwilligung gesehen werden kann, so ist diese zumindest dann nicht zulässig, wenn hiermit das gesetzlich vorgeschriebene Schutzniveau unterschritten werden soll.

3.3.3. Versand von Selbstzahler-Rechnungen

Ebenfalls in einem Krankenhaus sind Selbstzahler-Rechnungen an den falschen Empfänger übermittelt worden. Im Rahmen der Rechnungstellung haben zwei betroffene Personen die Rechnung der jeweils anderen betroffenen Person erhalten. Nach Bekanntwerden des fehlerhaften Versands der Rechnung sind die betroffenen Personen hierüber informiert worden.

Auch wenn es im Rahmen der Rechnungstellung und der Hektik im Klinikbetrieb durchaus turbulent zugehen kann, so ist gerade in einem so sensiblen Bereich wie dem eines Krankenhauses der datenschutzkonforme Umgang mit personenbezogenen Daten von enormer Wichtigkeit.

3.3.4. Postversand bei Wohnungswechsel

Eine Verkettung unglücklicher Umstände führte in einem weiteren gemeldeten Fall dazu, dass personenbezogene Daten einer kirchlichen Beratungsstelle in die Hände einer unbefugten Person gelangen konnte.

Die Beratungsstelle führt die Fallbesprechungen mit den Kollegen üblicherweise in der Einrichtung selbst durch. Diese Präsenztermine wurden durch die Pandemie jedoch ausgesetzt. Stattdessen sind die Einsatztermine mit einer Kurzinformation zu den betroffenen Familien an die jeweiligen Beraterinnen und Berater per Post verschickt worden. Die zuständige Beraterin hatte jedoch den Wohnsitz gewechselt und die neue Postadresse nicht umgehend der Beratungseinrichtung mitgeteilt. Ein Nachsendeauftrag, auf den die Beraterin vertraute, war eingerichtet.

Die Beratungseinrichtung, welche nicht über den Wohnsitzwechsel informiert gewesen ist, hat den Einsatztermin mit der Kurzinformation an die im System hinterlegte Adresse verschickt. Durch den eingerichteten Nachsendeauftrag hätte diese Infor-

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

mation auch an die Beraterin weitergeleitet werden sollen. Leider ist gerade dies jedoch nicht geschehen. So hatte die Nachmieterin zumindest die Möglichkeit, von dem Inhalt der Kurzinformation Kenntnis zu nehmen.

Die Einrichtung hat diesen Vorfall zum Anlass genommen, jeden Berater und jede Beraterin darüber zu informieren, wie wichtig die zeitnahe Aktualisierung der Stammdaten im System ist. Nur dadurch lassen sich solche Fehler vermeiden. Der Fall zeigt auch, dass allein ein Nachsendeauftrag bei der Post nicht ausreicht, um die zuverlässige Weiterleitung von Briefen zu gewährleisten.

3.4. Prüfungen

Aufgrund der Pandemie war es uns im vergangenen Jahr nur möglich, zwei Einrichtungen vor Ort zu prüfen. Die erste vor-Ort-Prüfung fand bereits im Januar statt. Die zweite Prüfung vor Ort wurde im September durchgeführt. Bei der ersten Einrichtung handelte es sich um ein Krankenhaus, bei der zweiten um eine kirchliche Beratungsstelle. Die vollständig digital durchgeführte Querschnittsprüfung in den Kitas konnte fortgesetzt werden.

3.4.1. Entwicklung und Vorbereitung Querschnittsprüfungen

Nach einer Zunahme der Meldungen über Datenverluste, bedingt durch gestohlene Laptops und Datenträger in Kindertageseinrichtungen, erfolgte im August 2019 zu diesem Thema eine Information und Sensibilisierung der Kindertageseinrichtungen in Trägerschaft der Kirchengemeinden über die (Erz-)Bischöflichen Generalvikariate sowie das Bischöflich Münstersche Offizialat in Vechta i. O. Im Dezember 2019 wurden ausgewählte Kindertagesstätten aus dem Zuständigkeitsbereich des Diözesandatenschutzbeauftragten der norddeutschen Bistümer zur Teilnahme an einer Online-Umfrage zur Überprüfung der Umsetzung der Anforderungen an die Datensicherheit aufgefordert. Die durch die Umfrage behandelten Themenbereiche waren der betriebliche Datenschutzbeauftragten, Grundlagen zur Datenverarbeitung und organisatorischer Datenschutz, das Löschen von Daten und Verschlüsselung sowie allgemein die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.

In einer ersten Runde wurde der Umsetzungsstand in den Einrichtungen über einen Fragebogen erfasst. Zu einigen der eingereichten Antworten hatten sich noch Rück-

fragen ergeben, die in einer zweiten Runde in Form einer Fragenliste an die Einrichtungen gesendet worden sind. Für die Beantwortung einiger Fragen war eine Beteiligung der betrieblichen Datenschutzbeauftragten der Einrichtung / des Trägers sowie ggf. eines IT-Dienstleisters empfohlen. Mit Ende des Jahres 2020 liefen die Arbeiten zur finalen Auswertung.

3.4.2. Krankenhaus

Die Prüfung des Krankenhauses ist auf Wunsch der Einrichtung selbst durchgeführt worden. Aufgrund der Größe des Krankenhauses und des Umfangs der Prüfung mussten hier Schwerpunkte gesetzt werden.

Dem Krankenhaus wurden zwei Musterfälle in Form von fiktiven Patienten vorgegeben und diese wurden auf ihrem jeweiligen Weg durch die Klink in datenschutzrechtlicher Hinsicht „begleitet“ und die zugehörigen Abläufe und Prozesse geprüft.

Bei dem ersten Musterfall handelte es sich um eine reguläre Aufnahme eines fiktiven Patienten zur Abklärung vorgegebener Symptome. Besonderes Augenmerk wurde dabei auf die administrative Aufnahme sowie auf das Entlassungsmanagement gelegt. Beim zweiten Musterfall wurde ein fiktiver Patient, der über die Notaufnahme aufgenommen worden ist, auf seinem Weg durch die Klinik begleitet.

Bei der Aufnahme hat jeder Patient als betroffene Person eine Vielzahl von Dokumenten mit diversen datenschutzrechtlichen Informationen und Einwilligungen zu unterschreiben. Gerade in diesem Bereich ist es wichtig, dass die betroffene Person trotz des belastenden Umstands einer Aufnahme in ein Krankenhaus diese transparent und klar vermittelt bekommt. Im Bereich des Entlassungsmanagements kommt es häufig zu einer Weitergabe von Gesundheitsdaten des Patienten an Dritte, um einen reibungslosen Ablauf in der weiteren Therapie zu gewährleisten. In diesem Bereich kann es bei der Beendigung des Krankenhausaufenthaltes viele Schnittstellen zu Hausärzten, Krankenkassen, häusliche Pflege, Rehaeinrichtungen und weiteren Ein-richtungen geben.

Grundsätzlich ist darauf hinzuweisen, dass alle Einwilligungserklärungen einen Hinweis nach § 8 Abs. 6 Satz 2 KDG enthalten müssen, wonach die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung durch den Widerruf unberührt bleibt. Auch reicht ein DIN-A4 großes Informationsschreiben als Aushang in der

administrativen Aufnahme nicht aus, um den Informationspflichten nach § 15 KDG zu genügen. Die Informationen müssen der betroffenen Person in geeigneter Weise, d.h. etwa durch Handouts, große Hinweisschilder und/oder Hinweise auf der Homepage, zugänglich gemacht werden. Auch sollten Abschnitte des Behandlungsvertrages, welche mit „datenschutzrechtliche Einwilligungen“ überschrieben sind, auch tatsächlich nur datenschutzrechtliche Einwilligungen enthalten. So sind zumindest in diesem Abschnitt auch Hinweise auf Dienstleister und Kooperationspartner des Krankenhauses irreführend.

In technischer Hinsicht lag ein Schwerpunkt bei der Prüfung von Zutritts-, Zugangs- und Zugriffsberechtigungen. Zu beachten ist in diesem Zusammenhang, dass auch wenn definierte Abläufe für die Vergabe von Berechtigungen (z.B. Laufzettel) und ein differenziertes Berechtigungskonzept (z.B. Schlüsselkarte, Rechte- und Rollenkonzept) bestehen, diese Berechtigungsvergabe in regelmäßigen Abständen zumindest stichprobenartig zu überprüfen sind.

3.5. Informationsveranstaltungen

Es gehört zu den Aufgaben (Beratung) der Datenschutzaufsicht der Nachfrage nach Informationsbedarf in den kirchlichen Einrichtungen nachzukommen. Die Mitarbeiter der Behörde 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 kirchlichen Datenschutzaufsicht zu informieren.

4. Über die Dienststelle des DDSB/Nord-Bremen

4.1. Infrastruktur

Das Büro der Datenschutzaufsicht 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 - 16:00 Uhr und am Freitag von 09:00 bis 12:00 zu erreichen.

Telefon: 0421 330056-0
E-Mail: info@kdsa-nord.de

4.2. Finanzen

Die Personal- und Sachkosten der Datenschutzaufsicht 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 2020 standen Haushaltsmittel in Höhe von 421.100,00 Euro zur Verfügung.

4.3. Personal

Das Stellentableau umfasste im Berichtszeitraum 4 Vollzeitstellen, einschließlich des Sekretariats.

4.4. Vertretung in Konferenzen und Arbeitsgruppen

Der Leiter der Datenschutzaufsicht für die norddeutschen Diözesen 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
- Tagung der Mitglieder des Virtuellen Datenschutzbüros
- Regelmäßige Treffen mit den betrieblichen Datenschutzbeauftragten

Die von der KDSA Nord ausgerichteten Veranstaltungen konnten aufgrund der Pandemiesituation nicht wie gewohnt als Präsenztermine ausgerichtet werden. Gleichwohl ist es gelungen, die etablierten Runden und Austauschmöglichkeiten – wenn auch in einem anderen Format – aufrechtzuerhalten.

4.5. 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.

4.6. Öffentlichkeitsarbeit

Der Internetauftritt der Datenschutzaufsicht Nord „www.kdsa-nord.de“ wird bundesweit genutzt und geschätzt. Es wird auch deshalb zukünftig das Ziel sein, die Internetseite wie bisher zu pflegen und sie jeweils dem neuesten Stand des kirchlichen, und gegebenenfalls auch weltlichen, Datenschutzrechts anzupassen.

Auch die elektronische Meldung von betrieblichen Datenschutzbeauftragten, Datenschutzpannen oder Beschwerden sind über diese Webseite möglich. Jeder Besucher der Homepage hat neben der schriftlichen oder telefonischen Meldung auch

die Möglichkeit, seine Anliegen über ein entsprechendes Portal an die Datenschutzaufsicht zu melden.

Die vorgehaltenen Informationen, Arbeitshilfen, Praxishilfen und Mitteilungen dienen dazu, die Einrichtungsleiter und Mitarbeiter der kirchlichen Dienststellen gleichermaßen zu informieren und sie für das Recht auf informationelle Selbstbestimmung für sich und andere zu sensibilisieren.

5. Schlussbemerkung

Auch wenn der vorliegende Bericht keine „Highlights“ im eigentlichen Sinn darstellt zeigt er doch, dass im Bereich der Katholischen Datenschutzaufsicht Nord ein unaufgeregter und professioneller Einsatz für die Rechte der Menschen geleistet wird.

Mit den vorhandenen rechtlichen und materiellen Ressourcen haben wir es unternommen, auch in diesen durchaus „schwierigen“ Zeiten, die nach dem kirchlichen Datenschutzgesetz vorgeschriebenen Aufgaben zu erfüllen. Dabei haben wir uns auch von dem Gedanken leiten lassen, dass situativ und ohne Aufgabe unserer datenschutzrechtlichen Überzeugungen der Grundsatz der Praktikabilität bei der Lösung der mit der Pandemie entstandenen Herausforderungen nicht in Vergessenheit geraten ist.

In der Konsequenz wird das, was tatsächlich von vielen Beteiligten geleistet worden ist, dazu führen, dass die Akzeptanz des kirchlichen Datenschutzrechts gesteigert wird und die Ressentiments abnehmen. Das ist jedenfalls die nicht unbegründete Hoffnung.

Je größer das Bewusstsein der Menschen dafür wird, dass personenbezogene Daten nicht etwas Beliebiges sind, Bsp. die Bilder der Kinder, sondern unmittelbar mit dem Wert und der Würde des Einzelnen in Beziehung stehen, je einfacher wird die Aufgabe, die wir übernommen haben. Wir kommen dieser Aufgabe frei von geleiteten Interessen nach und realisieren unabhängig den Auftrag, den die Kirche in ihren Regelungen festgeschrieben hat. Der Einsatz für die Belange der Einzelnen und deren Grundecht auf informationelle Selbstbestimmung.

Die Katholischen Datenschutzaufsicht Nord wird auch zukünftig dafür Sorge tragen, dass die Menschen im Zusammenhang mit ihren personenbezogenen Daten wahrgenommen und beachtet werden.

6. Anlage

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

Einrichtung	Datenschutzbeauftragte	Anschrift
Bischöfliches Generalvikariat Osnabrück	Thomas Marien datenschutz@bistum-os.de	Hasestraße 40a 49074 Osnabrück
Ehe-/Familien-/Lebens-/Erziehungs-Beratungsstelle	Ludger Lüken l.lueken@bistum-os.de	Domhof 2 49074 Osnabrück
Kirchliche Einrichtungen im Bistum Osnabrück	Itebo GmbH Kim Schoen datenschutz@bistum-os.de	Dielinger Straße 40 49074 Osnabrück
Offizialat Vechta	Datenschutz nord GmbH 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 Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Kirchliche Einrichtungen im Bistum Hildesheim	datenschutz nord GmbH Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Erzbischöfliches Generalvikariat Hamburg	Itebo GmbH Kim Schoen dsb@itebo.de	Dielinger Straße 40 49074 Osnabrück
Kirchliche Einrichtungen im Erzbistum Hamburg	datenschutz nord GmbH Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen