Jahresbericht 2020

des Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

Berichtszeitraum
01.01.–31.12.2020

Katholisches
Datenschutzzentrum

Herausgegeben vom

Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn
sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

Katholisches Datenschutzzentrum
Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Hinweis: Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt adäquate andere Formen gleichberechtigt ein.

Bildnachweis Titelmotiv: istockphoto.com | matejmo

5. Jahresbericht

des Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

für den Zeitraum 01.01.2020– 31.12.2020

Redaktionsschluss: 31.05.2021

Inhaltsverzeichnis

Vorwort

Corona. Ein Thema bestimmte den Großteil des Jahres 2020 und das Leben der Menschen. Die pandemiebedingten Umbrüche und Einschränkungen haben auch in der Arbeit des Diözesan- und Verbandsdatenschutzbeauftragten und des Katholischen Datenschutzzentrums ihren Niederschlag gefunden.

Fiebermessen bei Beschäftigten, Besucherlisten in Pflegeheimen, Fragen nach erfolgter Impfung oder durchgestandener Erkrankung mit dem Corona-Virus durch den Dienstgeber oder Kontaktnachverfolgung bei Gottesdiensten waren nur einige der vielen Fragestellungen, die im Rahmen der Pandemie an die Datenschutzaufsicht herangetragen wurden. Daher haben wir diesem Thema in Abschnitt 3 dieses Berichts einen Schwerpunkt gewidmet. Der Europäische Datenschutzausschuss (EDSA) als Gremium der nationalen Datenschutzaufsichten der EU-Staaten hat bereits in einer Erklärung vom 19.03.2020 festgehalten, dass die Datenschutzvorschriften (wie die Datenschutz-Grundverordnung der Europäischen Union, kurz DSGVO) der Ergreifung von Maßnahmen gegen die Coronavirus-Pandemie nicht entgegenstünden. Dennoch wollte der Europäische Datenschutzausschuss unterstreichen, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter den Schutz der personenbezogenen Daten der betroffenen Personen auch in dieser Ausnahmesituation sicherstellen müssen.

Aus datenschutzrechtlicher Sicht ebenfalls einschneidend war das Urteil des Europäischen Gerichtshofs zur Unwirksamkeit des Privacy-Shield, mit dem vielen Übermittlungen von Daten in die USA die Grundlage entzogen wurde. Auch diesem Thema haben wir in Abschnitt 3 einen Schwerpunkt gewidmet.

Zwei weitere Schwerpunkte in Abschnitt 3 bilden der in 2020 endgültig vollzogene Brexit und die Betroffenenrechte des Gesetzes über den Kirchlichen Datenschutz (KDG). Gerade die mit den neuen datenschutzrechtlichen Regelungen der DSGVO beziehungsweise dem darauf aufbauenden KDG ausgebauten Betroffenenrechte bereiten vielen kirchlichen Einrichtungen immer noch Probleme. Der bessere Schutz der Betroffenen war aber eines der Anliegen der neuen datenschutzrechtlichen Regelungen. Zu diesem Thema erhielten wir viele Beschwerden, die deutlich machen, dass es hier noch Nachholbedarf bei der Implementierung der Betroffenenrechte gibt.

Insgesamt erreichte das Katholische Datenschutzzentrum eine weiterhin hohe Zahl an Anfragen und Beschwerden aus allen kirchlichen Einrichtungstypen und zu vielen Themenbereichen. Die Zahl der Meldungen von Datenschutzverletzungen stieg im Vergleich zum Jahr 2019 im Berichtszeitraum sogar noch deutlich an. Hier sind sicherlich auch eine gestiegene Sensibilität für die datenschutzrechtlichen Probleme und neue, ungewohnte Abläufe und Prozesse aufgrund der Umstellungen durch die Corona-Pandemie ursächlich.

Dies macht aber auch deutlich, dass Datenschutz bei der Neueinrichtung oder Änderung von Prozessen und Abläufen immer wieder mitgedacht werden muss. Datenschutz ist ein Prozess, der lebt und der immer wieder überprüft und verbessert werden muss. In diesem Sinne hoffe ich weiterhin auf Ihre Mithilfe, damit wir gemeinsam einen hohen Schutz der personenbezogenen Daten im Bereich der Kirche gewährleisten können.

Steffen Pau
Diözesan- und Verbandsdatenschutzbeauftragter
und Leiter des Katholischen Datenschutzzentrums (KdöR)

„Datenschutz ist ein Prozess, der lebt und der immer wieder überprüft und verbessert werden muss."

1 Entwicklungen im Datenschutzrecht

Auch in diesem Berichtszeitraum gab es eine Vielzahl von gesetzgeberischen oder regulatorischen Initiativen zur Weiterentwicklung des Datenschutzrechts auf europäischer, nationaler und kirchlicher Ebene.

1.1 Gesetzgeberische Entwicklungen auf Ebene der Europäischen Union

Auf europäischer Ebene wurde im Berichtszeitraum über die Folgen des Brexits, den internationalen Datentransfer und andere Themen diskutiert. Nachfolgend sind einige aus Sicht des Katholischen Datenschutzzentrums wichtige Vorhaben erläutert.

1.1.1 Brexit vollzogen, aber endgültige datenschutzrechtliche Auswirkungen immer noch unklar

Im Berichtszeitraum setzten sich die Unsicherheiten bezüglich der zukünftigen Bedingungen für eine Datenübermittlung von und nach Großbritannien und Nordirland fort, die mit dem Beschluss Großbritanniens und Nordirlands zum Austritt aus der Europäischen Union im Jahr 2016 entstanden waren („Brexit").[1]

Durch das am 24.01.2020 unterzeichnete Austrittsabkommen wurde der Zeitpunkt für den Austritt aus der EU auf den 31.01.2020 festgelegt. Gleichzeitig wurde eine Übergangsfrist bis zum 31.12.2020 vereinbart, in der das EU-Recht – und damit auch die DSGVO – erst einmal unverändert weiter gelten.

Welche Regeln nach dem 31.12.2020 gelten sollten, wurde während des gesamten Berichtszeitraums verhandelt. Am 30.12.2020 unterzeichneten die Vertreter beider Seiten das Handels- und Kooperationsabkommen zwischen der Europäischen Union und dem Vereinigten Königreich, das zum 01.01.2021 in Kraft trat.

Mit dem Ende der Übergangsphase zum Austritt aus der EU zum 31.12.2020 ist die DSGVO in Großbritannien und Nordirland nicht mehr direkt anwendbar.

In dem ausgehandelten Handels- und Kooperationsabkommen haben sich die Vertreter der EU und des Vereinigten Königreichs dahingehend verständigt, dass Transfers personenbezogener Daten zwischen der EU und dem Vereinigten Königreich für einen Übergangszeitraum von bis zu sechs Monaten ab dem 01.01.2021 nicht als Transfers in ein Drittland angesehen werden. Vorbedingung dafür ist jedoch, dass das Vereinigte Königreich sein weiteres Vorgehen in datenschutzrechtlichen Fragen

[1] Zum Brexit siehe auch Abschnitt 1.1.4 des Jahresberichts 2019.

mit der EU abstimmt.[2] Sollte es innerhalb dieses Übergangszeitraums nicht zu einer weitergehenden Vereinbarung oder zu einer Festlegung des Status des Vereinigten Königreichs aus Sicht der EU durch einen Angemessenheitsbeschluss der EU-Kommission kommen, wird das Vereinigte Königreich spätestens ab diesem Zeitpunkt als Drittland im Sinne des Datenschutzrechts mit allen sich daraus ergebenden Konsequenzen anzusehen sein.

Für kirchliche Einrichtungen bedeutet dies weiterhin, dass die zukünftigen Bedingungen für die Übermittlung von personenbezogenen Daten von und nach Großbritannien und Nordirland immer noch nicht endgültig geklärt sind. Damit müssen sich kirchliche Einrichtungen als Nutzer von Serviceleistungen und Angeboten britischer Unternehmen weiterhin auf mehrere mögliche Szenarien vorbereiten und für sich prüfen, ob sowohl unter den aktuellen, als auch unter den zukünftig zu erwartenden veränderten Bedingungen ein Datenaustausch noch zulässig ist beziehungsweise gestaltet werden kann. Das gilt auch in den Fällen, in denen britische Unternehmen von Vertragspartnern einer kirchlichen Einrichtung als Unterauftragnehmer eingesetzt werden oder Speicherorte in Großbritannien liegen. Dazu gehört ferner die Analyse, welche konkreten Dienstleistungen oder Serviceangebote in Anspruch genommen und welche Produkte von Herstellern oder Anbietern aus dem Vereinigten Königreich oder mit dortigen Niederlassungen oder Standorten eingesetzt werden, etwa Software, IT-Produkte, Nutzungen von Diensten und Cloud-Diensten, Konferenztools oder Serverkapazitäten. Weiter ist zu untersuchen, ob in diesem Zusammenhang Daten in das Vereinigte Königreich übermittelt werden. Die Verträge mit entsprechenden Anbietern sind darauf zu überprüfen, ob sie mit Vollzug des EU-Austritts weiterhin eine tragfähige Rechtsgrundlage darstellen können, um Datenübermittlungen und Datenverarbeitungen zuzulassen.

Das Katholische Datenschutzzentrum hat die Entwicklung im Berichtszeitraum fortlaufend begleitet und die kirchlichen Einrichtungen allgemein oder zu einzelnen Anfragen beraten. Es wird auch weiterhin die Entwicklungen beobachten und über die Ergebnisse berichten, die sich aus weiteren Vereinbarungen zwischen Großbritannien und der EU beziehungsweise einem möglichen Angemessenheitsbeschluss der EU ergeben.

1.1.2 Bericht der Europäischen Kommission zur Evaluation der DSGVO

Jahrestage sind ein willkommener Anlass zur Überprüfung der zurückliegenden Entwicklung. Daneben bieten zwischenzeitlich eingetretene Ereignisse Gründe, über zurückliegend getroffene Entscheidungen und Vorgaben nachzudenken. Entwicklungen durch technischen Fortschritt, aber auch durch richterliche Entscheidungen bieten eine sinnvolle Grundlage, um zu überprüfen, ob die Rechtsgrundlagen, die zu einem bestimmten Zeitpunkt geschaffen wurden, noch die an sie gestellten Anforderungen und Erwartungen erfüllen. Dies gilt auch für die Datenschutz-Grundverordnung der Europäischen Union. Ferner bieten gesetzesimmanente Überprüfungsvorgaben einen Anlass, sich

[2] Siehe Artikel FINPROV.10.A (interim provision for transmission of personal data to the United Kingdom) des Handels- und Kooperationsabkommens.

über bestehende Gesetzesgrundlagen und deren bisherige Bewährung in der Anwendung sowie über mögliche Novellierungsnotwendigkeiten Gedanken zu machen.

Die Europäische Kommission hat in ihrer Mitteilung an das Europäische Parlament und den Rat vom 24.06.2020 unter dem Titel „Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – 2 Jahre Anwendung der Datenschutz-Grundverordnung" eine Bewertung der DSGVO und ihrer Auswirkung auf die Lebensbereiche in der EU vorgenommen. Ein Blick auf die Vorstellungen der Kommission ist auch für das kirchliche Datenschutzrecht von Bedeutung, da die Kommission einer der maßgebenden Mitgestalter des Datenschutzrechts auf europäischer Ebene ist. Ihre Vorstellungen fließen in die Überlegungen zu weiteren Ausgestaltungen des Datenschutzes und zu Novellierungen der DSGVO in nicht unerheblichem Maße ein. Insofern beobachtet das Katholische Datenschutzzentrum die Entwicklungen, die eine Vorbildwirkung für vergleichbare Überlegungen zum katholischen Datenschutzrecht entfalten können. Auch kirchliche Anwender des Datenschutzrechts sollten Überlegungen auf europäischer Ebene durchaus in den Blick nehmen. Mindestens haben diese Auswirkungen auf die Ausgestaltungen von Rechtsbeziehungen mit Vertragspartnern, die der Rechtsanwendung der DSGVO unterliegen.

Die Kommission stellt in ihrer Mitteilung den Wert der einheitlichen DSGVO für die europäischen Staaten heraus. Sie betont die Bedeutung für den Schutz personenbezogener Daten, aber auch für den Binnenmarkt und den Bereich der Wirtschaft. Neben der Funktion der Gewährleistung des im europäischen Recht verankerten Grundrechts auf Datenschutz und der Stärkung der Rechte des Einzelnen sowie der Erhöhung von Transparenz wird auch die Auswirkung auf die Gewährleistung eines freien Datenverkehrs und der gleichartigen Wettbewerbsbedingungen hervorgehoben. Nicht ohne Stolz weist die Kommission auf die Vorbildfunktion des europäischen Datenschutzrechts auf Gesetzesbestimmungen in außereuropäischen Ländern hin, z. B. in Japan, Südkorea oder dem Bundesstaat Kalifornien in den USA, sowie auf eine positive Beurteilung durch den Generalsekretär der Vereinten Nationen. Allerdings sieht die Kommission auch Ansatzpunkte für Verbesserungen.

So spricht sich die Kommission als flankierende Maßnahme für eine weitergehende Sicherstellung des Datenschutzes für die zügige Prüfung und Annahme einer e-Privacy-Verordnung durch die Gesetzgebungsorgane der EU aus. Zur Realisierung eines sicheren Datenaustauschs und zur Förderung der Datenverfügbarkeit empfiehlt die Kommission einen europäischen Cloud-Zusammenschluss, über den Datenverarbeitungs- und Cloud-Infrastrukturdienste im Einklang mit der DSGVO angeboten werden könnten.

In Ihrer generellen Bewertung kommt die Europäische Kommission zu dem Ergebnis, dass die Ziele der Stärkung des Rechts des Einzelnen auf Schutz seiner personenbezogenen Daten und die Gewährleistung des freien Datenverkehrs für personenbezogene Daten innerhalb der EU erreicht worden seien. Bei aller positiver Einschätzung warnt die Kommission jedoch davor, bereits jetzt und damit aus ihrer Sicht zu früh,

endgültige Schlüsse bezüglich einer abschließenden Gesamtbewertung der DSGVO zu ziehen.

So lobt die Kommission zwar die in der DSGVO niedergelegten neuen Verfahren zur Zusammenarbeit und Kohärenz der Datenschutzaufsichtsbehörden in den europäischen Staaten und die bereits unternommenen Schritte zur Nutzung dieser Verfahren, sieht jedoch noch Verbesserungsbedarf in der Verwendung und Umsetzung.

Gleiches gilt für die Harmonisierung von nationalem Datenschutzrecht, um auf diese Weise in grenzüberschreitenden Fällen die Bearbeitung in der gesamten EU zu verbessern. Als einen wesentlichen Faktor sieht die Kommission dabei auch die Tätigkeit des Europäischen Datenschutzausschusses und die Verabschiedung von dessen Leitlinien als Orientierungsvorgaben für die Umsetzung des Datenschutzrechts in den Mitgliedstaaten der EU. Aufgrund der Bedeutung dieser Leitlinien für die Anwendung des Datenschutzrechts in der EU beobachtet auch das Katholische Datenschutzzentrum die Entscheidungen des EDSA und deren mögliche Folgen auf das kirchliche Datenschutzrecht.

„Aufgrund der Bedeutung dieser Leitlinien .... beobachtet auch das Katholische Datenschutzzentrum die Entscheidungen des EDSA und deren mögliche Folgen ...“

In ihrer Analyse kommt die Kommission zu dem Ergebnis, dass die im Gesetz ausdrücklich vorgesehene Möglichkeit für die Mitgliedstaaten, bestimmte Bereiche des Datenschutzrechts eigenständig und an den nationalen Bedürfnissen ausgerichtet regeln zu können, voneinander abweichende Voraussetzungen entstehen lässt, die aus Sicht der Kommission im grenzüberschreitenden Binnenmarkt zu Behinderungen führen. Einen weiteren Schwerpunkt für Schwierigkeiten sieht die Kommission in der unterschiedlichen Gewichtung bei der Abwägung von Rechten, wie etwa der Meinungsfreiheit im Verhältnis zum Schutz personenbezogener Daten in den Rechtssystemen der Mitgliedstaaten. Auch der Bereich der Gesundheits- und Forschungszwecke wird hervorgehoben. Hier erhofft sich die Kommission von künftigen Leitlinien des EDSA eine innereuropäische Vereinheitlichung, wozu die Kommission dem EDSA bereits ihre Unterstützung zusagt.

Die Kommission hat in ihrer Einschätzung zur Sicherstellung eines angemessenen Datenschutzes hervorgehoben, dass dazu auch die Bereitstellung ausreichender personeller, finanzieller und technischer Ressourcen für die Ausstattung der Datenschutzbehörden erforderlich ist. Sie beurteilt die entsprechende Situation in den Mitgliedstaaten als uneinheitlich und aus Sicht der Kommission als noch nicht zufriedenstellend. Dies verbindet die Kommission mit dem ausdrücklichen Appell an die Mitgliedstaaten, den Datenschutzaufsichten gemäß den gesetzlichen Vorgaben angemessene Ressourcen zur Verfügung zu stellen.

In der Analyse hebt die Kommission positiv hervor, dass mit der DSGVO das Thema des Datenschutzes und die Kenntnis der den Einzelnen zustehenden Rechte stärker in das Bewusstsein der Menschen gerückt ist. Die durch die DSGVO ausgeweitete Befähigung von Betroffenen, über ihre Daten und deren Übertragung entscheiden zu können sowie die Nutzung der Rechte bis hin zur gerichtlichen Geltendmachung, findet die Zustimmung der Kommission. Insbesondere werden die Rechte auf Zugang zu den eigenen personenbezogenen Daten, auf Berichtigung und Löschung von Daten, auf Datenübertragung, auf Widerspruch

gegen Verarbeitungen und die Möglichkeit der Beschwerde bei den Datenschutzaufsichten hervorgehoben.

Seitens der Kommission wird bei der Betrachtung der DSGVO ebenfalls deren Technologieneutralität angesprochen. Die Kommission sieht dadurch die Möglichkeit gegeben, auch neue Technologien, die sich noch in der Entwicklung befinden, in den durch die DSGVO gewährleisteten Datenschutz einzubeziehen.

Mit dem Themenbereich der Datenübermittlung in ein europäisches oder außereuropäisches Ausland spricht die Europäische Kommission ein, auch für die kirchlichen Stellen in der Zusammenarbeit mit ihren Dienstleistern und ausländischen Vertragspartnern, wichtiges Thema an. Die Entwicklungen in der EU zu diesen Themen werden daher gleichfalls vom Katholischen Datenschutzzentrum beobachtet und deren mögliche Auswirkungen auf den katholischen Bereich analysiert. Die Kommission weist zu diesem Thema auf den Nutzen der Angemessenheitsbeschlüsse der Kommission für die Datenübermittlung in Drittländer hin, etwa den Beschluss zu Japan im Jahr 2019. Aufgrund des Austritts des Vereinigten Königreichs Großbritannien und Nordirland (sogenannter „Brexit") besteht die Notwendigkeit, den Austausch personenbezogener Daten auf eine angemessene rechtliche Grundlage zu stellen, wobei ein Angemessenheitsbeschluss eine mögliche Lösung darstellen kann, sofern die dafür erforderlichen Kriterien im Vereinigten Königreich erfüllt werden können.[3]

Daneben sieht die Kommission auch die Nutzung der Standardvertragsklauseln als ein wesentliches Instrument im Datenverkehr an, insbesondere auch im grenzüberschreitenden Bereich. Sie sieht sich dabei in der Pflicht, die Standardvertragsklauseln stetig weiterzuentwickeln und zu aktualisieren.[4] Auch die Übermittlung auf Basis von angemessenen Datenschutzgarantien steht im Blickpunkt der Überlegungen der Kommission.

Als Ziele benennt die Europäische Kommission u. a. die bessere Durchsetzung der DSGVO, eine Verbesserung des Datenschutzes, die Schaffung einer gemeinsamen europäischen Datenschutzkultur und die Verbesserung der Bearbeitung grenzüberschreitender Vorgänge. Hierzu erklärte die Kommission ihre Absicht, im Dialog mit den Mitgliedstaaten dazu beitragen zu wollen, die Vorgaben der DSGVO in Europa umzusetzen.

[3] Siehe dazu auch Abschnitt 1.1.1 in diesem Jahresbericht.
[4] Siehe dazu auch Abschnitt 1.1.3 in diesem Jahresbericht.

1.1.3 Aktualisierung der Standardvertragsklauseln der EU-Kommission

Die im Berichtszeitraum aktuellen Standardvertragsklauseln der EU-Kommission hatte diese durch Entscheidung vom 15.06.2001[5] und Beschluss vom 05.02.2010[6] in Kraft gesetzt. Diese Klauseln basieren noch auf den datenschutzrechtlichen Vorgaben der Datenschutzrichtlinie 95/46/EG und mussten daher an die neue Rechtslage der DSGVO angepasst werden. Seit der Anwendbarkeit der DSGVO im Mai 2018 war eine Aktualisierung der bisherigen Standardvertragsklauseln erwartet worden.

Mit Datum vom 12.11.2020 hat die EU-Kommission einen Entwurf für neue Standardvertragsklauseln vorgelegt[7], die die Vorgaben der DSGVO umsetzen und die bestehenden Standardvertragsklauseln modernisieren. Im Rahmen einer öffentlichen Konsultation zum Entwurf der neuen Klauseln konnten bis zum 10.12.2020 Rückmeldungen bei der EU-Kommission eingereicht werden.

Derzeit werden die Rückmeldungen ausgewertet. Eine Veröffentlichung der überarbeiteten Klauseln wird voraussichtlich im Jahr 2021 erfolgen.

1.1.4 Beratungen zur e-Privacy-Verordnung dauern an

Die e-Privacy-Verordnung („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)")[8] sollte eigentlich schon parallel zur DSGVO im Mai 2018 in Kraft treten.[9] Auch im Berichtszeitraum gab es verschiedene Initiativen, das Gesetzgebungsverfahren voranzubringen. Es fehlt aber noch die gemeinsame Position des EU-Ministerrates für die Trilog-Verhandlungen.[10] Der weitere zeitliche Ablauf des Gesetzgebungsverfahrens ist daher weiter ungewiss.

Damit können die sich aus der neuen Verordnung ergebenden Auswirkungen auf die verschiedenen Formen der Datenverarbeitung durch kirchliche Stellen auch weiterhin noch nicht beurteilt werden.

---

5 Entscheidung der Kommission vom 15.06.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (2001/497/EG), geändert durch die Entscheidung der Kommission vom 27.12.2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2004/915/EG) und den Durchführungsbeschluss (EU) 2016/2297 der EU-Kommission vom 16.12.2016.

6 Beschluss der EU-Kommission vom 05.02.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (2010/87/EU), geändert durch den Durchführungsbeschluss (EU) 2016/2297 der EU-Kommission vom 16.12.2016.

7 "Commission Implementing Decision (EU) .../... of XXX on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council" incl. Annex, Ref. Ares(2020)6654686 - 12/11/2020.

8 Entwurf der Europäischen Kommission vom 10.02.2017, COM (2017) 10.

9 Siehe hierzu auch Abschnitt 1.1.1 des Jahresberichts 2019.

10 Im Februar 2021 hat sich der EU-Ministerrat auf eine gemeinsame Position geeinigt, so dass die Trilog-Verhandlungen starten können.

1.1.5 EU-Richtlinie zum Schutz von Personen, die Verstöße melden

Mit der Richtlinie (EU) 2019/1937 vom 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, soll es Hinweisgebern ermöglicht werden, risikolos auf ungesetzliche Zustände hinzuweisen.[11] Die Umsetzung der Richtlinie in das jeweilige nationale Recht soll durch die Mitgliedstaaten bis zum 17.12.2021 erfolgen.

Im Berichtszeitraum wurde von der Bundesregierung aber noch kein Gesetzentwurf zur Umsetzung der EU-Richtlinie vorgelegt. Aufgrund der Umsetzungsfrist bis zum 17.12.2021 und der Bundestagswahl im September 2021 wird die Bundesregierung wahrscheinlich im Frühjahr 2021 einen Entwurf für die Umsetzung der Richtlinie vorlegen.

Da die Umsetzung dieser Richtlinie in nationales Recht dann auch die kirchlichen Einrichtungen betrifft, wird mit der Vorlage des Gesetzentwurfes eine voraussichtlich eher kurze Vorbereitungszeit auf die geplanten und dann spätestens zum Dezember 2021 in Kraft gesetzten nationalen Regelungen beginnen. Das Katholische Datenschutzzentrum wird diesen Prozess weiter beobachten, da diese Thematik in der Ausgestaltung der Meldesysteme viele datenschutzrechtliche Berührungspunkte hat.

1.2 Gesetzgeberische Entwicklungen in der Bundesrepublik Deutschland

Auf nationaler Ebene gab es mehrere, datenschutzrechtlich relevante Gesetzgebungsvorhaben, von denen einige hier erwähnt werden sollen.

1.2.1 Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze

Im Berichtszeitraum hat die Bundesregierung ihre Pläne konkretisiert, ein registerübergreifendes Identitätsmanagement in der Verwaltung einzuführen. Mit dem „Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung“ als Teil des Registermodernisierungsgesetzes plant die Bundesregierung Veränderungen der in der Verwaltung geführten Register.

Als eine der geplanten Maßnahmen in diesem Rahmen soll zukünftig die Steuer-Identifikationsnummer als übergreifendes Ordnungsmerkmal für verschiedene Register genutzt werden. Damit ist aber auch die Gefahr verbunden, dass die Daten dieser über 50 Register zukünftig viel leichter miteinander verknüpft werden können. Dadurch wächst die Gefahr der Erstellung umfassender Persönlichkeitsprofile.

[11] Siehe hierzu die ausführliche Darstellung in Abschnitt 1.1.3 des Jahresberichts 2019.

Da das Bundesverfassungsgericht in den bisherigen Entscheidungen bei Fragen zentraler Personenkennzeichen hohe Maßstäbe angesetzt hat, gibt es aus datenschutzrechtlicher Sicht noch Verbesserungsbedarf an dem Gesetzentwurf.[12]

1.2.2 Sicherung von Patientenunterlagen im Falle der Insolvenz des Krankenhausbetreibers

Mit Datum vom 29.09.2020 legten die Fraktionen der CDU und der FDP einen Gesetzentwurf für ein „Drittes Gesetz zur Änderung des Krankenhausgestaltungsgesetzes des Landes Nordrhein-Westfalen“[13] vor.

Mit dem Gesetzentwurf soll die neue Vorschrift des § 34c Krankenhausgestaltungsgesetz Nordrhein-Westfalen (KHGG NRW) mit dem folgenden Inhalt eingefügt werden:

„§ 34c
Sicherung von Patientenunterlagen

Der Krankenhausträger hat Maßnahmen zu treffen, dass im Falle der Schließung eines Krankenhauses aufgrund einer drohenden Zahlungsunfähigkeit die dort geführten Patientenunterlagen entsprechend ihrer individuellen Aufbewahrungsdauer unter Beachtung der datenschutzrechtlichen Vorgaben, insbesondere zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit aufbewahrt werden können, und dass Ansprüche der Patientinnen und Patienten auf jederzeitige Durchsetzung ihrer Rechte nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72, ABl. L 127 vom 23.5.2018, S. 2) sowie ihrer Rechte nach dem Bürgerlichen Gesetzbuch nicht beeinträchtigt werden. Maßnahmen im Sinne des Satzes 1 sind insbesondere Sicherungsmaßnahmen, die einen Zugang zu, einen Zugriff auf und die Kenntnisnahme von Patientenunterlagen durch unbefugte Personen verhindern sowie die in regelmäßigen Abständen durchgeführte Prüfung, ob Patientenunterlagen vernichtet werden können. Der Krankenhausträger weist die getroffenen Sicherungsmaßnahmen entsprechend der individuellen Aufbewahrungsdauer ab dem [einsetzen: Datum des Inkrafttretens dieses Gesetzes] und sodann alle zwei Jahre gegenüber der zuständigen oberen Aufsichtsbehörde gemäß § 11 Absatz 4 nach. Es ist sicherzustellen, dass die Maßnahmen auch im Falle der Schließung eines Krankenhauses während der individuellen Aufbewahrungsdauer aufrechterhalten werden können.“

[12] Siehe auch die Entschließung „Registermodernisierung verfassungskonform umsetzen!“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26.08.2020.

[13] Landtags-Drucksache 17/11162; der Gesetzentwurf wurde mittlerweile vom Landtag verabschiedet und im Gesetzblatt verkündet (Gesetz vom 09.03.2021 – GV NRW 2021 Nr. 22, S.272-275; Berichtigung vom 26.03.2021 – GV NRW 2021 Nr. 31, S.394).

Einer der Auslöser dieser Gesetzesänderung war wohl auch ein Video auf Youtube im Mai 2020, in dem ein Youtuber über verlassene Orte berichtete, im konkreten Fall über ein leerstehendes Krankenhausgebäude in NRW.

Das ehemals kirchliche Krankenhaus war an einen privaten Krankenhausbetreiber verkauft worden. Die Betreiberin, eine Krankenhausträgergesellschaft dieses privaten Konzerns, meldete einige Jahre später im Jahr 2010 Insolvenz an und stellte den Betrieb im selben Jahr ein. Sie gab die Immobilie an eine Grundstücksgesellschaft zurück, die ebenfalls eine 100-prozentige Tochter des gleichen Konzerns ist. Die in Papierform geführten Patientenakten (Behandlungsdokumentationen) wurden weiterhin in dem jetzt leerstehenden Gebäude verwahrt.

Der Youtuber betrat im Jahr 2020 das fast 10 Jahre leerstehende Gebäude und fand die dort immer noch lagernden Patientenakten. Das dazu veröffentliche Video fand ein entsprechendes Medienecho.

Da der Krankenhauskonzern – als Muttergesellschaft sowohl für die insolvente Krankenhausbetreibergesellschaft als auch für die Grundstücksgesellschaft – seinen Sitz in Hamburg hat, nahm der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit den Sachverhalt auf und forderte den Konzern erfolglos zur Sicherung der Akten auf. Die folgende Anordnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gegen die Grundstücksgesellschaft zur Sicherung der Akten wurde gerichtlich angegriffen. Das Verwaltungsgericht Hamburg[14] gab dem Antrag der Grundstücksgesellschaft statt und führte aus, dass es zu einer Verarbeitung im datenschutzrechtlichen Sinne einer Handlung bedürfe und nicht nur eines Zustands. Hier seien die Akten der Grundstücksverwaltung aber einfach nur mit dem Grundstück übergeben worden. Die Grundstücksgesellschaft habe keine Verarbeitung der Daten vorgenommen oder vornehmen wollen. Das OVG Hamburg[15] bestätigte diese Sicht durch Beschluss in der zweiten Instanz.[16]

Diese Beschlüsse bewirken im Ergebnis, dass nach der Insolvenz der Krankenhausbetreibergesellschaft als bisherigem Verarbeiter kein neuer Verantwortlicher vorhanden ist, der für den Schutz der personenbezogenen Daten sorgt und auch Betroffenenrechte erfüllen kann, wie z. B. das Recht auf Auskunft[17] über die eigenen Daten.

Um zukünftig solche Fälle zu vermeiden, wird für NRW mit dem neuen § 34c KHGG NRW die gesetzliche Verpflichtung geschaffen, für den Fall der Insolvenz geeignete Maßnahmen zu treffen, die den Schutz der Patientendaten sicherstellen.

[14] VG Hamburg, Beschluss vom 30.7.2020 (17 E 2756/20).
[15] OVG Hamburg, Beschluss vom 15.10.2020 (5 Bs 152/20).
[16] Ausführlich zum Sachverhalt: Jahresbericht 2020 des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, S. 111 - 113.
[17] Zum Recht aus Auskunft siehe auch Abschnitt 3.4.1 dieses Jahresberichts.

1.3 Gesetzgeberische Entwicklungen in der römisch-katholischen Kirche

Im kirchlichen Bereich sind im Berichtszeitraum ebenfalls neue Regelungen in Kraft getreten oder verabschiedet worden, die datenschutzrechtliche Vorgaben enthalten.

1.3.1 Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens

In den fünf nordrhein-westfälischen (Erz-)Diözesen gab es bisher schon eine „Ordnung zum Schutz von Patientendaten in Katholischen Krankenhäusern (PatDSO)".[18] Diese enthielt kirchenspezifische Regelungen zum Datenschutz von Patienten in den katholischen Krankenhäusern.

Nach der Überarbeitung der „Anordnung über den kirchlichen Datenschutz (KDO)" zum „Gesetz über den Kirchlichen Datenschutz (KDG)" im Zuge der Einführung der Datenschutz-Grundverordnung auf europäischer Ebene im Mai 2018 bestand der Bedarf an einer Überarbeitung der bisherigen kirchlichen Regelungen zum Patientendatenschutz, die noch auf der KDO basierten.

Im Ergebnis ist nunmehr nicht ein neues Gesetz zum Schutz von Patientendaten (PatDSG) als eine umfassende kircheneigene spezifische Grundlage für den Datenschutz in katholischen Krankenhäusern geschaffen worden. Der Gesetzgeber hat sich nach intensiven Beratungen für eine enger gefasste bereichsspezifische Regelung zum Schutz von Patientendaten in der Seelsorge entschieden und das „Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens (Seelsorge-PatDSG)" erarbeitet.

Diese Gesetzesregelung ist zunächst als Musterfassung von der Vollversammlung des VDD im November 2020 verabschiedet worden. In den (Erz-)Diözesen in Nordrhein-Westfalen ist das Seelsorge-PatDSG als diözesanes Gesetz in Kraft gesetzt worden beziehungsweise wird es noch in Kraft gesetzt werden.[19]

Dem weiter gefassten Regelungsansatz der bisherigen PatDSO, die neben Regelungen zur Seelsorge im Krankenhaus auch Vorgaben zum Schutz der Patientendaten inklusive deren Übermittlung an Dritte enthielt, ist das Seelsorge-PatDSG damit nicht gefolgt. Soweit die spezialgesetzlichen Bestimmungen der PatDSO nicht mehr gelten, sind künftig – mit Ausnahme des Bereichs der Seelsorge – allein die Rechtsvorschriften des KDG maßgebend. Dies führt aber zu keiner Minderung des Datenschutzniveaus in den katholischen Krankenhäusern, da das KDG auch entsprechende Vorgaben für bisher in der PatDSO geregelte Bereiche enthält, etwa zu betrieblichen Datenschutzbeauftragten, Auf-

[18] Vergleichbare Regelungen gab es – teilweise auch aufgrund schon bestehender gleichlautender staatlicher Regelungen auf Ebene der Bundesländer - aber nicht in allen 27 (Erz-)Diözesen.

[19] Amtsblatt des Erzbistums Köln 2021, Nr. 40 (S. 50 f); Kirchliches Amtsblatt für die Erzdiözese Paderborn 2021, Nr. 25 (S. 42 f); Kirchlicher Anzeiger für die Diözese Aachen 2021, Nr. 31 (S. 61 f); Kirchliches Amtsblatt Bistum Essen 2021, Nr. 19 (S. 33 f); Kirchliches Amtsblatt Bistum Münster 2021, Art. 51 (S. 141 ff).

tragsdatenverarbeitung, Datennutzung bei Forschungsvorhaben oder Auskunftsrechten. Damit ist weiterhin ein adäquates Schutzniveau in den katholischen Krankenhäusern sichergestellt.

Das Seelsorge-PatDSG enthält nur noch Regelungen für die Datenverarbeitungen im Zusammenhang mit der Krankenhausseelsorge. In § 2 Abs. 1 lit. b) Seelsorge-PatDSG wird klargestellt, dass es sich bei den Daten, welche von der Krankenhausseelsorge verwendet werden, um besondere Kategorien personenbezogener Daten in Form von Gesundheitsdaten gemäß § 4 Nr. 17 KDG handelt.[20] Diese Daten unterliegen daher nach dem KDG den strengeren Vorgaben bezüglich einer Datenübermittlung, insbesondere denjenigen, die in § 11 KDG niedergelegt sind.

Der Gesetzgeber unterscheidet jetzt zwischen Einrichtungen, bei denen eine sog. „implementierte Krankenhausseelsorge" gemäß § 3 Seelsorge-PatDSG eingeführt ist und Einrichtungen, die eine solche implementierte Krankenhausseelsorge nicht eingeführt haben und deren Vorgaben für die Krankenhausseelsorge sich in § 4 Seelsorge-PatDSG wiederfinden.

In der bisherigen PatDSO waren diese Formen der Seelsorge nicht erwähnt. Die PatDSO enthielt Regelungen, wonach eine Übermittlung zur jeweiligen Aufgabenerfüllung erforderlich sein musste. Alternativ konnte die Übermittlung auf eine Rechtsvorschrift oder die Einwilligung des Patienten gestützt werden. Eine Unterrichtung des Seelsorgers der Kirchengemeinde war nur unter der Voraussetzung, dass der Patient nicht widersprochen hatte, erlaubt. Bedingung war jedoch, dass der Patient bei seiner Aufnahme ausdrücklich auf dieses Widerspruchsrecht hingewiesen worden war. Eine Übermittlung war in den Fällen unzulässig, wenn Anhaltspunkte vorlagen, dass sie nicht angebracht sein würde.

Der Gesetzgeber löst sich mit dem Seelsorge-PatDSG von diesen Vorgaben der PatDSO und setzt für die Anwendung des § 3 Seelsorge-PatDSG voraus, dass es ein Modell der Krankenhausseelsorge gibt, in welchem die Seelsorge in die konzeptionelle Aufstellung des Krankenhauses implementiert ist. Dies kann sich darin ausdrücken, dass der Krankenhausseelsorger im Einzelfall je nach Erkrankung in das Behandlungsteam, welches sich mit der Behandlung des Patienten befasst, eingebunden wird. Der Krankenhausseelsorger kann im Rahmen eines solchen Konzeptes z. B. auch den Ethikkomitees von Krankenhäusern angehören.

Im Fall der nichtimplementierten Seelsorge gemäß § 4 Seelsorge-PatDSG trägt der Gesetzgeber der Situation Rechnung, dass auch Seelsorgeangebote, die nicht die Voraussetzungen des § 3 Seelsorge-PatDSG erfüllen, in den Krankenhäusern existieren. Das Gesetz sieht daher vor, dass bestimmte im Gesetz aufgeführte Informationen an die Seelsorger weitergegeben werden können, wenn der Patient im Krankenhaus seine Religion oder Konfession angibt und dabei darauf hingewiesen wird, dass diese Angabe freiwillig ist und dass seine Daten im

[20] In § 2 Abs. 1 lit. b) Seelsorge-PatDSG wird der im KDG nicht enthaltene Begriff der „Patientendaten" eingeführt.

gesetzlich definierten Umfang an den Krankenhausseelsorger weitergegeben werden, soweit er nicht widerspricht.

§ 5 Seelsorge-PatDSG stellt schließlich noch klar, dass eine ausdrückliche Einwilligung des Patienten erforderlich ist, um die in der Vorschrift genannten Daten an die Heimat-Kirchengemeinde übermitteln zu können. Dabei kann die bloße Angabe der Religion beziehungsweise Konfession im Behandlungsvertrag nicht als Nachweis einer Einwilligung des Patienten angesehen werden. Eine regelmäßige Übermittlung von Daten an die Heimat-Kirchengemeinde ohne die Einwilligung des jeweiligen Patienten ist damit ausgeschlossen.

„Durch die Weichenstellung im Gesetz, ob eine Einrichtung eine implementierte Seelsorge eingerichtet hat ..., müssen sich die katholischen Einrichtungen des Gesundheitswesens Gedanken darüber machen, ob und inwieweit die Krankenhausseelsorge zu einem Bestandteil des Krankenhauses werden soll ...“

Durch die Weichenstellung im Gesetz, ob eine Einrichtung eine implementierte Seelsorge eingerichtet hat oder nicht und damit die Regelungen des § 3 Seelsorge-PatDSG oder des § 4 Seelsorge-PatDSG greifen, müssen sich die katholischen Einrichtungen des Gesundheitswesens Gedanken darüber machen, ob und inwieweit die Krankenhausseelsorge zu einem Bestandteil des Krankenhauses werden soll, um die Vorgaben für das Modell der implementierten Seelsorge zu erfüllen. Für eine Einbeziehung der Krankenhausseelsorge und eine Berechtigung zur Übermittlung von Daten ist der Wille des Patienten jederzeit zu berücksichtigen.

Aus Sicht des Katholischen Datenschutzzentrums wird eine Herausforderung für die katholischen Einrichtungen des Gesundheitswesens unter diesem Gesetz sein, die gemäß den Regelungen der §§ 3 und 4 Seelsorge-PatDSG notwendige Information beziehungsweise Einwilligung des Patienten datenschutzgerecht und damit gesetzeskonform zu geben beziehungsweise einzuholen. Ob die Erklärung im Behandlungsvertrag wirklich ausreicht, wird im konkreten Einzelfall der Verwendung im Vertrag jeweils zu untersuchen sein. Es wird im Einzelfall zu untersuchen sein, ob sich ein Patient im Rahmen der Darstellungen über eine implementierte Seelsorge wirklich die Gedanken macht, dass seine Gesundheitsdaten dem Krankenhausseelsorger offenbart werden. Die implementierte Seelsorge stellt jedenfalls hohe Anforderungen an den Umfang und die Qualität der Informationen, so dass der Patient eine hinreichende Aufklärung erhält und auf dieser Basis im konkreten Fall reagieren und entscheiden kann.

Auch im Fall der nichtimplementierten Seelsorge sind die mit der Information verbundenen Erklärungsinhalte so sicherzustellen, dass der Patient in informierter Weise über die Ausübung seines Widerspruchsrechts entscheiden kann. Darüber hinaus kann es bedenklich sein, dass Informationen über den Patienten weitergegeben werden dürfen, auch wenn er sich nicht dazu geäußert hat. Daher muss dem Patienten zuvor die Tragweite der Angabe von Religion oder Konfession in klarer Weise verdeutlicht werden.

Das Katholische Datenschutzzentrum wird die Einführung des Seelsorge-PatDSG begleiten und sich die Umsetzung in den betroffenen kirchlichen Einrichtungen anschauen.

1.3.2 Evaluierung des Gesetzes über den Kirchlichen Datenschutz

Das Gesetz über den Kirchlichen Datenschutz enthält in § 58 Absatz 2 KDG die Vorgabe, dass das Gesetz innerhalb einer Frist von drei Jahren nach dessen Inkrafttreten überprüft werden soll. Zur Umsetzung dieses gesetzlichen Auftrages haben die (Erz-)Bischöfe auf der Ebene des Verbandes der Diözesen Deutschlands eine Arbeitsgruppe eingerichtet, die sich mit den Rückmeldungen zu den geltenden Rechtsnormen und mit möglichen, sich aus der Rechtsanwendung ergebenden Novellierungsbedürfnissen befasst.

Diese Arbeitsgruppe hat ihre Tätigkeit im Berichtsjahr 2020 aufgenommen. Zu den konkreten Überlegungen und den sich möglicherweise aus den Ergebnissen der Beratungen ergebenden Novellierungsvorschlägen kann im derzeit laufenden Prozess der Analyse noch keine Aussage getroffen werden. Die katholischen Datenschutzaufsichten beraten die Arbeitsgruppe und bringen so ihre Erfahrungen aus der Praxis der Gesetzesanwendung des KDG mit ein. Im Jahr 2021 will die Arbeitsgruppe ein Dokument mit den Ergebnissen ihrer Überlegungen vorlegen.

Das Katholische Datenschutzzentrum wird diesen Prozess über die Konferenz der Diözesandatenschutzbeauftragten, aber auch beratend als Verbandsdatenschutzbeauftragter und damit Datenschutzaufsicht für den Verband der Diözesen Deutschlands, begleiten.

1.3.3 Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz

Mit dem Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG) liegt im Berichtszeitraum ein weiteres Gesetz zur Inkraftsetzung durch die einzelnen Diözesen bereit. Für die (Erz-)Diözesen in NRW soll die durch die Vollversammlung des Verbandes der Diözesen Deutschlands vom 23.11.2020 beschlossene Fassung zum 01.02.2021 in diözesanes Recht umgesetzt werden.

Die Arbeit der Datenschutzaufsichten der katholischen Kirche ist ebenso wie die Arbeit der Landesdatenschutzbeauftragten und des Bundesdatenschutzbeauftragten an gesetzliche Verfahrensvorgaben gebunden, welche sich (auch) aus den Verwaltungsverfahrensgesetzen ergeben. Ein spezielles Gesetz zum Ablauf eines Verwaltungsverfahrens für die Datenschutzaufsichten kannte die katholische Kirche bislang nicht. Das KDS-VwVfG soll nun die spezielle Grundlage für das Verwaltungshandeln der Datenschutzaufsichten liefern und orientiert sich dabei eng an dem Verwaltungsverfahrensgesetz des Bundes. Anders als die Evangelische Kirche Deutschlands hat die katholische Kirche den Anwendungsbereich des Gesetzes auf die Arbeit der Datenschutzaufsichten beschränkt und kein allgemeines Verwaltungsverfahrensgesetz erlassen.

1.3.4 Umsetzung des § 29 KDG-Gesetzes in den nordrhein-westfälischen (Erz-)Diözesen

Bei einer Auftragsverarbeitung sieht § 29 Abs. 3 KDG als mögliche Grundlagen für die Auftragsverarbeitung neben dem Abschluss eines entsprechenden Auftragsverarbeitungsvertrages auch die Nutzung eines „anderen Rechtsinstruments" vor. Mit dem „Gesetz zur Regelung des Rechtsinstruments nach § 29 Gesetz über den Kirchlichen Datenschutz (KDG)" (§ 29-KDG-Gesetz) hat der kirchliche Gesetzgeber die notwendige kirchliche Grundlage geschaffen, damit das Instrument im kirchlichen Bereich auch genutzt werden kann. Dabei gibt das § 29-KDG-Gesetz aber nur den Rahmen für die eigentlichen Regelungen der konkreten Auftragsverarbeitungen vor. Die Regelungen des „anderen Rechtsinstruments" müssen – wie bei einem Auftragsverarbeitungsvertrag – auf den konkreten Sachverhalt abgestimmt sein.[21]

Auch in den Fällen, wo eine kirchliche Stelle eine (Dienst-)Leistung für eine andere kirchliche Stelle erbringt, muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden, wenn die Voraussetzungen einer Auftragsverarbeitung vorliegen. Der Charakter als rein innerkirchlicher Austausch der (Dienst-)Leistung, z. B. zwischen zwei selbständigen Kirchengemeinden, entbindet nicht von der Notwendigkeit, einen Auftragsverarbeitungsvertrag abzuschließen.

Zur Ausführung des Gesetzes und zur Festlegung aller notwendigen Inhalte zur Auftragsvereinbarung sieht das § 29-KDG-Gesetz in § 3 des Gesetzes eine Ermächtigung des Generalvikars zum Erlass von Verwaltungsverordnungen vor.

Die Mindestvorgaben, die das „andere Rechtsinstrument" inhaltlich abdecken muss, sind nach § 29 Abs. 3 und 4 KDG identisch mit denen eines Auftragsverarbeitungsvertrages. Aus dem Zusammenspiel zwischen § 29-KDG-Gesetz und der konkreten Verordnung ergibt sich die rechtliche Grundlage für eine Auftragsverarbeitung.

Mittlerweile haben die nordrhein-westfälischen (Erz-)Diözesen jeweils für sich ein entsprechendes § 29-KDG-Gesetz in Kraft gesetzt und auch die notwendigen Verordnungen zur Ausfüllung des Gesetzes auf den Weg gebracht.

Bei der Umsetzung der Verordnungen wurden unterschiedliche Schwerpunkte in der Darstellung und Gliederung der Inhalte gewählt. Unabhängig von der konkreten Umsetzung in der Verordnung müssen aber letztendlich mit den Regelungen, die für eine konkrete Verarbeitung personenbezogener Daten im Auftrag gelten sollen, alle in § 29 KDG genannten Mindestinhalte einer Vereinbarung zur Auftragsverarbeitung vorliegen. Dabei spielt es keine Rolle, ob alles in der Umsetzungsverordnung zum § 29-KDG-Gesetz geregelt ist oder noch individualvertraglich ergänzt wird. In der Summe müssen die Regelungen vorhanden sein.

[21] Ausführlich zu § 29 Abs. 3 KDG und dem „anderen Rechtsinstrument": Abschnitt 3.3 des Jahresberichts 2019.

Das Katholische Datenschutzzentrum wird sich die Umsetzung der Vorgaben des § 29 KDG an Auftragsverarbeitungen in der Praxis anschauen und dabei auch die Umsetzung des § 29-KDG-Gesetzes mit einbeziehen.

1.4 Gesetzgeberische Entwicklungen in der Evangelischen Kirche in Deutschland (EKD)

Im Berichtszeitraum hat die EKD als solche keine weiteren eigenständigen Regelungen im Kernbereich des Datenschutzrechts getroffen. Weitere Landeskirchen haben aber landesspezifische Ausführungsbestimmungen zum Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) erlassen beziehungsweise geändert.

Das Katholische Datenschutzzentrum stimmt sich regelmäßig mit der für die Landeskirchen und Diakonien in NRW zuständigen Außenstelle Dortmund des Beauftragten für den Datenschutz der EKD und mit dem Beauftragten selbst ab, um aktuelle Entwicklungen auf Seiten der EKD zu verfolgen.[22]

1.5 Aus der Arbeit des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss hat sich im Berichtszeitraum sowohl zu wichtigen grundlegenden Fragen der Auslegung der DSGVO geäußert als auch aktuelle Entwicklungen mit Stellungnahmen begleitet.

So hat der Ausschuss unter anderem Leitlinien zur Einwilligung unter der DSGVO[23] oder zur Ausgestaltung der Anforderungen an Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[24] verabschiedet. Der Ausschuss hat auch Erklärungen zur Verarbeitung personenbezogener Daten im Zusammenhang mit Covid-19[25] oder zum EuGH-Urteil (Urteil des Europäischen Gerichtshofs) zur Ungültigkeit des Privacy Shield[26] abgegeben.

Die Veröffentlichungen des Europäischen Datenschutzausschusses fließen in die Arbeit des Katholischen Datenschutzzentrums ein und werden den kirchlichen Stellen und Einrichtungen – je nach Relevanz für den kirchlichen Bereich – auf unterschiedliche Art kommuniziert.

---

[22] Siehe auch Abschnitt 4.7.1 in diesem Bericht.

[23] Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1 vom 04.05.2020).

[24] Leitlinien 4/2019 zu Artikel 25 - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Version 2.0 vom 20.10.2020).

[25] Erklärung zur Verarbeitung personenbezogener Daten im Zusammenhang mit COVID-19 vom 19.03.2020.

[26] Erklärung zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 – Data Protection Commissioner gegen Facebook Ireland und Maximilian Schrems vom 17.07.2020 inkl. FAQ vom 23.07.2020.

Gerade diese Kommunikation der Veröffentlichungen des EDSA zusammen mit einer Beschreibung der Bedeutung der Veröffentlichung für die kirchlichen Einrichtungen will das KDSZ zukünftig noch verstärken.

1.6 Modernisierung der „Konvention 108" des Europarates

Weniger bekannt als die Datenschutz-Grundverordnung, handelt es sich bei der Konvention 108 des Europarates dennoch um einen nicht unbedeutenden Baustein in der Entwicklung des europäischen Datenschutzrechts. Diese Konvention stellte im Jahr 1981 das erste rechtsverbindliche zwischenstaatliche Übereinkommen zum Datenschutz dar. Sie enthielt bereits wichtige Grundsätze des Datenschutzrechts. Die Bedeutung des Übereinkommens für die Entwicklung des Datenschutzes weltweit zeigt sich auch daran, dass neben den Mitgliedstaaten der Europäischen Union auch außereuropäische Länder diese Konvention ratifiziert haben.

„Diese Konvention stellte im Jahr 1981 das erste rechtsverbindliche zwischenstaatliche Übereinkommen zum Datenschutz dar."

Aufgrund ihres bereits länger zurückliegenden Entstehungszeitpunkts war eine Anpassung der Konvention 108[27], einschließlich ihres Zusatzprotokolls aus dem Jahr 2001, an die zwischenzeitlichen Entwicklungen erforderlich geworden. Als Ergebnis mehrjähriger Verhandlungen konnten sich die Konventionsstaaten auf ein Änderungsprotokoll einigen. Dieses beinhaltete unter anderem die Stärkung der Betroffenenrechte und die Einführung einer Meldepflicht für Verantwortliche bei Verletzungen des Datenschutzes an eine Aufsichtsbehörde. Weiterhin wurde die Schaffung von unabhängigen Aufsichtsbehörden für alle Konventionsstaaten verpflichtend. Mit der Erweiterung der Bestimmungen durch das Änderungsprotokoll wurde zudem die Hoffnung verbunden, dass das Datenschutzniveau insgesamt, insbesondere in den Konventionsstaaten, erhöht und dass die Übermittlung personenbezogener Daten erleichtert wird.

Der Botschafter der Ständigen Vertretung der Bundesrepublik Deutschland beim Europarat hatte am 10.10.2018 im Namen der Bundesrepublik Deutschland das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (sog. Konvention 108 des Europarates) unterzeichnet. Die Bundesrepublik Deutschland bekannte sich damit zu einem hohen Schutzstandard für die Persönlichkeitsrechte und stärkte zugleich die internationale Zusammenarbeit im Bereich des Datenschutzes. Rechtlich waren jedoch noch weitere Schritte erforderlich. Der Rat der Europäischen Union hatte dazu die Mitgliedstaaten der Europäischen Union ermächtigt, das Änderungsprotokoll zu ratifizieren. Nach Artikel 59 Absatz 2 Satz 1 des Grundgesetzes ist die Zustimmung der gesetzgebenden Körperschaften zu dem Änderungsprotokoll Voraussetzung für dessen Ratifikation.

Mit dem „Gesetz zu dem Protokoll vom 10. Oktober 2018 zur Änderung des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen

[27] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten", sog. „Konvention 108" des Europarates.

bei der automatischen Verarbeitung personenbezogener Daten“ vom 12.11.2020 (BGBl. 2020 II S. 874) wurde diesem Anliegen Rechnung getragen. Der Bundestag hat mit Zustimmung des Bundesrates das Gesetz beschlossen, mit welchem dem in Straßburg am 10.10.2018 von der Bundesrepublik Deutschland unterzeichneten Protokoll zur Änderung des Übereinkommens vom 28.01.1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zugestimmt wird. Das Gesetz trat am Tag nach der Verkündung in Kraft.

1.7 Ökumenische Projektgruppe „Kirchliches Datenschutzmodell (KDM)“

Die im Vorjahr begonnene Arbeit am Kirchlichen Datenschutzmodell wurde im Jahr 2020 fortgesetzt. Dazu fanden mehrere Sitzungen der ökumenischen Projektgruppe statt, die Vertreter der katholischen Datenschutzaufsichten und Vertreter des Beauftragten für den Datenschutz der EKD sowie weiterer Datenschutzaufsichten evangelischer Landeskirchen umfasst. Das Katholische Datenschutzzentrum bringt sich hier durch den Diözesandatenschutzbeauftragten, der zusammen mit Michael Jacob, dem Beauftragten für den Datenschutz der EKD, die Leitung der ökumenischen Projektgruppe übernommen hat, und durch einen Referenten, der die operative Projektleitung zusammen mit einem Vertreter des Beauftragten für den Datenschutz der EKD wahrnimmt, ein.

Gemeinsam wurde ein an das Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder (DSK) angelehntes Vorgehen beschrieben, welches zukünftig als ein Handwerkszeug für Verantwortliche, betriebliche Datenschutzbeauftragte sowie die Aufsichtsbehörden dienen soll.

Die Datenschutzaufsichtsbehörden erhalten ein Werkzeug, mit dem Prüfungen standardisiert durchgeführt werden können. Die kirchlichen Stellen können ihre gelebte Datenschutzpraxis durch Abgleich ihrer Maßnahmen mit dem KDM verbessern und überprüfen. Hierbei handelt es sich um ein Werkzeug zur Bestimmung risikoadäquater technischer und organisatorischer Schutzmaßnahmen, das von den Einrichtungen genutzt werden kann. Es besteht aber keine Verpflichtung der kirchlichen Stellen, gerade dieses Hilfsmittel für ihre eigene Arbeit zu nutzen.

Kurz gesagt beschreibt das KDM eine Methode, wie in einer gegebenen oder geplanten Situation von Verarbeitungen personenbezogener Daten über eine Analyse der Bedrohung von datenschutzrelevanten Gewährleistungszielen für jede im Verarbeitungsprozess beteiligte technische oder organisatorische Komponente die richtigen Schutzmaßnahmen aus einem vorgegeben Katalog (Referenzmaßnahmenkatalog beziehungsweise „Bausteine“) ausgewählt werden können.

Weil die Situationen von Verarbeitungen personenbezogener Daten im kirchlichen Umfeld sich teilweise von Situationen im außerkirchlichen Bereich unterscheiden können, wurde das KDM gegenüber dem SDM an manchen Stellen entsprechend neu formuliert. Die verfügbaren

Schutzmaßnahmen unterscheiden sich jedoch nicht, so dass die Referenzmaßnahmenkataloge praktisch unverändert übernommen werden.

Eine besondere Überarbeitung erfolgte bei der Anleitung zur Ermittlung und Behandlung von Risiken durch die Verarbeitung für die Betroffenen. Das Ergebnis ist eine eigenständige Richtline zur Risikoermittlung und Risikobehandlung, die auch eine Brücke zu den Begriffen der Datenschutz-Folgenabschätzung schlägt.

Die Projektgruppe hat sich im Laufe ihrer Arbeit mehrfach mit der Unterarbeitsgruppe SDM der DSK über Begriffe, Vorgehen und Zielrichtung von SDM und KDM abgestimmt. Auch zukünftig sollen so eine gemeinsame Zielrichtung und die Weiterentwicklung der Modelle sichergestellt werden.

Das KDM soll auf dem ökumenischen Datenschutztag im Frühjahr 2021, bei dem sich die Datenschutzaufsichten der katholischen und der evangelischen Kirche zu ihrem jährlichen Austausch treffen, verabschiedet und danach den kirchlichen Stellen präsentiert werden.

2 Ausgewählte Rechtsprechung zum Datenschutzrecht

Das Katholische Datenschutzzentrum hat im Berichtszeitraum die Rechtsprechung der Gerichte beobachtet, die Urteile zum Datenschutz erlassen haben oder deren Entscheidungen zumindest Auswirkungen auf datenschutzrechtlich relevante Sachverhalte hatten.

2.1 Europäischer Gerichtshof und nationale Gerichte

Von den unzähligen Urteilen auf europäischer und nationaler Ebene sollen hier nur zwei hervorgehoben werden. Weitere Urteile werden noch im Zusammenhang mit der Darstellung der Arbeit des Katholischen Datenschutzzentrums erwähnt.

2.1.1 Urteil des Europäischen Gerichtshofs vom 16.07.2020 (Rs. C-311/18 – Schrems II)

Eine der Entscheidungen im Berichtszeitraum, die eine bedeutende Auswirkung auf die Übermittlungen von personenbezogenen Daten in Drittländer hat und daher ein entsprechendes mediales Echo hervorgerufen hat, ist das Urteil der Großen Kammer des Europäischen Gerichtshofs vom 16.07.2020 in der Rechtssache C-311/18 (Schrems II).

Der Entscheidung liegt ein Vorabentscheidungsersuchen des irischen High Court zugrunde. In dem Verfahren vor den irischen Gerichten wollte Maximilian Schrems die irische Datenschutzaufsicht zum Handeln gegenüber Facebook bewegen, damit keine von ihm bei Facebook gespeicherten Daten mehr in die USA transferiert werden.

Zu entscheiden war insbesondere über die Auslegungen von Art. 3 Abs. 2, 25, 26 und 28 Abs. 3 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (als bis zum 25.05.2016 geltende Vorgängerregelung zur DSGVO) im Hinblick auf Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union. Weiterhin war über die Auslegung und die Gültigkeit des Beschlusses 2010/87/EU der Kommission vom 05.02.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG in der durch den Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16.12.2016 geänderten Fassung sowie über die Auslegung und die Gültigkeit des Durchführungsbeschlusses (EU) 2016/1250 der Kommission vom 12.07.2016 gemäß der Richtlinie 95/46/EG über die Angemessenheit des vom EU-US-Datenschutzschild (sog. „Privacy Shield“) gebotenen Schutzes zu befinden.

Auch wenn der Beginn der streitgegenständlichen Verfahren vor 2018 und damit vor Geltung der DSGVO lag, entschied der EuGH, dass die Vorlagefragen aufgrund der Verfahrensumstände anhand der Bestimmungen der DSGVO und nicht nach der Richtlinie 95/46/EG zu beantworten sind.

Er hat darüber hinaus entschieden, dass sich der Anwendungsbereich der europäischen Datenschutzregelungen, insbesondere der DSGVO, auch auf den vorliegenden Sachverhalt und die zugrunde liegenden Konstellationen der Beteiligten erstreckt. Dies gilt selbst in den Fällen von Übermittlungen personenbezogener Daten in ein Drittland, in denen es aus Gründen der nationalen Sicherheit oder Verteidigung zu einem Zugriff durch Geheimdienste dieses Drittlandes kommt. Nach den Darlegungen des EuGH gelten die Ausnahmen des Art. 2 Abs. 2 lit. a), b), d) DSGVO nur für die Mitgliedstaaten der Europäischen Union.

Ungültigkeit des „Privacy Shield“

„Weitreichende Folgen für die Übermittlung personenbezogener Daten in die USA …“

Weitreichende Folgen für die Übermittlung personenbezogener Daten in die USA hat der Beschluss dadurch bekommen, dass der EuGH in seiner Entscheidung feststellt, dass in den Vereinigten Staaten von Amerika als dem entscheidungserheblichen Drittland nicht das nach dem Recht der Europäischen Union erforderliche Schutzniveau für die Verarbeitung personenbezogener Daten gewährleistet wird.

Mit seiner Entscheidung hat der EuGH den bisher als Rechtsgrundlage für den Austausch personenbezogener Daten aus der EU heraus in die USA herangezogenen Durchführungsbeschluss (EU) 2016/1250 der EU-Kommission vom 12.07.2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutz stellt gebotenen Schutzes („Privacy Shield“) für ungültig erklärt, so dass dieser nicht mehr als Grundlage für Datentransfers zwischen diesen Staaten verwendet werden kann. Diesem Datenschutzschild lag die Vorstellung zugrunde, dass die USA unter bestimmten Umständen ein hinreichend angemessenes Schutzniveau für die dort verarbeiteten Daten vorsehen würde und auf diese Weise die Übermittlung personenbezogener Daten in die USA zulässig sein könnte.

Die Auffassung des EuGH, dass in den USA kein angemessenes Datenschutzniveau besteht, beruht auf der Bewertung der in den USA bestehenden Rechtslage und der Befugnisse der dortigen Geheimdienste, wie sie sich z. B. aus Section 702 des Foreign Intelligence Surveillance Act (FISA), der Executive Order 12333 sowie weiteren Gesetzen und Direktiven ergeben.

Darüber hinaus besteht in den USA auch für einzelne betroffene EU-Bürger kein geeigneter Rechtsschutz, wie er nach europäischem Recht verlangt wird. Die im Rahmen der „Privacy Shield“-Regelungen vorgesehene Stelle eines Ombudsmanns besitzt weder eine hinreichende Unabhängigkeit von der US-amerikanischen Exekutive, noch eine angemessene Durchsetzungsfähigkeit, um mögliche Verstöße beim Datentransfer zu verfolgen und sie zu ahnden.

Standarddatenschutzklauseln

In seiner Entscheidung äußert sich der EuGH auch zur Nutzung der Standarddatenschutzklauseln im Rahmen von Datenübermittlungen in die USA. Der EuGH hat die Anwendbarkeit von Standarddatenschutzklauseln, die von der EU-Kommission im Jahr 2010 zuerst als Standardvertragsklauseln beschlossen worden waren, weiterhin für zulässig erachtet und dieses Instrument gestärkt. Dabei hat er jedoch darauf hingewiesen, dass für deren Anwendbarkeit bestimmte Voraussetzungen erfüllt sein müssen. Es muss ein Schutzniveau hergestellt werden können, dass den Vorgaben des Rechts der Europäischen Union entspricht. Verantwortliche stehen daher in der Pflicht, das Schutzniveau im Drittland zu überprüfen und festzustellen, ob mit den Standarddatenschutzklauseln die mit deren Anwendung beabsichtigte Datensicherheit erreicht werden kann. Dabei sind geeignete (zusätzliche) Garantien der Vertragspartner, das für diese geltende Recht, die Durchsetzbarkeit von Rechten und das Vorhandensein wirksamer Rechtsbehelfe mit zu berücksichtigen. Gegebenenfalls ist auch zu überlegen, ob durch geeignete Anonymisierung ein hinreichender Schutz erreicht werden kann.

Sofern das Recht, dem der Vertragspartner unterliegt, kein entsprechendes Datenschutzniveau zulässt oder verhindert, dass der Vertragspartner seine Verpflichtungen und Vorgaben aus den Standarddatenschutzklauseln erfüllen kann, kann über die Standarddatenschutzklauseln keine rechtssichere Situation geschaffen werden.

Der EuGH hat auch ausgeführt, dass eine Aufsichtsbehörde für den Fall, dass ein angemessenes Schutzniveau nicht sichergestellt werden kann, die Datenübermittlung aussetzen oder verbieten muss, sofern der Schutz nicht durch andere Maßnahmen hergestellt werden kann.

Im Ergebnis hat der EuGH zwar die Anwendbarkeit der Standarddatenschutzklauseln weiterhin für möglich gehalten, macht aber gleichzeitig in seinen Ausführungen deutlich, dass diese Klauseln für die Übermittlung von personenbezogenen Daten in die USA noch zusätzlicher, individueller Ergänzungen bedürfen, die das konkrete Risiko der vorgesehenen Übermittlung der Daten zusätzlich absichern, um so das von der DSGVO angestrebte Schutzniveau für die personenbezogenen Daten erreichen zu können.

2.1.2 Urteil des Bundesgerichtshofs vom 27.07.2020 (Az. VI ZR 405/18 - Auslistungsbegehren gegen Google)

Mit seinem Urteil vom 27.07.2020 hat der Bundesgerichtshof (BGH) ein Verfahren zum Themenbereich „Recht auf Vergessenwerden" entschieden. In der Entscheidung ging es um die Voraussetzungen eines Auslistungsanspruchs gegen den Verantwortlichen eines Internetsuchdienstes nach Art. 17 DSGVO[28].

Der Kläger des Verfahrens war Geschäftsführer eines gemeinnützigen Verbandes, der im Jahr 2011 wegen finanzieller Schieflage Ziel mehrfacher Presseberichterstattung war. In diesem Zusammenhang wurde der Kläger auch mit vollem Namen genannt.

[28] § 19 KDG entspricht im kirchlichen Recht dem Art. 17 DSGVO.

Ab dem Jahr 2015 forderte der Kläger die Beklagte als Verantwortliche für den Internet-Suchdienst „Google“ auf, verschiedene Ergebnislinks aus ihren Suchergebnislisten zu entfernen. In diesen wurden bei Eingabe seines Vor- und Familiennamens, sowohl isoliert als auch in Verbindung mit bestimmten Ortsangaben, diese Ergebnislinks angezeigt. Der Aufforderung kam die Beklagte teilweise nach, jedoch nicht bezogen auf die verfahrensgegenständlichen Ergebnislinks. In den Vorinstanzen blieben die Anträge des Klägers, bei der Suche nach seinem Namen bestimmte Ergebnislinks nicht mehr anzuzeigen, die auf ihn identifizierende Presseveröffentlichungen hinführten, erfolglos.

Der BGH hat die Revision des Klägers gegen das Urteil der Vorinstanz zurückgewiesen. Nach den Feststellungen des BGH hatte der Kläger zum Zeitpunkt der Entscheidung keinen Anspruch gegen die Beklagte auf Auslistung der streitgegenständlichen Ergebnislinks. Ein solcher Anspruch ergab sich im konkreten Fall insbesondere nicht aus Art. 17 Abs. 1 DSGVO. Im Verfahren hat der Senat eine umfassende Interessenabwägung vorgenommen unter Berücksichtigung grundrechtlicher und europarechtlicher Positionen, wie z. B. der EU-Grundrechtecharta (GRCh). Dies führte im Ergebnis zu einer Entscheidung zu Lasten des Revisionsklägers. Dieser hat nach Auffassung des Gerichts auch keinen Anspruch darauf, nur so wahrgenommen zu werden, wie es seinen eigenen Vorstellungen entspricht.

In der Begründung hat der Senat unter Bezugnahme auf Art. 2 Abs. 1 DSGVO ausgeführt, dass die Tätigkeit einer Suchmaschine in den sachlichen Anwendungsbereich der DSGVO fällt, sofern die Informationen personenbezogene Daten enthalten. Dies hat der Senat für den streitgegenständlichen Fall als erfüllt angesehen, wobei er die Vorgänge als automatisierte Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 1 und 2 DSGVO eingestuft hat. Das Gericht hat auch die Beklagte in ihrer Eigenschaft als verantwortliche Stelle für die Verarbeitung von Daten in dem Index des Internet-Suchdienstes unter Bezugnahme auf Entscheidungen des EuGH als Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO angesehen.

Der räumliche Anwendungsbereich der DSGVO wurde seitens des Senats unter Bezugnahme auf Art. 3 Abs. 1 DSGVO bejaht, da die Beklagte als Betreiberin einer deutschen Niederlassung ein Angebot zur Nutzung der Suchmaschine in deutscher Sprache an Nutzer in Deutschland unterbreitet.

Zum Inhalt des Art. 17 DSGVO hat das Gericht ausgeführt, dass ein auf dauerhafte Auslistung gerichtetes Rechtsschutzbegehren grundsätzlich von der Vorschrift mitumfasst ist. Dabei ist es nach Auffassung des Gerichts nicht relevant, dass die technische Umsetzung eines solchen Begehrens sich nicht in einem einmaligen Löschen von Daten durch die Beklagte erschöpft, sondern weitere Maßnahmen, etwa die Aufnahme der beanstandeten Information in eine Datenbank, erforderlich sind, um eine erneute Indexierung dieser Information unter dem fraglichen Suchbegriff zu verhindern. Eine Beschränkung auf ein schlichtes Löschen von Daten ist nach den Ausführungen des Senats auch schon deshalb nicht die alleinige Möglichkeit zur Umsetzung des Rechts auf Löschung, da der für den Betroffenen letztlich schwer einzuschätzende und sich zudem stetig ändernde Entwicklungsfortschritt, dem die technischen

Voraussetzungen der beanstandeten Datenverarbeitungen unterworfen sind, dazu führt, dass notwendigerweise weitere Maßnahmen ergriffen werden müssen. Unabhängig von der technischen Umsetzung umfasst, wie der Senat unter Bezugnahme auf den EuGH feststellt, das Recht auf Löschung auch das Auslistungsrecht der von einer Suchmaschine betroffenen Person.

Der Senat trifft weiterhin die Feststellung, dass der Kläger sich nicht darauf verweisen lassen muss, vorrangig die Presseorgane in Anspruch zu nehmen, auf die bei den Suchergebnissen verlinkt wird. Die Haftung eines Suchmaschinenbetreibers wird vom Gericht nicht als subsidiär angesehen. Begründet wird dies damit, dass ein wirksamer und umfassender Schutz nicht erreicht werden kann, wenn grundsätzlich klagende Personen darauf verwiesen werden müssten, vorher oder parallel bei den Inhalteanbietern die Löschung der sie betreffenden Informationen erwirken zu müssen. Die Tätigkeit eines Suchmaschinenbetreibers wird als ein für sich stehender Akt der Datenverarbeitung angesehen. Insofern ist nach Maßgabe des Gerichts die damit einhergehende Grundrechtsbeschränkung eigenständig zu beurteilen.

Der Senat verneint jedoch in der Entscheidung zum konkreten Fall das Vorliegen der erforderlichen materiellen Voraussetzungen für das vom Kläger betriebene Auslistungsbegehren. Der Senat sieht zwar Art. 17 Abs. 1 DSGVO als einschlägige Grundlage für das Begehren des Klägers. Bezüglich des Rechts auf Schutz personenbezogener Daten ist nach Auffassung des Senats jedoch zu berücksichtigen, dass dieses kein uneingeschränktes Recht darstellt, sondern unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss. Im konkreten Einzelfall berücksichtigt der BGH auf Seiten des Klägers die Grundrechte auf Achtung des Privat- und Familienlebens aus Art. 7 GRCh und auf Schutz personenbezogener Daten aus Art. 8 GRCh.

Zugunsten der beklagten Suchmaschinenverantwortlichen wird deren Recht auf unternehmerische Freiheit aus Art. 16 GRCh gegenübergestellt. Eine Berufung auf Art. 11 GRCh hält der Senat jedoch nicht für zulässig. In die Erwägung einbezogen werden die in einem solchen Rechtsstreit möglicherweise unmittelbar betroffenen Grundrechte Dritter, wozu vorliegend die Meinungsfreiheit der Inhalteanbieter und die Informationsinteressen der Nutzer angesprochen werden. Voraussetzung dafür ist, dass im Rahmen der Entscheidungsfindung zwingend zugleich auch über eine in der Auslistung liegende Einschränkung von Grundrechten Dritter mit entschieden werden muss. Einem Suchmaschinenverantwortlichen darf laut BGH unter Verweis auf die Rechtsprechung des Bundesverfassungsgerichts nichts aufgegeben werden, was die Grundrechte Dritter verletzt.

Weiterhin sind die Zugangsinteressen der Internetnutzer zu berücksichtigen und damit das Interesse einer breiten Öffentlichkeit am Zugang zu Informationen als Ausdruck des in Art. 11 GRCh verbürgten Rechts auf freie Information. Auch die Rolle der Presse in der demokratischen Gesellschaft ist nach Auffassung des Gerichts mit zu berücksichtigen.

Im Ergebnis seiner Prüfung kommt der Senat zu dem Schluss, dass nach den anzulegenden Grundsätzen und Maßstäben die Grundrechte des

Klägers hinter den Grundrechten der Beklagten und den mit zu berücksichtigenden Interessen der Nutzer, der Öffentlichkeit und der für die verlinkten Zeitungsartikel verantwortlichen Presseorgane zurückzutreten haben.

Auch kirchliche Stellen oder Persönlichkeiten könnten in die Situation geraten, mit einer vielleicht nicht in allen Aspekten ihren eigenen Vorstellungen entsprechenden Berichterstattung konfrontiert zu werden. Die Entscheidung hilft bei der Abschätzung, welche Möglichkeiten im Rahmen eines Auslistungsbegehrens zur Verfügung stehen und welche Voraussetzungen für einen möglichen Erfolg zu erfüllen sind.

2.1.3 Entscheidungen zur Arbeit der Datenschutzaufsichten

Aus den im Berichtszeitraum ergangenen Gerichtsentscheidungen, die sich mit Entscheidungen der Datenschutzaufsichtsbehörden befassen, werden nachfolgend zwei Entscheidungen vorgestellt, aus denen sich über den konkreten Einzelfall hinaus grundsätzliche Aussagen zur Arbeit der Datenschutzaufsicht ableiten lassen.

In einem Verfahren hatte das Verwaltungsgericht Mainz zu entscheiden, inwieweit ein Beschwerdeführer einen Anspruch auf ein konkretes Handeln der staatlichen Datenschutzaufsicht hat.[29] Der Kläger des Verfahrens hatte bei der Datenschutzaufsicht eine Beschwerde erhoben. Da die vorgetragenen Informationen aus Sicht der Datenschutzaufsicht nicht ausreichend waren, um die Beschwerde zu bearbeiten, forderte sie den Beschwerdeführer mehrfach auf, die Beschwerde zu ergänzen beziehungsweise zu konkretisieren. Da der Beschwerdeführer dies unterließ, beendete die Datenschutzaufsicht das Verfahren ohne weitere Prüfung.

Das Gericht stellte fest, dass der Kläger keine prüffähige Beschwerde erhoben habe. Mangels konkreter Informationen zu einem Datenschutzrechtsverstoß habe die Beschwerde nicht geprüft werden können. Das Gericht rügte dazu, dass der Kläger versäumt habe, seine Beschwerde und darauf aufbauend seine Klage zumindest rudimentär zu begründen.

Das Gericht hat in seiner Entscheidung festgehalten, dass zwar an die Beschwerde eines Betroffenen keine zu strengen Anforderungen zu stellen sind, damit dieser das Beschwerderecht grundsätzlich einfach und unbürokratisch ausüben kann. Es legt dem Beschwerdeführer aber durchaus die Verpflichtung auf, zu seiner Rüge substantiiert vorzutragen. Es muss der Datenschutzaufsicht durch den Vortrag ermöglicht sein, den Sachverhalt zu erfassen und daraus sowohl seine Zuständigkeit, als auch die inhaltliche Betroffenheit prüfen zu können. Sofern kein ausreichender Vortrag vorliegt, ist es nach Auffassung des Gerichts Aufgabe der Aufsichtsbehörde, durch geeignete Hinweise auf eine prüfungsfähige Konkretisierung hinzuwirken. Wenn der Beschwerdeführer darauf nicht in geeigneter Weise vorträgt, ist die Datenschutzaufsicht berechtigt, das Verfahren zu beenden.

[29] Urteil des Verwaltungsgerichts Mainz vom 22.07.2020 – 1 K 473/19.MZ.

Als weiteren Aspekt hatte der Kläger geltend gemacht, dass die Datenschutzaufsicht gemäß Art. 51 DSGVO dafür Sorge tragen müsse, dass die staatlichen Stellen die DSGVO (hier im speziellen das Auskunftsrecht) einheitlich auslegen und handhaben. Nach Ansicht des Gerichts lässt sich aus Art. 51 Abs. 2 S. 1 DSGVO aber kein einklagbarer Rechtsanspruch beziehungsweise keine Verletzung eines subjektiven Rechts ableiten. Dementsprechend könne der Kläger auch nicht von der Datenschutzaufsicht die Durchsetzung einer einheitlichen Rechtsanwendungspraxis verschiedenen Behörden gegenüber einfordern.

In dem zweiten Verfahren hatte das Verwaltungsgericht Ansbach zu entscheiden, inwieweit ein Beschwerdeführer einen Anspruch auf aufsichtsbehördliches Einschreiten hat. Insbesondere hatte das Gericht zu prüfen, ob ein Anspruch auf die Verhängung einer Geldbuße besteht.[30]

Das Gericht stellt hierzu fest, dass ein Betroffener grundsätzlich keinen Anspruch auf aufsichtsrechtliches Einschreiten der Datenschutzaufsicht hat. Ein solcher Anspruch kann sich nach Ansicht des Gerichts aber dann ergeben, wenn im konkreten Fall für die Datenschutzaufsicht eine Ermessensreduktion auf Null zu bejahen ist.

Auf Basis dieser grundsätzlichen Feststellung kommt das Gericht zu dem Ergebnis, dass grundsätzlich kein Anspruch auf die Verhängung eines Bußgeldes besteht, weil die Verhängung eines Bußgeldes nach der DSGVO im Ermessen der Datenschutzaufsicht steht.

Das Verwaltungsgericht führt als Begründung an, dass die DSGVO in Art. 58 mehrere sogenannte Abhilfebefugnisse vorsehe, wovon die Geldbuße nur eine sei. Die Frage, welche dieser Abhilfebefugnisse die Datenschutzaufsicht auswählt, steht jedoch im Ermessen der Behörde als Ausfluss des Opportunitätsprinzips aus § 47 Abs. 1 OWiG. Dies folgt nach Ansicht des Gerichts aus dem Wortlaut der entsprechenden Regelung der DSGVO und den dazugehörigen Entscheidungsgründen.

Anders sei nur zu entscheiden, wenn sich das Entschließungsermessen der Datenschutzaufsicht auf Null reduzieren würde. Dies könne aber nur angenommen werden, wenn die Verhängung einer Geldbuße als einzig mögliche Abhilfemaßnahme in Frage komme, um einen rechtmäßigen Zustand herbeizuführen. Im konkreten Fall des Urteils sah das Gericht die Voraussetzungen für eine Ermessensreduzierung auf Null als nicht gegeben an.

[30] Urteil des Verwaltungsgerichts Ansbach vom 16.03.2020 - AN 14 K 19.00464.

2.2 Die Datenschutzgerichte der katholischen Kirche

Nachdem im Jahr 2019 zwei Entscheidungen des Interdiözesanen Datenschutzgerichts (IDSG) veröffentlich worden waren, sind im Berichtszeitraum 2020 mehrere veröffentlichte Entscheidungen des Gerichts hinzugekommen. Entscheidungen des Datenschutzgerichts der Deutschen Bischofskonferenz als der zweiten Instanz der Datenschutzgerichte der katholischen Kirche in Deutschland wurden im Berichtszeitraum nicht veröffentlicht.

Die Entscheidungen des IDSG sind nachfolgend mit dem Aktenzeichen und dem Datum der Entscheidung sowie mit der Kurzbeschreibung des Gegenstandes der Entscheidung von der Internetseite[31] der Deutschen Bischofskonferenz aufgeführt.

IDSG 03/2019 vom 22.04.2020

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

IDSG 02/2018 vom 05.05.2020

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

IDSG 02/2019 vom 18.06.2020

Wenn eine Pfarrei oder ein Pfarrverband die in ihrer/seiner Meldedatenbank gespeicherten Namen und Anschriften der Pfarr(verbands)angehörigen zu dem Zweck nutzt, Spendenaufrufe für Caritas-Sammlungen, zu deren Durchführung die Pfarreien durch bischöfliche Anordnung verpflichtet sind, in die Briefkästen der Pfarr(verbands)angehörigen einwerfen zu lassen, nimmt sie/er eine nach dem kirchlichen Datenschutzrecht zulässige Verarbeitung personenbezogener Daten vor.

IDSG 05/2019 vom 09.12.2020
(Rechtsmittel eingelegt: DSG-DBK 05/2020)

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

IDSG 01/2020 vom 14.12.2020

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

[31] Die veröffentlichten Urteile sind abrufbar unter https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen

3 Aus der Tätigkeit des Datenschutzzentrums

Im Berichtszeitraum waren unter den vielen Anfragen, Beschwerden, Meldungen von Datenschutzverletzungen und anderen Sachverhalten einige Themen und Fragestellungen so präsent, dass das KDSZ die damit zusammenhängenden Fragen nachfolgend als Schwerpunkte zusammengefasst hat. Neben Corona waren dies die Fragen im Zusammenhang mit der Entscheidung des Europäischen Gerichtshofs zum Privacy Shield, die Folgen des Brexits und die Ausübung der Betroffenenrechte.

3.1 Schwerpunkt I: Corona

Die Corona-Pandemie war natürlich auch für die kirchlichen Einrichtungen, sowohl mit ihren direkten Auswirkungen im Bereich der Krankenhäuser und der Pflegeeinrichtungen als auch mit den indirekten Folgen für die Durchführung von Gottesdiensten oder der Ausübung ehrenamtlicher Tätigkeiten und der Vereins- und Verbandsarbeit im kirchlichen Bereich, im überwiegenden Teil des Berichtszeitraums eines der beherrschenden Themen, auch in der Arbeit des Katholischen Datenschutzzentrums.

In verschiedensten Situationen mussten in den kirchlichen Einrichtungen bestehende Prozesse geändert oder neue Prozesse aufgesetzt werden. Daraus ergaben sich auch viele datenschutzrechtliche Fragen, bei denen das Katholische Datenschutzzentrum den kirchlichen Einrichtungen beratend zur Seite stand.

3.1.1 Übertragung von Gottesdiensten im Internet

Im Rahmen der Schutzmaßnahmen der nordrhein-westfälischen Landesregierung waren auch die Gottesdienste von unterschiedlich ausgeprägten Einschränkungen betroffen. So war die Feier von Gottesdiensten mit den Gläubigen im Frühjahr 2020 zeitweise nicht möglich und konnte erst nach gewissen Lockerungen und damit verbundenen Gesprächen zwischen Vertretern der Kirchen und der Landesregierung aufgrund eines gemeinsam entwickelten Schutzkonzeptes wieder stattfinden. Aufgrund der angespannten Pandemielage im Dezember wurde nochmals nachgeschärft.

Gerade in dieser ersten Phase der Pandemie und der fehlenden Möglichkeit der Feier der Gottesdienste mit Besuchern nutzten viele Gemeinden die Möglichkeiten, die Gottesdienste ohne anwesende Gemeindemitglieder zu feiern und diese Gottesdienste dann im Internet zu streamen. So konnten zumindest über dieses Format die Gemeindemitglieder an den Gottesdiensten teilnehmen.

Bei den Anfragen, die das Katholische Datenschutzzentrum hierzu erreichten, konnte auf die allgemeinen Grundsätze zur Übertragung von Gottesdiensten im Fernsehen oder im Internet verwiesen werden.

Aus datenschutzrechtlicher Sicht waren hier die gleichen Fragen zu beachten, die auch vor der Pandemie bei der Übertragung von Veranstaltungen im Internet durch kirchliche Einrichtungen zu berücksichtigen waren. Hierzu gehören vor allen Dingen die Einwilligung der Personen, die als Mitwirkende an dem Gottesdienst im Bild zu sehen sind. Da dies ein eng gefasster Kreis ist, stellt dies in der Regel kein organisatorisches Problem dar.

Sofern die Übertragungen auch nach der (Wieder-)Zulassung von Gläubigen bei den Gottesdiensten fortgesetzt wurden, waren die Besucher durch Aushänge über die Übertragung zu informieren. Wenn in den Gottesdiensten Bereiche in den Kirchen ausgewiesen sind, die nicht von den Kameras erfasst werden, können auch die Besucher der Gottesdienste ihre Religion ausüben, die nicht dabei gefilmt werden wollen. Aus diesen Erwägungen heraus sollte dann auch die individuelle Ausübung des Glaubens, die z. B. während der Kommunionspendung sichtbar wird, von den Kameras nicht in einer Weise erfasst werden, die die Personen individuell erkennbar zeigt.

3.1.2 Kontaktnachverfolgung bei Gottesdiensten

In den Gemeinden und Seelsorgebereichen entstand viel Unsicherheit, unter welchen Voraussetzungen Gottesdienstfeiern möglich und welche Vorgaben der Landesverordnung (Coronaschutzverordnung[32]) dabei zu beachten sind. Da zunächst keine Kontaktnachverfolgung und somit keine Registrierungspflicht für Gottesdienstbesucher in der Verordnung vorgesehen war, fehlte es an einer rechtlichen Grundlage zur Erfassung der personenbezogenen Daten im Vergleich z. B. zu Gastronomiebetrieben oder Fitnessstudios.

Durch die Coronaschutzverordnung[33] mit Gültigkeit ab 30.05.2020 wurde die Verpflichtung zur einfachen Rückverfolgbarkeit in den Paragrafen für Gottesdienste mit aufgenommen, so dass diesbezüglich Klarheit durch den Verordnungsgeber geschaffen wurde und die Gemeinden darauf in kurzer Zeit reagieren mussten, um die Landesvorgaben umzusetzen. Dies wurde in den (Erz-)Diözesen unterschiedlich gehandhabt. So war es teilweise möglich, sich per Online-Ticket einen Platz für die gewünschte Messfeier zu reservieren, was zum Vorteil hatte, dass es keiner auszufüllenden Zettel bedurfte und es nicht zu Ansammlungen vor den Kirchen kam. Das Ausfüllen eines Zettels war aber - genau wie in Krankenhäusern - sehr verbreitet. Dabei war zunächst - auch aufgrund der schnellen Umsetzung - teilweise noch nicht darauf geachtet worden, dass die Listen nicht für jedermann einsehbar am Eingang liegen durften. Bei den zu erfassenden Daten (Vorname, Name, Adresse, Telefonnummer) handelt es sich um personenbezogene Daten gemäß § 4 Nr. 1 KDG. Die Coronaschutzverordnung schreibt vor, dass diese Daten nach den geltenden datenschutzrechtlichen Bestimmungen zu verarbeiten, vor dem Zugriff Unbefugter zu schützen und nach 4 Wochen zu vernichten sind. Die Regelung des § 2a Abs. 1 Coronaschutzverordnung NRW stellt eine rechtliche Verpflichtung dar, welcher der Verantwortliche unterliegt (vgl. § 6 Abs. 1 lit. d) KDG).

[32] Aufgrund der sich oft geänderten Paragrafen der Coronaschutzverordnung wird hier im Folgenden auf eine genaue Zitierung der einzelnen Vorschriften verzichtet.

[33] „Dritte Verordnung zur Änderung der Coronaschutzverordnung vom 8. Mai 2020" vom 27.05.2020, GV.NRW 2020, Seite 340g.

Sofern die Verantwortlichen eine vorherige Anmeldung zu den Gottesdiensten vorgesehen haben, noch freie Plätze dann aber vor dem Gottesdienst an Personen vergeben werden, die ohne Anmeldung erschienen sind, müssen und dürfen die nach der Coronaschutzverordnung notwendigen Daten vor Ort erhoben werden.

Im Berichtszeitraum erhielt das Katholische Datenschutzzentrum mehrere Beschwerden, die das Führen von Gottesdienst-Besucherlisten im Rahmen der Corona-Pandemie zum Gegenstand hatten. Aufgrund der anfangs herrschenden Unsicherheit im Umgang mit den neuen Anforderungen kam es zu mehreren Beschwerden bezüglich der Umsetzung der rechtlichen Verpflichtung der Verantwortlichen.

In mehreren Beschwerden, welche nicht nur aus dem Bereich der Kirchengemeinden, sondern auch aus Gesundheitseinrichtungen kamen, war Gegenstand der Beschwerden, dass die zu führenden Listen entweder für Dritte einsehbar waren, es sich um Sammellisten handelte oder personenbezogene Daten abgefragt wurden, die nach der geltenden nordrhein-westfälischen Coronaschutzverordnung nicht abzufragen waren. Die Ausbesserung der anfänglichen Defizite ist in den meisten Fällen schnell erfolgt, wobei gerade die betrieblichen Datenschutzbeauftragten durch ihre Unterstützung bei der Umsetzung der Vorgaben aus der Verordnung behilflich waren. Hier kam es vor allem darauf an, die Mängel im Umgang mit und bei der Erhebung der personenbezogenen Daten zeitnah zu beheben, um die Verarbeitung der personenbezogenen Daten datenschutzkonform zu gestalten und auch die Akzeptanz in die Maßnahmen zum Schutze vor einer Infektion mit dem Virus zu stärken beziehungsweise zu erhalten.

In den Fällen, in denen es auch Monate nach Erlass der Verordnung beziehungsweise der entsprechend gültigen Fassung oder vorangegangener Hinweise durch das Katholische Datenschutzzentrum zu nicht gesetzeskonformer Verarbeitung personenbezogener Daten im Rahmen der Erfassung zur Kontaktnachverfolgung gekommen ist, ergingen auch Untersagungsverfügungen, welche die weitere nichtverordnungskonforme Führung der Listen zum Inhalt hatten und somit einen datenschutzkonformen Umgang mit dem Erfordernis der Ermöglichung der Kontaktnachverfolgung herstellen sollten.

Ebenfalls kam es zu Beschwerden, dass die geführten Listen zu anderen Zwecken als der Kontaktnachverfolgung genutzt wurden. Da in der nordrhein-westfälischen Coronaschutzverordnung und auch in den anderen Bundesländern die Zweckbindung nicht eindeutig formuliert war und es daher zu unterschiedlichen Auslegungen der Regelungen kam, hat der Bundesgesetzgeber mit der Einführung des § 28a Infektionsschutzgesetz (IfSG) möglicherweise bestehende Unklarheiten endgültig beseitigt. § 28a Abs. 4 S. 1 und 3 IfSG stellt nun klar, dass die erhobenen Daten nur zum alleinigen Zweck der Aushändigung auf Anforderung der zuständigen Behörden verwendet werden dürfen.[34]

Beim Interdiözesanen Datenschutzgericht ist ein Verfahren zu dieser Thematik anhängig.

[34] Vgl. auch https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Corona-Kontaktlisten---Zugriffe-von-Strafverfolgungsbehoerden-nun-ge-setzlich-ausgeschlossen/Corona-Kontaktlisten---Zugriffe-von-Strafverfolgungsbehoerden-nun-gesetzlich-ausgeschlossen.html; bereits eindeutig: OVG NRW, Beschluss vom 23.6.2020 – 13 B 695/20.NE.

3.1.3 Besuchsregister in Krankenhäusern und Pflegeeinrichtungen

Bedingt durch die Corona-Pandemie ergab sich für die kirchlichen Krankenhäuser und Pflegeeinrichtungen eine vergleichbare Problematik der Erfassung zusätzlicher personenbezogener Daten der Besucher der Einrichtungen, wie sie bei der Erfassung der Gottesdienstbesucher für die Pfarreien auftraten beziehungsweise noch auftreten.

Zur Nachverfolgung von Kontakten der Patienten beziehungsweise Bewohner müssen die Einrichtungen Besuchsregister führen.[35] Danach mussten Besucher eines Krankenhauses (in der Zeit, in der Besuche erlaubt waren) ihre Kontaktdaten angeben, um eine mögliche erforderliche Nachverfolgung durch die zuständigen Behörden bei einem Infektionsfall gewährleisten zu können. Auch bei dieser Erfassung der personenbezogenen Kontaktdaten galt es, die Einsichtnahme Dritter zu vermeiden. Dies wurde in den meisten Fällen auch durch das Verwenden von separaten Erfassungsbögen gewährleistet.

In den Fällen, in denen es Beschwerden zu offen einsehbaren Besucherlisten gab, haben die Verantwortlichen schnell reagiert und die Praxis der Erfassung der Kontaktdaten kurzfristig angepasst, so dass die datenschutzrechtlichen Vorgaben Beachtung fanden.

3.1.4 Mobiles Arbeiten während der Corona-Pandemie

Mit den steigenden Infektionszahlen im Frühjahr und Herbst 2020 verlagerten auch kirchliche Einrichtungen die Arbeit im Büro aus Gründen des Gesundheitsschutzes der Beschäftigten in das heimische Umfeld der Mitarbeitenden.

Dabei war die Verlagerung der Arbeit nicht als dauerhafte Einrichtung eines heimischen Arbeitsplatzes gedacht, sondern als akute Maßnahme aufgrund der pandemischen Lage.

Dies bedeutete aber auch, dass hier nicht die klassischen Regelungen zur Einrichtung eines Homeoffice-Arbeitsplatzes oder eines Telearbeitsplatzes im Sinne der Arbeitsstättenverordnung greifen sollten, sondern es um eine Form von mobilem Arbeiten geht, bei der der Beschäftigte vorübergehend und nicht auf Dauer angelegt seine Arbeit aus dem heimischen Umfeld erledigt.

Telearbeits- (Homeoffice-)Arbeitsplätze werden auf Basis betrieblicher und einzelvertraglicher Regelungen eingerichtet, die auch die datenschutzrechtlichen Fragen des Umgangs mit personenbezogenen Daten bei der Arbeit regeln. Kennzeichnend für den Telearbeitsplatz ist die Einrichtung eines festen Arbeitsplatzes durch den Dienstgeber (typischerweise) zu Hause beim Dienstnehmer.

[35] Siehe z. B. § 5 Abs. 3 Nr. 7 der „Verordnung zum Schutz vor Neuinfizierungen mit dem Coronavirus SARS-CoV-2 (Coronaschutzverordnung – CoronaSchVO)“ vom 10.06.2020 (Art. 1 der „Siebten Verordnung zur Änderung von Rechtsverordnungen zum Schutz vor dem Coronavirus SARS-CoV-2“, GV.NRW 2020, Seite 381a).

Mobiles Arbeiten zeichnet sich eher dadurch aus, dass es weniger regelmäßig angelegt und nicht auf einen Ort festgelegt ist. Wird die dreistündige Zugfahrt zu einem Besprechungstermin genutzt, um mit dem Laptop noch zu arbeiten, entspricht dies nicht der Vorgabe eines Telearbeitsplatzes, aber die Arbeit wird während der Arbeitszeit mobil erledigt[36].

Dies macht aber auch deutlich, dass aus datenschutzrechtlicher Sicht die Anforderungen an technische und organisatorische Schutzmaßnahmen zur Absicherung der Verarbeitung der Daten in beiden Varianten nur teilweise deckungsgleich sind.

Während die Verschlüsselung mobiler Geräte (z. B. des Laptops) in beiden Szenarien wichtig ist, rückt beim mobilen Arbeiten, z. B. in der Bahn, der Schutz vor unberechtigter Kenntnisnahme durch „mitlesen" auf dem Bildschirm eher ins Blickfeld, als beim Arbeiten im Homeoffice. Hier sind für beide Szenarien jeweils die angemessenen Schutzmaßnahmen zu treffen.

Da mit der Pandemie die Arbeitsplätze nicht dauerhaft in das heimische Umfeld verlagert werden sollten, handelt es sich derzeit eher um mobiles Arbeiten, das die kirchlichen Einrichtungen und deren Beschäftigten praktizieren, auch wenn die konkrete Ausübung der Arbeit zu Hause schon eher der Arbeit an einem festen Homeoffice-Arbeitsplatz ähnelt.

Die datenschutzbezogenen Herausforderungen dieser neuen Art des Arbeitens sind vielfältig und resultieren oft aus einem größeren Einfluss des Arbeitnehmers auf den individuellen Umgang mit personenbezogenen Daten in der neuen Verarbeitungsform. Das Katholische Datenschutzzentrum hat die wichtigsten Hinweise im April 2020 in Form eines Infoblattes[37] an die kirchlichen Einrichtungen gegeben.

„Ein datenschutzkonformes mobiles Arbeiten verlangt zwingend die Beachtung der ... Schutzziele ..."

Ein datenschutzkonformes mobiles Arbeiten verlangt zwingend die Beachtung der klassischen Schutzziele der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität. Hinzu kommt das Schutzziel der Belastbarkeit, um ein System auch unter ungünstigen Bedingungen wie z. B. hohem Datenvolumen oder instabiler Datenverbindung sicher und verlässlich betreiben zu können.

Der Verantwortliche der Datenverarbeitung muss seinen Mitarbeitenden die notwendige Ausstattung an die Hand geben. Dazu gehören sowohl die dienstlichen Endgeräte als auch die sichere Datenverbindung aus dem mobilen Umfeld in die Netze der Einrichtung. Nur beim Einsatz dienstlicher Endgeräte lassen sich durch eine restriktive Konfiguration alle Sicherheitsrichtlinien konsequent durchsetzen. In Ausnahmefällen ist der Einsatz privater Geräte zu dienstlichen Zwecken nach § 20 KDG-DVO (Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz) gesondert zu begründen. Eine „abhörsichere" verschlüsselte VPN-Verbindung vom Endgerät zum Router der Einrichtung schützt die Daten während des Transports. Noch besser ist eine Ver-

[36] Die Begriffe Telearbeitsplatz / Homeoffice und mobiles Arbeiten werden hier im Sinne der Beschreibung der Ausarbeitung des wissenschaftlichen Dienstes des Bundestages "Telearbeit und Mobiles Arbeiten - Voraussetzungen, Merkmale und rechtliche Rahmenbedingungen" (Az. WD 6 -3000 -149/16 vom 10.07.2017) gebraucht.

[37] Siehe hierzu Abschnitt 5.2.1 dieses Jahresberichts.

meidung der lokalen Speicherung von Daten durch Arbeiten in speziellen webbasierten Oberflächen in zentralen Systemen (wie z. B. CITRIX), wobei nicht nur die Daten, sondern auch die Anwendungen zentral auf den Servern der Einrichtung verbleiben. Eine zusätzliche Verschlüsselung aller Datenträger der Endgeräte sollte inzwischen selbstverständlicher Standard geworden sein.

Das Infoblatt schließt mit Hinweisen zur Organisation des häuslichen Arbeitsumfelds und zur weitestgehenden Vermeidung von Papier.

3.1.5 Videokonferenzen ersetzen Besprechungen vor Ort

Mit der Verschärfung der Maßnahmen zur Bekämpfung der Corona-Pandemie im Frühjahr 2020, in deren Folge viele Präsenztermine – Besprechungen, Fortbildungsveranstaltungen und nicht zuletzt auch Unterricht an den Schulen – ausfallen mussten beziehungsweise durch andere Formen ersetzt werden sollten, stieg in den vom Katholischen Datenschutzzentrum betreuten Einrichtungen der Bedarf an technischer und rechtlicher Beratung zum Einsatz geeigneter Online-Tools.

Im März 2020 hat das KDSZ deshalb ein erstes Infoblatt zum Thema des mobilen Arbeitens veröffentlicht, in dem u. a. auch auf die Auswahl geeigneter Software für Telefon- und Videokonferenzen eingegangen wurde. Im April 2020 veröffentlichte das Katholische Datenschutzzentrum Frankfurt ein Infoblatt zu Beurteilungskriterien bei der Auswahl von Online-Meeting-Tools, auf das das KDSZ bei Anfragen immer wieder hingewiesen hat.

Bei der Dienstleistung „Videokonferenz“ handelt es sich meistens um einen klassischen Cloud-Service, bei dem zwei oder mehrere Anwender („Clients“) ihre Daten (Audio- und Videoströme) über eine Zentrale („Server“) austauschen. Nur in wenigen Fällen wird eine „Peer-to-Peer“-Kommunikation aufgebaut, bei der sich alle Teilnehmer gleichberechtigt untereinander ohne eine zentrale Instanz verbinden. Bei Videokonferenzen fallen wie beim herkömmlichen Telefonat Nutzdaten (die Gesprächsinhalte) und Verbindungsdaten (Metadaten: wer mit wem und zu welcher Zeit verbunden ist) an. Aus Datenschutzsicht sind beide Datenkategorien von Interesse:

Bei der Verarbeitung der Nutzdaten, also den Gesprächsinhalten, war in 2020 eine kontinuierliche Weiterentwicklung der Datenschutzfreundlichkeit der Dienste zu beobachten. Mittlerweile bieten alle namhaften Anbieter von Videokonferenzen, einschließlich der großen US-amerikanischen Anbieter, eine volle Ende-zu-Ende-Verschlüsselung der Gespräche an, bei der die Gesprächsinhalte nur auf den Endgeräten der Teilnehmer unverschlüsselt gehört und gesehen werden können. Selbst auf dem zentralen Server ist im Fall der richtigen Umsetzung der Ende-zu-Ende-Verschlüsselung ein Mithören nicht möglich. Dabei muss der Anwender systembedingt allerdings einige Einschränkungen der Funktionalität hinnehmen: Bei einer Ende-zu-Ende-Verschlüsselung können keine Teilnehmer per Telefon mitsprechen (eine Funktion, die bei schlechter Internetanbindung oder nicht ausreichender Hardwareausstattung oft genutzt wird). Auch eine Aufzeichnung der Konferenz ist nicht möglich. Teilnehmer können meistens nicht über einen

einfachen Browser teilnehmen, sondern benötigen eine proprietäre Softwareinstallation auf ihrem Endgerät. Weiterhin haben fast alle Anbieter aufgrund der großen Nachfrage ihre Serverkapazitäten erhöht und global verteilte Rechenzentren installiert, auf denen der wachsende Netzwerkverkehr („Traffic") verteilt wird. Als Nebeneffekt der globalen Expansion können die Kunden in der Regel entscheiden, dass ihre Konferenzen nur über Server in ihrer geografischen Heimatregion, z. B. Europa, abgewickelt werden.

Die Verbindungsdaten sind hingegen weitaus weniger geschützt. Für Abrechnungszwecke werden diese in die Firmenzentrale übermittelt, die sich meistens im Heimatland des Anbieters befinden dürfte, selbst wenn Server in Europa betrieben werden und dem Anwender zugesichert ist, dass seine Nutzdaten in Europa verbleiben. Datenschutzfreundlich sind Anbieter in diesem Bereich, wenn sie außer den echten Abrechnungsdaten alle weiteren technisch benötigten Verbindungsdaten nur kurzzeitig, etwa während der Dauer der Konferenz, speichern und anschließend umgehend löschen. Anwender, besonders die Veranstalter von Videokonferenzen, können die Datenschutzfreundlichkeit unterstützen, indem sie die Teilnehmer über die Verarbeitung ihrer Daten durch sich selbst und den Konferenzdienstleister informieren und z. B. eine pseudonymisierte Teilnahme zulassen.

Zur Vermeidung der datenschutzrechtlichen Probleme, die mit einem Drittlandtransfer von personenbezogenen Daten einhergehen können, wenn der Anbieter der Videokonferenz-Lösung seinen Sitz in einem Drittland hat beziehungsweise die Daten in einem Drittland speichert, rät das Katholische Datenschutzzentrum daher, die Nutzung von Anbietern zu prüfen, bei denen diese Problematik nicht auftritt.

3.1.6 Beschäftigtendatenschutz in der Corona-Pandemie

Bei der Verarbeitung von personenbezogenen Daten der Beschäftigten aus Anlass der Corona-Pandemie können aus Sicht des Katholischen Datenschutzzentrums bei vielen Fragestellungen zwei Fallgruppen unterschieden werden.

Während die eine Gruppe als Beschäftigte in Bereichen, die von der Corona-Pandemie besonders betroffen (z. B. Pflegeeinrichtungen) beziehungsweise für die Bekämpfung der Pandemie besonders relevant (z. B. Krankenhäuser) waren, Ziel von Regelungen der verschiedenen Corona-Verordnungen waren, war die andere Gruppe der Beschäftigten in anderen Bereichen von den allgemeinen Fragen des Beschäftigtendatenschutzes im Zusammenhang mit der Pandemie betroffen.

Für beide Gruppen tauchte aber in verschiedenen Formen und bei verschiedenen Gelegenheiten die Frage auf, ob und wie die Gesundheitsdaten als besonders schützenswerte personenbezogene Daten erhoben und verarbeitet werden durften. Die Verarbeitung von Gesundheitsdaten als Daten besonderer Kategorien nach § 11 KDG ist aber an ganz besondere Voraussetzungen geknüpft.

Die Verarbeitung von Gesundheitsdaten ist grundsätzlich nur restriktiv möglich. Zur Eindämmung der Corona-Pandemie oder zum Schutz der Beschäftigten kirchlicher Einrichtungen können für verschiedene Maßnahmen datenschutzkonform (Gesundheits-)Daten erhoben und verwendet werden. Auch in diesen Fällen ist der Grundsatz der Verhältnismäßigkeit zu beachten und die Maßnahme ist auf eine konkrete gesetzliche (Ermächtigungs-)Grundlage zu stützen.

Während aber im Verlaufe des Jahres für die eine Gruppe von Beschäftigten zum Schutz der Patienten beziehungsweise der Bewohner Rechtsgrundlagen, z. B. für die verpflichtende regelmäßige Testung der Beschäftigten im Krankenhaus oder Pflegeheim, eingeführt wurden, konnten andere Dienstgeber außerhalb dieses Anwendungsbereiches nicht einfach eine Testpflicht für die Beschäftigten ihrer Einrichtungen verfügen. Hierfür fehlte regelmäßig die rechtliche Grundlage für eine Verpflichtung.

Andere Maßnahmen betreffen beide Gruppen von Beschäftigten gleichermaßen. Die Datenverarbeitung des Dienstgebers im Fall einer positiv festgestellten Infektion zur Erfüllung der Pflichten aus der Kontaktnachverfolgung sind für alle Beschäftigten gleich. Die Pflichten und damit die Rechtsgrundlage für die Verarbeitung der Daten durch den Dienstgeber ergeben sich aus den Regelungen der Coronaschutzverordnungen oder dem Infektionsschutzgesetz.

Die Kontaktnachverfolgung als eine Maßnahme, welche in § 2a der nordrhein-westfälischen Coronaschutzverordnung[38] verortet ist, ist in vielen Bereichen vorgeschrieben. Dabei ist jedoch stets darauf zu achten, dass das Prinzip der Datensparsamkeit beachtet wird, also nur die wirklich vorgeschriebenen Daten erhoben werden. Zudem sind offene Listen, die für jedermann einsehbar sind, zu vermeiden.

Darüber hinaus muss auch der Grundsatz der Transparenz gewahrt bleiben, was bedeutet, dass die Mitarbeitenden zum Beispiel darüber informiert werden müssen, zu welchem Zweck die Daten erhoben werden oder wie lange diese gespeichert werden.

3.1.7 Änderung der Mitarbeitervertretungsordnung aufgrund der Corona-Pandemie

Aufgrund der Corona-Pandemie hat der kirchliche Gesetzgeber die Mitarbeitervertretungsordnung (MAVO) Ende März 2020 kurzfristig ergänzt, um die MAVO an die sich aus der Corona-Pandemie ergebenden Bedingungen anzupassen. Die Änderungen traten in den nordrhein-westfälischen (Erz-)Diözesen zum 01.04.2020 in Kraft und sind auf zwei Jahre befristet.

Mit der hier betrachteten Änderung des § 14 MAVO zur Tätigkeit der Mitarbeitervertretung wurde durch die Einfügung in § 14 Abs. 4 MAVO die Möglichkeit geschaffen, Sitzungen der Mitarbeitervertretung auch

[38] Siehe z. B. die Regelung in der „Verordnung zum Schutz vor Neuinfizierungen mit dem Coronavirus SARS-CoV-2 (Coronaschutzverordnung – CoronaSchVO)" vom 30.09.2020, GV.NRW 2020, Seite 915.

unter Einsatz moderner Informations- und Telekommunikationsmittel durchzuführen, sofern sichergestellt ist, dass Dritte vom Inhalt der Sitzung keine Kenntnis nehmen können.

Die vom Gesetz schon selbst angeführte Bedingung, auch unter den neuen Bedingungen die Vertraulichkeit der Beratungen sicherzustellen, hat nicht nur den Hintergrund der immer zu gewährleistenden Vertraulichkeit der Beratung der Mitarbeitervertretung. Es sind auch datenschutzrechtliche Anforderungen zu beachten, die mit dem Schutz personenbezogener Daten in den Beratungen und Vorlagen der Mitarbeitervertretungen zu tun haben.

Bei der Vorbereitung und Durchführung von Sitzungen der Mitarbeitervertretung sollten folgende Hinweise beachtet werden:

Anforderungen an die örtlichen Begebenheiten

Auch bei der Arbeit von zu Hause aus sind die datenschutzrechtlichen Vorgaben einzuhalten. Es ist darauf zu achten, dass dienstliche und private Daten nicht vermischt werden. Wird der Arbeitsplatz kurzfristig verlassen und eine Kenntnisnahme anderer Personen (z. B. Familienmitglieder) ist nicht auszuschließen, ist ein Kennwortschutz zu aktivieren, der einen unberechtigten Zugriff auf die Daten verhindern kann. Dies gilt auch für Papierakten. Wird der Arbeitsplatz längere Zeit verlassen, sind die Daten in Papierform entsprechend zu sichern (z. B. in einem verschlossenen Schrank aufzubewahren).

„Auch bei der Arbeit von zu Hause aus sind die datenschutzrechtlichen Vorgaben einzuhalten."

Wird der dienstliche PC oder Laptop für die Arbeit im mobilen Office genutzt, sollten keine privaten USB-Sticks oder andere private Hardware angeschlossen werden, um die Gefahr eines Befalls von Schadsoftware zu verringern.

Bei der Entsorgung von Papiermüll, dazu zählen auch handschriftliche Notizen aus Sitzungen, ist auf eine datenschutzkonforme Entsorgung zu achten.

Während der Videokonferenzen oder Telefonkonferenzen ist darauf zu achten, dass andere Personen keine Kenntnisse von den Inhalten der Gespräche erlangen. Das Mithören oder Mitansehen z. B. durch Familie, Freunde oder Nachbarn ist auszuschließen. Dies gilt auch für Systeme mit intelligenten Lautsprechern wie Amazon-Echo, Google-Assistent oder Cortana.

Anforderungen an die Telefon- und Videokonferenzsysteme

Seit Beginn der Pandemie wurden viele Konferenzsysteme eingesetzt und von unterschiedlicher Seite datenschutzrechtlich beurteilt. Bei dem Einsatz der Systeme ist darauf zu achten, inwieweit die Dienste Zugriff auf die Inhalts- oder Metadaten der Kommunikation beanspruchen und in welchen Ländern die Daten verarbeitet werden.

Anforderungen an die benutzten Endgeräte

Für die Teilnahme an Telefon- oder Videokonferenzen sollten möglichst dienstliche Endgeräte genutzt werden. Durch die Nutzung von dienst-

lichen Endgeräten kann auch bei Arbeiten im mobilen Office der technische und organisatorische Schutzstandard gewährt werden, der bei der Nutzung der Geräte in den Einrichtungen eingerichtet ist. Der Verantwortliche hat auch bei der Nutzung der Geräte im mobilen Office die Einhaltung der Schutzstandards zu gewährleisten.

Werden Dokumente für eine MAV-Sitzung oder Protokolle auf private Computer heruntergeladen, so hat der Verantwortliche keine Kontrolle mehr darüber, ob und wie die Daten der MAV auf diesen Geräten vor dem Zugriff Unbefugter geschützt werden.

Die Mitglieder der Mitarbeitervertretungen sollten daher für ihre Arbeit möglichst Geräte, Programme und Kommunikationswege nutzen, die in den Einrichtungen eingerichtet und/oder freigegeben worden sind und die die Vertraulichkeit der MAV-Daten auch vor, während und nach der Teilnahme an einer MAV-Sitzung sicherstellen. Bei der Nutzung von privaten Geräten sind die Vorgaben des § 20 KDG-DVO zu beachten.

Schweigepflicht gilt auch bei mobilem Arbeiten

Auch in dieser Ausnahmesituation der Pandemie gelten die Verschwiegenheitspflichten der MAV-Mitglieder weiter. Informationen, die der Schweigepflicht nach § 20 MAVO unterliegen, sind daher besonders zu schützen. Bei den durch die MAV verarbeiteten Daten handelt es sich in der Regel um Daten der Schutzklasse III gemäß § 13 KDG-DVO. Die für den Schutz der Daten relevanten Anforderungen gelten auch außerhalb der Einrichtungsinfrastruktur und müssen auch in dieser Situation sichergestellt werden.

Weitere Informationen

Das Katholische Datenschutzzentrum hat im April 2020 ein Informationsblatt „Mobiles Arbeiten und Datenschutz in Zeiten der Corona-Pandemie“ mit Hinweisen zum mobilen Arbeiten in der derzeitigen Ausnahmesituation herausgegeben.[39] Die dort genannten datenschutzrechtlichen Maßnahmen sollten auch im Kontext der Arbeit der Mitarbeitervertretungen beachtet werden.

3.2 Schwerpunkt II: Das Urteil des Europäischen Gerichtshofs zum Privacy Shield und die Folgen

Am 16.07.2020 verkündete der Europäische Gerichtshof seine lange erwartete Entscheidung in dieser Sache. Auch wenn einige Elemente der Entscheidung erwartet (oder – je nach Betrachtungswinkel – befürchtet) worden waren, so war die konkrete Entscheidung für viele datenverarbeitende Stellen eine Überraschung.

[39] Das Infoblatt ist abgedruckt in Abschnitt 5.2.1 dieses Jahresberichts.

3.2.1 Urteil des Europäischen Gerichtshofs vom 16.07.2020 (Rs. C-311/18 - Schrems II)

Mit dem Urteil des EuGH, das oben in Abschnitt 2.1.1 schon ausführlich vorgestellt wurde, wurde nach dem EuGH-Urteil zur Safe-Harbor-Regelung zum zweiten Mal eine Vereinbarung zwischen den USA und der Europäischen Union zur Zulässigkeit von Übermittlungen personenbezogener Daten für ungültig erklärt.

Mit seiner aktuellen Entscheidung hat der EuGH den bisher als Rechtsgrundlage für den Austausch personenbezogener Daten aus der EU in die USA herangezogenen Durchführungsbeschluss (EU) 2016/1250 der EU-Kommission vom 12.07.2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutz gebotenen Schutzes („Privacy Shield") für ungültig erklärt. Dieser Vereinbarung zwischen der EU und den USA lag die Vorstellung zugrunde, dass die USA unter bestimmten Umständen ein hinreichend angemessenes Schutzniveau für die dort verarbeiteten Daten vorsehen würde und auf diese Weise die Übermittlung personenbezogener Daten in die USA zulässig sein könnte.

Die Auffassung des EuGH, dass in den USA kein angemessenes Datenschutzniveau besteht, beruht auf der Bewertung der in den USA bestehenden Rechtslage und der Befugnisse der dortigen Geheimdienste. Darüber hinaus besteht in den USA auch für einzelne betroffene EU-Bürger kein geeigneter Rechtsschutz, wie er nach europäischem Recht verlangt wird.

3.2.2 Die Auswirkungen des Urteils

Das Urteil hat faktisch Auswirkungen auf fast alle Einrichtungen und Unternehmen in den Mitgliedstaaten der EU, da viel mehr Einrichtungen und Unternehmen personenbezogene Daten in die USA übermitteln, als es auf den ersten Blick vielleicht erscheint. Neben den direkten Verträgen zur Verarbeitung solcher Daten (z. B. Vertrag mit einem Dienstleister, der die Personaldaten der eigenen Einrichtung auf Servern in den USA archiviert) können Verarbeitungen von Daten z. B. auch im Rahmen von Wartungsverträgen betroffen sein, bei denen in der Einrichtung eingesetzte Geräte personenbezogene Daten im Rahmen der Wartung an den Hersteller in die USA übermitteln oder im Rahmen der Nutzung von Cloud-Diensten, nicht nur im Umfeld von Office-Programmen.

In der Folge wirkt sich dieses Urteil auch auf die Beurteilungen und Entscheidungen der kirchlichen Datenschutzaufsicht und die katholischen Einrichtungen aus, wenn bei der Übermittlung personenbezogener Daten ein Transfer in die USA involviert ist.

Ein einfaches „weiter so" wie bisher ist nach dem Urteil nicht mehr möglich.

3.2.3 Standarddatenschutzklauseln als Ausweg?

Die Entscheidung des EuGH verwirft zwar den „Privacy Shield", lässt die Standarddatenschutzklauseln aber ausdrücklich als mögliche rechtliche Grundlage für die Übermittlung von Daten – auch in die USA – bestehen. Im Falle der USA hält das Gericht dies aber nur mit weitreichenden flankierenden Maßnahmen weiterhin für möglich.

Aus Sicht des EuGH muss durch die Anwendung der Klauseln ein Schutzniveau für die einzelne Verarbeitung hergestellt werden können, das den Vorgaben des Rechts der Europäischen Union entspricht. Verantwortliche stehen daher in der Pflicht, das Schutzniveau im Drittland zu überprüfen und festzustellen, ob mit den Standarddatenschutzklauseln die mit deren Anwendung beabsichtigte Datensicherheit erreicht werden kann. Dabei sind geeignete (zusätzliche) Garantien der Vertragspartner, das für diese geltende Recht, die Durchsetzbarkeit von Rechten und das Vorhandensein wirksamer Rechtsbehelfe mit zu berücksichtigen. Gegebenenfalls ist auch zu überlegen, ob durch geeignete Anonymisierung ein hinreichender Schutz erreicht werden kann.

Sofern das Recht, dem der Vertragspartner unterliegt, kein entsprechendes Datenschutzniveau zulässt oder verhindert, dass der Vertragspartner seine Verpflichtungen und Vorgaben aus den Standarddatenschutzklauseln erfüllen kann, kann über die Standarddatenschutzklauseln keine rechtssichere Situation geschaffen werden.

3.2.4 Die Reaktionen der Datenschutzaufsichtsbehörden

Das Katholische Datenschutzzentrum hat auf seiner Internetseite im Juli 2020 eine mit den anderen Diözesandatenschutzbeauftragten abgestimmte erste Einschätzung veröffentlicht.[40]

Die Datenschutzaufsichten weisen darauf hin, dass das Urteil sofort zu beachten ist, machen aber auch deutlich, dass die Datenschutzaufsichten berücksichtigen werden, dass die Suche nach Alternativen oder der Abschluss einer neuen Rechtsgrundlage für bestehende Verarbeitungen je nach Gegenstand und Umfang der Verarbeitung nicht immer sofort erfolgen kann.

Teil der Veröffentlichung sind auch das nachfolgende Prüfungsschema und FAQ.

[40] Siehe https://www.katholisches-datenschutzzentrum.de/eugh-erklaert-eu-us-privacy-shield-fuer-ungueltig/

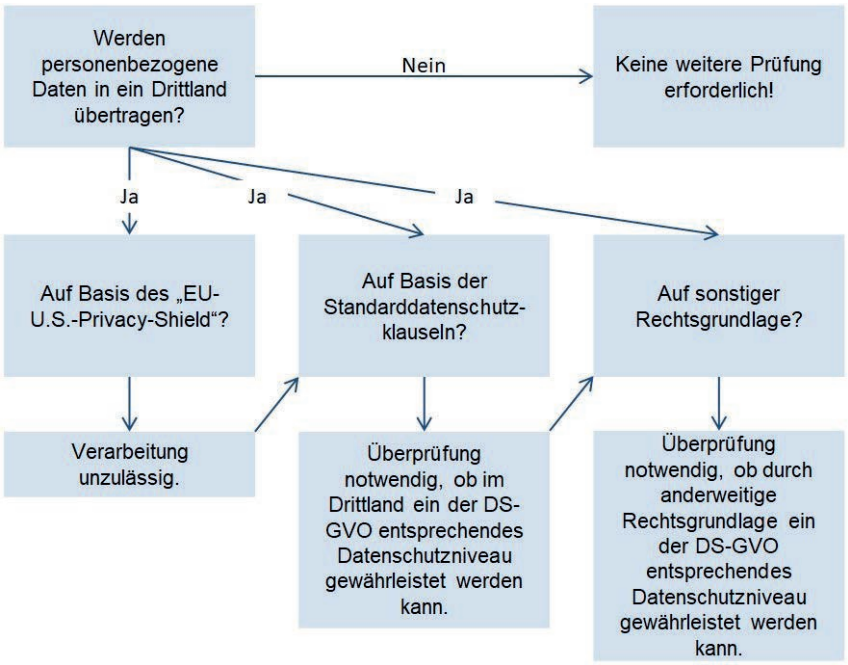


Abb.: Prüfungsschema zum Schrems-II-Urteil

Die staatlichen Datenschutzaufsichten und der europäische Datenschutzbeauftragte als Aufsicht für die EU-Institutionen haben schon angekündigt, dass sie 2021 die Umsetzung des Urteils überprüfen werden.

3.2.5 Verhandlungen der EU und der USA über eine Nachfolgeregelung

Kurz nach dem Urteil haben die Europäische Union und die USA Gespräche über eine Nachfolgeregelung zum Privacy-Shield aufgenommen.

Wann und mit welchem Ergebnis diese Gespräche beendet werden, ist noch nicht absehbar. Der Druck der datenverarbeitenden Wirtschaft ist aber groß. Hier bleiben die weiteren Entwicklungen zu den Verhandlungen abzuwarten.

3.2.6 Ausblick

Das Urteil hat unmittelbaren Handlungsdruck erzeugt. Es sieht keine Übergangsfrist vor. Die Verantwortlichen der kirchlichen Stellen und Einrichtungen mussten daher umgehend nach dem Urteil damit beginnen, die Rechtsbeziehungen und Vertragsgrundlagen mit ihren Vertragspartnern und Auftragsverarbeitern zu überprüfen und in der Folge sicherzustellen, dass die mit diesen oder durch diese Partner durchgeführten Datenübermittlungen auch weiterhin datenschutzkonform durchgeführt werden.

Bis zum Abschluss einer Nachfolgevereinbarung zum Privacy-Shield ist dies aber keine einfache Angelegenheit und sollte für einige Verarbeitungen und Prozesse vielleicht auch als Chance gesehen werden, die bestehenden Strukturen zu überprüfen und sich nach datenschutzkonformen Alternativen umzusehen.

Bei den Standarddatenschutzklauseln hat der EuGH im Ergebnis zwar die Anwendbarkeit weiterhin für möglich gehalten. Er hat aber auch deutlich gemacht, dass diese Klauseln für die Übermittlung von personenbezogenen Daten in die USA noch zusätzlicher, individueller Ergänzungen bedürfen, die das konkrete Risiko der vorgesehenen Übermittlung der Daten zusätzlich absichern, um so das von der DSGVO angestrebte Schutzniveau für die personenbezogenen Daten erreichen zu können.

Den Datenschutzaufsichten hat der EuGH schließlich noch mitgegeben, dass eine Aufsichtsbehörde für den Fall, dass ein angemessenes Schutzniveau nicht sichergestellt werden kann, die Datenübermittlung aussetzen oder verbieten muss, sofern der Schutz nicht durch andere Maßnahmen hergestellt werden kann. Daher werden die Datenschutzaufsichten nicht auf Dauer abwarten können, welche Lösungen die Stellen und Einrichtungen für die bestehenden oder neuen Datenübermittlungen in die USA finden. Die staatlichen Aufsichten haben auch schon angekündigt, dass Sie 2021 handeln werden.

„Die Einrichtungen sollten die notwendige Überprüfung nutzen, sich die bestehenden Prozesse anzuschauen und evtl. auf andere Lösungen ohne Datenübermittlungen in die USA umzustellen."

Die Einrichtungen sollten die notwendige Überprüfung nutzen, sich die bestehenden Prozesse anzuschauen und evtl. auf andere Lösungen ohne Datenübermittlungen in die USA umzustellen. Seit dem Urteil sind auch viele Anbieter aktiv geworden und haben neue Lösungen angekündigt, die DSGVO-konform (und damit auch KDG-konform) sein sollen.

3.3 Schwerpunkt III: Brexit

Nach jahrelangen Unklarheiten, wann und wie der Brexit konkret durchgeführt wird, gab es im Berichtszeitraum am 31.01.2020 den formellen Austritt und mit dem 31.12.2020 auch das Auslaufen der Übergangsphase. Der Austritt des Vereinigten Königreichs und Nordirlands aus der Europäischen Union ist damit vollzogen.

3.3.1 Der Austritt/die Übergangsphase/das Abkommen

Wie in Abschnitt 1.1.1 dieses Jahresberichts zusammengefasst, lagen im Berichtszeitraum mit dem 31.01.2020 sowohl der Zeitpunkt für den Austritt aus der EU als auch mit dem 31.12.2020 der Zeitpunkt des Endes der Übergangsfrist, in der das EU-Recht – und damit auch die DSGVO – erst einmal unverändert weiter gegolten hat.

Mit dem Ende der Übergangsphase zum Austritt aus der EU zum 31.12.2020 ist die DSGVO in Großbritannien und Nordirland nicht mehr direkt anwendbar.

Ein am 30.12.2020 unterzeichnetes Handels- und Kooperationsabkommen zwischen der Europäischen Union und dem Vereinigten Königreich, das zum 01.01.2021 in Kraft trat, regelt zwar auch datenschutzrechtliche Fragen.[41] Es trifft aber im Kern wieder nur eine Übergangsregelung

[41] Siehe Artikel FINPROV.10.A (interim provision for transmission of personal data to the United Kingdom) des Handels- und Kooperationsabkommens.

von vier bis sechs Monaten, in der ein Angemessenheitsbeschluss der Europäischen Kommission für das Vereinigte Königreich und Nordirland gefasst werden soll.

3.3.2 Die Auswirkungen

Während der vereinbarten Übergangsphase von Februar bis Dezember 2020 gab es aus datenschutzrechtlicher Sicht für die kirchlichen Stellen und Einrichtungen zunächst keine Veränderungen.

Mit dem Jahreswechsel 2020/2021 wurde diese Übergangsregelung durch das neue Handelsabkommen ersetzt, das für den Bereich der Datenverarbeitung aber wiederum nur eine Übergangslösung von vier bis sechs Monaten enthält, in denen das Vereinigte Königreich und Nordirland nicht als Drittstaaten im datenschutzrechtlichen Sinne gelten.

Ob es mit dem Auslaufen der Übergangsregelung aus dem Handelsabkommen eine weitere Zwischenlösung geben wird, sofern bis dahin die angestrebte Angemessenheitsentscheidung der Europäischen Kommission noch nicht vorliegt, ist noch unklar und nicht absehbar.

3.3.3 Die Reaktionen der Datenschutzaufsichtsbehörden

Die Datenschutzaufsichten sowohl im staatlichen wie auch im kirchlichen Bereich haben aufgrund der unklaren Lage zu den Brexit-Verhandlungen und den damit geltenden Regelungen in der Phase nach dem Brexit immer wieder betont, die Unternehmen und Einrichtungen sollten ihre Verträge durchschauen und erfassen, an welcher Stelle Übermittlungen von Daten in das Vereinigte Königreich erfolgen und auf welcher gesetzlichen Grundlage. Auf Basis dieser Übersicht sollten dann Überlegungen erfolgen, wie mit diesen Verarbeitungen verfahren und auf welche Rechtsgrundlage diese gestützt werden könnten, sollte es kein Verhandlungsergebnis und keinen Angemessenheitsbeschluss geben, so dass Großbritannien und Nordirland den Status eines Drittlands im Sinne des Datenschutzrechts erhalten würden.

Die Diözesandatenschutzbeauftragten mussten Anfang 2021 reagieren, da mit dem Ende der Übergangsfrist Großbritannien und Nordirland endgültig aus der Europäischen Union ausgetreten waren, es aber noch keinen Angemessenheitsbeschluss gibt.

Hier enthält das KDG mit § 29 Abs. 11 KDG eine Regelung, die die DSGVO nicht enthält:

> *(11) Der Auftragsverarbeiter darf die Daten nur innerhalb der Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeiten. Abweichend von Satz 1 ist die Verarbeitung in Drittstaaten zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission gemäß § 40 Absatz 1 vorliegt oder wenn die Datenschutzaufsicht selbst oder eine andere Datenschutzaufsicht festgestellt hat, dass dort ein angemessenes Datenschutzniveau besteht.*

Während sich Unternehmen im Geltungsbereich der DSGVO für den Übergangszeitraum des neuen Handelsabkommens also noch auf die Regelung, Großbritannien sei kein Drittland, berufen können, entfällt diese Möglichkeit für kirchliche Stellen. Hier sieht das KDG eine abweichende Formulierung vor, die eine Verarbeitung ab 01.01.2021 in Großbritannien nicht mehr ermöglicht.

Die Konferenz der Diözesandatenschutzbeauftragten hat daher Anfang Januar 2021 beschlossen, dass aus Sicht der Datenschutzaufsichten mit der Übergangsregelung im Handelsabkommen die Voraussetzungen des § 29 Abs. 11 KDG als erfüllt angesehen werden können. So wurde für den kirchlichen Bereich eine Gleichstellung mit den Anwendern der DSGVO erreicht.

3.3.4 Wann kommt der Angemessenheitsbeschluss für Großbritannien und Nordirland?

Ein Angemessenheitsbeschluss wird von der Kommission der Europäischen Union vorbereitet und nach Konsultation von beziehungsweise Abstimmung mit verschiedenen Stellen letztendlich von ihr beschlossen.[42] Die Arbeiten an dem Angemessenheitsbeschluss sollen innerhalb der Übergangsfrist aus dem Handelsabkommen abgeschlossen werden. Ob dies innerhalb dieser Frist machbar ist, kann noch nicht abgeschätzt werden.[43]

3.3.5 Ausblick

Sollte es innerhalb dieses Übergangszeitraums nicht zu einer weitergehenden Vereinbarung oder zu einer Festlegung des Status des Vereinigten Königreichs aus Sicht der EU durch einen Angemessenheitsbeschluss der EU-Kommission kommen, wird das Vereinigte Königreich ab diesem Zeitpunkt als Drittland im Sinne des Datenschutzrechts mit allen sich daraus ergebenden Konsequenzen anzusehen sein.

Kirchliche Einrichtungen sollten sich daher weiterhin auf den Fall vorbereiten, dass die Datenübermittlungen in das Vereinigte Königreich und Nordirland auf eine andere Rechtsgrundlage nach den Regelungen für Datenübermittlungen in Drittländer umgestellt werden müssen. Das gilt auch in den Fällen, in denen britische Unternehmen von Vertragspartnern einer kirchlichen Einrichtung als Unterauftragnehmer eingesetzt werden oder Speicherorte in Großbritannien liegen. Dazu gehört ferner die Analyse, welche konkreten Dienstleistungen oder Serviceangebote in Anspruch genommen und welche Produkte von Herstellern oder Anbietern aus dem Vereinigten Königreich oder mit dortigen Niederlassungen oder Standorten eingesetzt werden, etwa Software, IT-Produkte, Nutzungen von Diensten und Cloud-Diensten, Konferenztools oder Serverkapazitäten. Weiter ist zu untersuchen, ob in diesem Zusammenhang Daten in das Vereinigte Königreich übermittelt werden.

[42] Zum Verfahren siehe Art. 45 DSGVO.
[43] Die Kommission hat einen ersten Entwurf des Beschlusses am 19.02.2021 veröffentlicht. Der Europäische Datenschutzausschuss hat am 13.04.2021 seine Stellungnahme dazu abgegeben.

Das Katholische Datenschutzzentrum hat die Entwicklung im Berichtszeitraum fortlaufend begleitet und die kirchlichen Einrichtungen allgemein oder in einzelnen Anfragen beraten. Es wird auch weiterhin die Entwicklungen beobachten und über die Konsequenzen berichten, die sich aus weiteren Vereinbarungen zwischen Großbritannien und der EU beziehungsweise einem möglichen Angemessenheitsbeschluss der EU ergeben.

3.4 Schwerpunkt IV: Betroffenenrechte

Ein erklärtes Ziel des europäischen Gesetzgebers bei der Einführung der DSGVO war die Stärkung der Rechte der Betroffenen bei der Verarbeitung ihrer Daten. Zur Erreichung dieses Ziels wurden die Möglichkeiten der Betroffenen in der DSGVO und dem folgend im KDG deutlich ausgeweitet, Informationen über Verarbeitungen ihrer Daten zu erhalten und auf diese Verarbeitungen Einfluss zu nehmen.

Auch im dritten Jahr der Anwendung der neuen Regelungen zeigen sich immer noch Schwierigkeiten bei der Anwendung der Betroffenenrechte durch die kirchlichen Stellen und Einrichtungen. Immer noch werden berechtigt geltend gemachte Rechte der Betroffenen nicht, nicht fristgerecht oder unvollständig erfüllt.

3.4.1 Auskunftsrecht der betroffenen Person (§ 17 KDG)

Das Recht auf Auskunft nach § 17 KDG – als eines der stärksten Betroffenenrechte – wird von den Verantwortlichen in den kirchlichen Einrichtungen weiterhin unterschätzt. Durch Anfragen und im besonderen Maße durch Beschwerden betroffener Personen, die ihr Auskunftsrecht geltend gemacht haben, aber keine oder nur eine unzureichende Auskunft erhalten haben, wurde das Katholischen Datenschutzzentrum im Berichtsjahr immer wieder auf das noch andauernde Problem aufmerksam.

Seit der Geltung des KDG sind die Betroffenenrechte stark in den Vordergrund gerückt. Gerade das Recht auf Auskunft, aber auch das Recht auf Löschung werden dabei von den kirchlichen Stellen und Einrichtungen unterschätzt. Die vom Katholischen Datenschutzzentrum immer wieder empfohlene Beschäftigung mit diesem Thema – auch als „Trockenübung" bevor ein Auskunftsersuchen eingeht – wird anscheinend in vielen Einrichtungen nicht durchgeführt. Wenn eine betroffene Person dann aber ihr Recht gegenüber dem Verantwortlichen geltend macht, ist in den Einrichtungen oft nicht klar, wie zu reagieren und wer überhaupt wie zu beteiligen ist.

> **„Seit der Geltung des KDG sind die Betroffenenrechte stark in den Vordergrund gerückt."**

Das Gesetz gibt in § 14 Abs. 3 S.1 KDG jedoch vor, dass der Verantwortliche die Anträge der betroffenen Person nach den §§ 17 bis 24 KDG **unverzüglich**, spätestens aber **innerhalb eines Monats** zu beantworten hat. Die Option, die Bearbeitungsfrist für den Antrag auf insgesamt maximal drei Monate zu verlängern (§ 14 Abs. 3 S. 2 KDG), kann nur angewendet werden, wenn dies „unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich" ist. Dies ist zu dokumen-

tieren und der Datenschutzaufsicht auf Nachfrage nachzuweisen. Weitere Voraussetzung für die Verlängerung der Bearbeitungsfrist ist, dass der Antragsteller „innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung" informiert wird. Da die Betroffenenrechte unter anderem die transparente Verarbeitung personenbezogener Daten durch Verantwortliche fördern sollen, ist bei der Begründung auch ein strenger Maßstab zu setzen. In der Praxis zeigt sich immer wieder, dass die Frist und die Voraussetzungen für die Verlängerung nicht eingehalten werden.

Gerade im Beschäftigtenkontext und wenn der Mitarbeitende schon länger bei dem Verantwortlichen beschäftigt ist, ist die Erfüllung des Auskunftsanspruchs nach § 17 Abs. 1 KDG und die Zurverfügungstellung einer Kopie nach § 17 Abs. 3 KDG oftmals mit großem zeitlichem Aufwand verbunden. Daher ist es ratsam, die Prozesse der Bearbeitung eines Auskunftsersuchens nach § 17 Abs. 1 und Abs. 3 KDG sicherzustellen und somit nicht Gefahr zu laufen, die Monatsfrist beziehungsweise die Dreimonatsfrist zu überschreiten. Sollte die Frist überschritten werden, ist alleine dies schon ein möglicher Grund für eine Beschwerde bei der Datenschutzaufsicht. Weiterhin kommen unzureichende Auskünfte hinzu, die eine Beschwerde bei der Datenschutzaufsicht begründen können.

Zwar kann die Auskunft zulässigerweise auf bestimmte Verarbeitungsvorgänge oder Zeiträume beschränkt werden, dies steht jedoch im Ermessen der betroffenen Person. Nur in den Fällen, wo dem Verantwortlichen eine Auskunft ohne Nachfrage oder Einschränkung nicht möglich oder in seltenen (und zu begründenden) Fällen in dem Umfang nicht zumutbar ist, kann der Verantwortliche von dem Antrag abweichen.

In den Fällen einer begründeten Beschwerde hat die Datenschutzaufsicht, neben der Möglichkeit nach § 47 Abs. 5 lit. f) KDG, der die Anordnung zur Erfüllung der Anträge der betroffenen Person regelt, auch die Möglichkeit, ein Bußgeld nach § 51 KDG zu verhängen.

3.4.2 Information über unmittelbare oder mittelbare Datenverarbeitung (§§ 15, 16 KDG)

Die Pflicht des Verantwortlichen, dem Betroffenen bei einer Erhebung von Daten direkt beim Betroffenen (unmittelbare Datenerhebung) oder bei Dritten (mittelbare Datenerhebung) eine Information zukommen zu lassen, besteht, vorbehaltlich der in den beiden Normen genannten Ausnahmen, immer – unabhängig von einem Antrag. Die verantwortliche Stelle hat vielmehr von sich aus dem Betroffenen die im Katalog der §§ 15 und 16 KDG genannten personenbezogenen Daten zu übermitteln.

Die Inhalte der Informationspflicht ergeben sich aus dem Katalog der §§ 15 und 16 KDG. Danach sind

- der Name und die Kontaktdaten des Verantwortlichen bekannt zu geben,

- die Kontaktdaten des betrieblichen Datenschutzbeauftragten mitzuteilen,
- durch die Mitteilung des Verarbeitungszweckes die Betroffenen darüber aufzuklären, auf welchen Erlaubnistatbestand der Verantwortliche die Datenverarbeitung stützen möchte,
- die Betroffenen über das Interesse aufzuklären, falls die Verarbeitung von personenbezogenen Daten zur Wahrung eines berechtigten Interesses des Verantwortlichen erforderlich ist,
- die Betroffenen bei Übermittlung von personenbezogenen Daten über den konkreten Empfänger zu informieren, es sei denn, konkrete Unternehmen können noch nicht bezeichnet werden, dann reicht die Bezeichnung der Kategorie von Empfängern und
- die Betroffenen darüber zu informieren, dass Daten in einen Staat oder eine internationale Organisation außerhalb des europäischen Wirtschaftsraumes übermittelt werden. Darüber hinaus ist darzustellen, welche Maßnahmen ergriffen wurden, um beim Empfänger ein angemessenes Datenschutzniveau herzustellen.

Weiterhin ist der Betroffene nach § 15 Abs. 2 KDG darüber zu informieren,

- wie lange personenbezogene Daten konkret gespeichert werden. Nur wenn eine konkrete Festlegung nicht möglich ist, reicht eine Angabe über die Kriterien für die endgültige Speicherdauer aus.
- welche Rechte er nach den §§ 17 – 20, 22 und 23 KDG hat: das Recht auf Auskunft (§ 17 KDG), das Recht auf Berichtigung (§ 18 KDG), das Recht auf Löschung (§ 19 KDG), das Recht auf Einschränkung der Verarbeitung (§ 20 KDG), das Recht auf Datenübertragbarkeit (§ 22 KDG) und das Widerspruchsrecht (§ 23 KDG).
- dass er, soweit die Verarbeitung der Daten auf einer Einwilligung der betroffenen Person beruht, diese jederzeit widerrufen kann; die Datenverarbeitung bis zum Widerruf aber rechtmäßig bleibt.
- dass er gemäß § 38 KDG das Beschwerderecht gegenüber der Datenschutzaufsicht hat.
- auf welcher Grundlage die Bereitstellung der Daten erfolgt ist.
- welche Tragweite und welche angestrebten Auswirkungen eine Entscheidung hat, wenn Verfahren einer automatisierten Entscheidung verwendet werden, und welcher Logik der verwendete Algorithmus folgt.

Ausnahmen von der Informationspflicht bestehen u. a. dann, wenn dem Betroffenen die Informationen bereits vorliegen, das Interesse des Betroffenen an der Informationserteilung gering ist und einen unverhältnismäßigen Aufwand zur Folge hätte oder die Informationen aufgrund besonderer Rechtsvorschriften oder überwiegender Interessen Dritter geheim zu halten sind. Diese Ausnahmen sind restriktiv auszulegen und im Einzelfall zu prüfen und zu begründen.

Im Falle der unmittelbaren Datenerhebung nach § 15 KDG ist die Information vor der Datenverarbeitung zur Verfügung zu stellen (§ 15 Abs. 1 KDG). Bei mittelbarer Datenerhebung ist die Information innerhalb einer angemessenen Frist nach Erlangung der Daten, spätestens nach einem Monat zu erteilen (§ 16 Abs. 2 lit. a) KDG).

3.4.3 Das Recht auf Berichtigung der eigenen Daten (§ 18 KDG)

Mit dem Recht auf Berichtigung nach § 18 KDG wird nicht die Rechtmäßigkeit der Verarbeitung an sich in Frage gestellt. Es wird nur verhindert, dass falsche Daten über eine Person verarbeitet werden. Es wird daher nicht die Rechtsgrundlage für die Verarbeitung in Frage gestellt, sondern nur die Richtigkeit der Daten.

Ein Recht auf Berichtigung besteht entweder gegen die Verarbeitung sachlich falscher personenbezogener Daten (§ 18 Abs. 1 Satz 1 KDG) oder zur Ergänzung unvollständiger personenbezogener Daten (§ 18 Abs. 1 Satz 2 KDG). Ein Anspruch gemäß § 18 Abs. 1 Satz 2 KDG setzt aber voraus, dass die personenbezogenen Daten, deren Ergänzung der Antragsteller begehrt, für den Zweck der Verarbeitung erforderlich, d. h. in Bezug auf die konkrete Verarbeitung lückenhaft sind.

3.4.4 Das Recht auf Löschung (§ 19 KDG)

§19 KDG gewährt ein Recht auf Löschung. Dieses hat zunächst zu erfolgen, wenn die Daten zu dem Zweck, zu dem sie erhoben worden sind, nicht mehr erforderlich sind, oder der Zweck weggefallen ist. Das Recht besteht auch dann, wenn eine ursprünglich erforderliche Einwilligung weggefallen ist. Die DSGVO bezeichnet dieses Recht plakativ auch als „Recht auf Vergessenwerden". Dieser Begriff wird in der Öffentlichkeit entsprechend publiziert, ist aber unscharf. Insbesondere bei veröffentlichten personenbezogenen Daten wird das Problem bestehen, dass die Daten weiterhin über Suchmaschinen bei anderen auffindbar sind und damit ein digitales „Vergessen" scheitert. § 19 Abs. 2 KDG legt dem Verantwortlichen in diesem Fall die Pflicht auf, alle vertretbaren Anstrengungen zu unternehmen, um die Stellen, welche die Daten verarbeiten, darüber zu informieren, dass die betroffene Person von ihnen die Löschung aller Links zu diesen Daten oder von Kopien u. ä. verlangt.

3.4.5 Weitere Betroffenenrechte

Zu den Betroffenenrechten zählen neben den vorgenannten Rechten auch noch weitere Rechte, wie z. B. die Möglichkeit, die Verarbeitung der Daten vorübergehend einzuschränken, wenn deren Richtigkeit streitig ist (Recht auf Einschränkung der Verarbeitung, § 20 KDG), die Möglichkeit, bestimmte Daten zwischen bestimmten Diensten übertragen zu können (Recht auf Datenübertragbarkeit, § 22 KDG) oder die Möglichkeit, der Verarbeitung der eigenen Daten zu widersprechen (Widerspruchsrecht, § 23 KDG).

Die einzelnen Voraussetzungen dieser Rechte sind den jeweiligen Normen zu entnehmen. Einen Überblick bietet auch die Praxishilfe zu den Betroffenenrechten[44].

[44] Siehe die KDG-Praxishilfe „Betroffenenrechte" (KDG-Praxishilfe Nr. 6) auf der Internetseite des Katholischen Datenschutzzentrums unter www.katholisches-datenschutzzentrum.de (Infothek > Praxishilfen).

3.5 Die Querschnittsprüfung kirchlicher Kindertagesstätten

Ende 2019 hatte das Katholische Datenschutzzentrum Fragebögen an 100 kirchliche Kindertagesstätten in seinem Zuständigkeitsbereich verschickt. Dies war der Auftakt zu einer Querschnittsprüfung kirchlicher Kindertageseinrichtungen, mit der die Umsetzung des Datenschutzes in den Einrichtungen überprüft werden sollte.[45]

Die Prüfung war in mehrere Teilabschnitte aufgeteilt. Der erste Teil begann Anfang Dezember 2019 mit einem online auszufüllenden Fragebogen.

Die Auswertung der Fragebögen fand dann parallel zum ersten Lockdown aufgrund der Corona-Pandemie statt, der mit einer Schließung der Kindertagesstätten einherging. Aus diesem Grund wurde die Weiterverfolgung der Prüfung bis zur Beruhigung der Lage ausgesetzt. Es sollte vermieden werden, dass die Einrichtungen zusätzlich zu den Belastungen durch die Pandemie weiteren Belastungen durch die Prüfung ausgesetzt würden.

Über den Sommer hinweg stabilisierte sich die allgemeine Lage, so dass einer Wiederaufnahme der Prüfung nichts entgegenstand.

Die elektronischen Fragebögen wurden nach dem zu Beginn der Prüfung festgelegten Auswertungsschema bearbeitet. Die Auswertung war so aufgebaut, dass die gesamten Antwortmöglichkeiten von optimal bis mangelhaft abgebildet waren. Bei den einzelnen Antwortmöglichkeiten war vor Beginn der Prüfung festgelegt worden, ob bei der Auswahl dieser Antwortmöglichkeit durch die Einrichtung eine weitere Nachfrage notwendig sein würde. Es wurde versucht, die aktuelle, einrichtungsspezifische Situation der jeweiligen Kindertagesstätte zu erfragen, um eine möglichst genaue Bewertungsgrundlage zu haben.

Im September 2020 wurden die Nachfragen an die geprüften Einrichtungen übermittelt. Gleichzeitig wurden die Träger über die Wiederaufnahme der Prüfung in einem separaten Schreiben informiert. Durch die im Herbst wieder zunehmende Belastung der Einrichtungen durch die Pandemie wurde die Bearbeitungsfrist auf Nachfrage bis zum Jahresende verlängert.

Mit den Nachfragen zum elektronischen Fragebogen wurden unterschiedliche Aspekte umgesetzt.

Die Nachfragen bezogen sich auf potenzielle Schwachstellen in der Datenschutzorganisation oder den technischen und organisatorischen Maßnahmen und sollten auch als Hinweis verstanden werden, die angesprochenen Punkte erneut kritisch zu betrachten.

[45] Siehe hierzu auch Abschnitt 3.11.2 des Jahresberichts 2019.

Im weiteren Verlauf der Prüfung in 2021 werden nunmehr die Ergebnisse der elektronischen Befragung und der Nachfragen zusammengestellt und in der Gesamtschau bewertet. Die ursprünglich vorgesehene stichprobenartige Vor-Ort-Überprüfung einzelner Kindertagesstätten hängt vom Verlauf der Corona-Pandemie ab. Es ist jedoch wahrscheinlich, dass dieser Prüfungsschritt vorerst zurückgestellt werden muss.

Auswertung der elektronischen Fragebögen

Bei den Nachfragen, die sich aus der Auswertung der Online-Fragebögen ergaben, sind deutliche Schwerpunkte zu erkennen. Der Hauptteil der Nachfragen entfiel auf den Bereich der Zugangskontrolle. Mit deutlichem Abstand folgte dann eine Gruppe zu den Bereichen der Weitergabekontrolle, des Löschens von Daten und der Zutrittskontrolle.

Nachfragen nach Themen

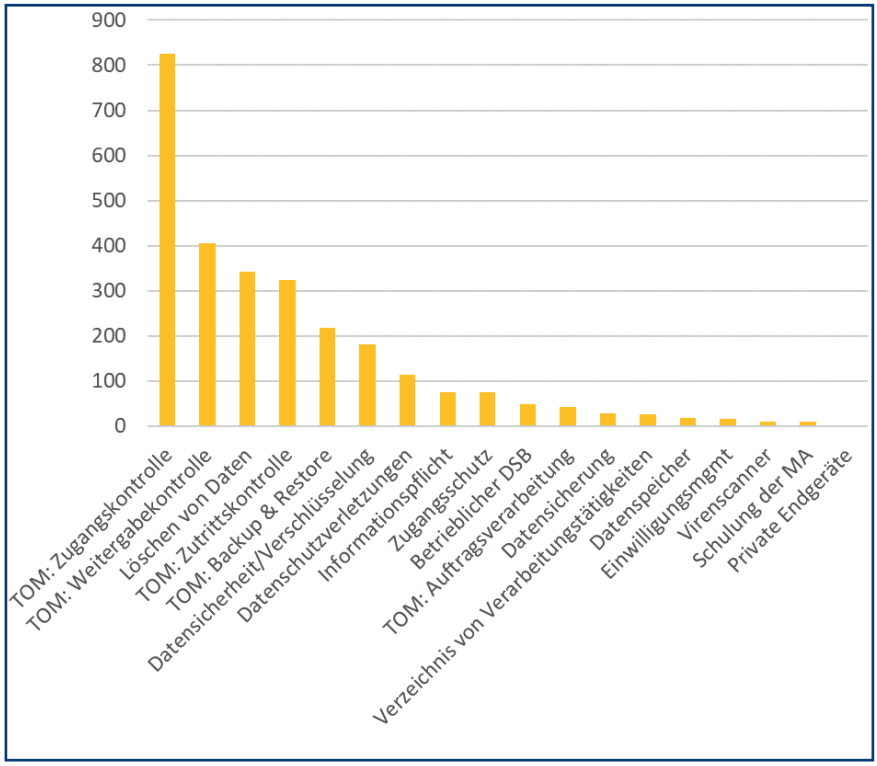


Abb.: Nachfragen nach Themen zur Querschnittsprüfung

Die Gesamtmenge der Nachfragen verteilt sich für die Themenbereiche Zugangs-, Zutritts- und Weitergabekontrolle, Datensicherung, Datensicherheit und dem Löschen von Daten flächendeckend auf fast alle geprüften Kitas. Bei den Nachfragen unauffällig waren die Bereiche der Nutzung von privaten Endgeräten, der Einsatz von Virenscannern und die Schulung von Mitarbeitern.

Kindertagesstätten mit Nachfragen nach Themen

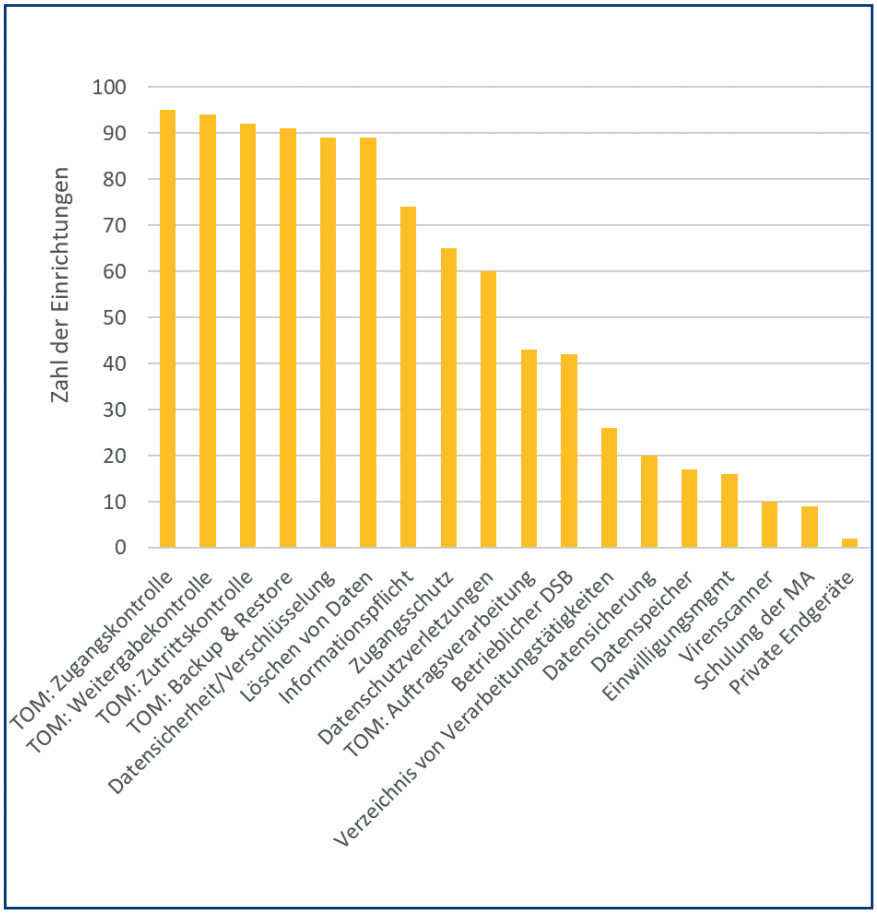


Abb.: Zahl der Kindertagesstätten mit Nachfragen nach Themen zur Querschnittsprüfung

Im ersten Halbjahr 2021 wird die Querschnittsprüfung mit den abschließenden Scheiben an die geprüften Einrichtungen abgeschlossen werden.

Ziel der Querschnittsprüfung war es von vornherein, das Datenschutzniveau in Kindertagesstätten insgesamt zu erhöhen. Dies betrifft selbstverständlich nicht nur die in der Querschnittsprüfung geprüfte Stichprobe, sondern Kindertagesstätten im Allgemeinen. Anhand der Rückmeldungen von an der Querschnittsprüfung teilnehmenden und nicht teilnehmenden Einrichtungen hat das Katholische Datenschutzzentrum feststellen können, dass man diesem Ziel einen Schritt nähergekommen ist. Das Thema Datenschutz wird flächendeckend im Bereich der Kindertagesstätten mit einer höheren Priorität behandelt. Es wäre wünschenswert, wenn diese positive Entwicklung fortgeschrieben würde.

„Ziel der Querschnittsprüfung war es von vornherein, das Datenschutzniveau in Kindertagesstätten insgesamt zu erhöhen."

3.6 Beschwerden

Auch in diesem Berichtszeitraum nutzten wieder viele Personen die gesetzliche Möglichkeit, sich über eine aus ihrer Sicht nicht gesetzeskonforme Behandlung ihrer personenbezogenen Daten durch kirchliche Stellen und Einrichtungen zu beschweren.

3.6.1 Stichwort: Beschwerde/Hinweis/anonyme Beschwerde

Bei einer Beschwerde macht eine Person die Verletzung gesetzlicher Vorgaben bei der Verarbeitung der eigenen Daten geltend. Die Person muss also selbst betroffen sein, um sich zu beschweren (Beschwerdebefugnis).

Macht die Person, die sich an das Katholische Datenschutzzentrum wendet, eine Verletzung gesetzlicher Vorgaben bei der Verarbeitung von personenbezogenen Daten anderer Personen geltend, für die diese Person nicht in geeigneter Form legitimiert ist (z. B. als Erziehungsberechtigter, als gesetzlicher Betreuer, mit Vollmacht, als Rechtsanwalt), so handelt es sich um einen Hinweis auf eine Datenschutzverletzung (z. B. Mitarbeitende weisen auf eine nicht datenschutzkonforme Verarbeitung von Daten anderer Personen in einer kirchlichen Einrichtung hin). Die Bearbeitung der Hinweise erfolgt entsprechend der Bearbeitung der Beschwerden. Im Unterschied zur Beschwerdebearbeitung wird der Hinweisgeber nicht formal über den Abschluss der Bearbeitung des Hinweises informiert, da bei der Person selbst keine Beschwer vorliegt und damit keine Rechtsschutzmöglichkeit eröffnet ist.

Aufgrund von persönlichen Arbeits- oder Betreuungssituationen kommt es auch vor, dass Beschwerden anonym beim Katholischen Datenschutzzentrum eingehen, da die Personen zwar auf Missstände aufmerksam machen wollen, sich aber gefühlt oder tatsächlich negativen Konsequenzen ausgesetzt sehen, wenn sie als Beschwerdeführer bekannt würden. Da dem KDSZ in diesen Fällen kein Beschwerdeführer bekannt ist, bei dem konkret überprüft werden kann, ob seine Rechte verletzt worden sind, werden solche Eingaben als Hinweise behandelt. Sollte durch den Hinweis die mögliche Datenschutzverletzung hinreichend substantiiert vorgetragen worden sein und ausgeschlossen werden können, dass hier das anonym ausgeübte Beschwerderecht aus persönlichen Gründen missbraucht wird, nimmt das Katholische Datenschutzzentrum die Bearbeitung des Sachverhaltes aufgrund des dann hinreichend konkreten Verdachts einer möglichen Datenschutzverletzung auf.

Bei Hinweisen und anonymen Beschwerden ist eine Bewertung des vorgetragenen Sachverhaltes ohne die Offenlegung der Identität der betroffenen Personen für das KDSZ unter Umständen nur sehr schwer oder gar nicht möglich, es sei denn, es handelt sich um eine Beschwerde, bei der die Identität des Betroffenen für die Aufklärung der Datenschutzverletzung nicht notwendig ist (z. B. bei offen ausliegenden Corona-Listen).

3.6.2 Thematische Schwerpunkte

Inhaltlich richteten sich im Berichtszeitraum viele Beschwerden gegen Verarbeitungen von Daten im Zusammenhang mit Corona und gegen den Umgang der kirchlichen Stellen mit den Betroffenenrechten.[46] Neben weiteren thematischen Schwerpunkten wie dem Beschäftigtendatenschutz oder dem Schutz der Patientendaten, waren von den Beschwerden alle Einrichtungstypen und eine breite Palette verschiedener Situationen der Verarbeitung personenbezogener Daten betroffen.

Beschwerden zur Verarbeitung der Daten im Zusammenhang mit der Corona-Pandemie

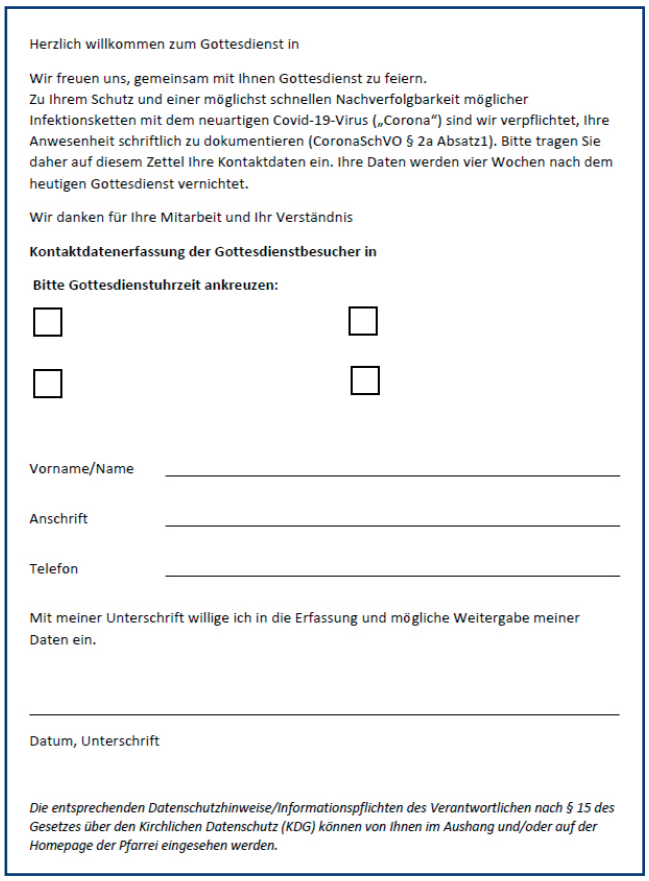
Im Zusammenhang mit der Corona-Pandemie beziehungsweise deren Folgen erreichten das Katholische Datenschutzzentrum viele Beschwerden.

Auch das schon in Abschnitt 3.1 dieses Jahresberichts angesprochene Thema der Umsetzung der Vorgaben zur Kontaktnachverfolgung bei Gottesdiensten war Gegenstand vieler Beschwerden.

Ein Aspekt waren Listen, auf denen die Kontaktdaten aller Gottesdienstbesucher eingetragen waren, so dass die jeweils nächste Person, die sich auf der Liste einträgt, alle Daten der vorhergehenden Personen einsehen konnte. Hier unterscheidet sich die datenschutzrechtliche Bewertung nicht von ähnlichen Fällen außerhalb der Corona-Pandemie, in denen Anwesenheits- oder Teilnehmerlisten geführt werden. In jedem Fall ist bei der Eintragung sicherzustellen, dass die Daten der vorhergehenden Personen nicht für die nachfolgenden einsehbar sind.

Als Lösung hat z. B. die Diözese Münster den Pfarreien die Nutzung von Karten vorgeschlagen, auf denen die einzelnen Personen ihre Daten eintragen und die dann in der Kirche vor dem Gottesdienst in eine Box eingeworfen werden. So kann eine Kenntnisnahme Dritter vermieden werden.

[46] Siehe hierzu auch die Abschnitte 3.1 und 3.4 dieses Jahresberichts.



Herzlich willkommen zum Gottesdienst in

Wir freuen uns, gemeinsam mit Ihnen Gottesdienst zu feiern.
Zu Ihrem Schutz und einer möglichst schnellen Nachverfolgbarkeit möglicher Infektionsketten mit dem neuartigen Covid-19-Virus („Corona") sind wir verpflichtet, Ihre Anwesenheit schriftlich zu dokumentieren (CoronaSchVO § 2a Absatz1). Bitte tragen Sie daher auf diesem Zettel Ihre Kontaktdaten ein. Ihre Daten werden vier Wochen nach dem heutigen Gottesdienst vernichtet.

Wir danken für Ihre Mitarbeit und Ihr Verständnis

Kontaktdatenerfassung der Gottesdienstbesucher in

Bitte Gottesdienstuhrzeit ankreuzen:

☐ ☐

☐ ☐

Vorname/Name _____

Anschrift _____

Telefon _____

Mit meiner Unterschrift willige ich in die Erfassung und mögliche Weitergabe meiner Daten ein.

_____

Datum, Unterschrift

Die entsprechenden Datenschutzhinweise/Informationspflichten des Verantwortlichen nach § 15 des Gesetzes über den Kirchlichen Datenschutz (KDG) können von Ihnen im Aushang und/oder auf der Homepage der Pfarrei eingesehen werden.

Abb.: Muster aus dem Schreiben des Generalvikars der Diözese Münster vom 29.05.2020[47]

Inhaltsgleiche Beschwerden erhielt das Katholische Datenschutzzentrum aus dem Bereich der Krankenhäuser und Pflegeeinrichtungen. Auch bei diesen Beschwerdefällen wurden die Besuchslisten ebenfalls nicht immer datenschutzkonform geführt.

Andere Beschwerden betrafen die Verwendung der so gesammelten Daten der Gottesdienstbesucher zu anderen Zwecken als dem der Kontaktnachverfolgung. Hier hat das Katholische Datenschutzzentrum immer darauf hingewiesen, dass auch für diese personenbezogenen Daten eine strenge Zweckbindung gilt. Dieser allgemeine Grundsatz des Datenschutzrechts wurde mit der Änderung des Infektionsschutzgesetzes für die Kontaktdaten zur Kontaktnachverfolgung in § 28a Absatz 4 IfSG nochmals ausdrücklich festgeschrieben.

Beschwerden zur Verarbeitung von Patientendaten

Ebenfalls aus dem Bereich der Krankenhäuser und Pflegeeinrichtungen (aber nicht im Zusammenhang mit der Corona-Pandemie) bekam das Katholische Datenschutzzentrum viele Beschwerden zum Umgang mit Patientendaten.

In diesen Themenbereich fallen einmal die Beschwerden zu falsch versandten Patientenunterlagen. Die eingereichten Beschwerden umfassten sowohl falsch versandte Arztbriefe oder Abrechnungen zu Krankenhausaufenthalten aufgrund von Fehlern bei der Bearbeitung der Ausgangspost in den Einrichtungen, als auch an falsche Adressaten von

[47] Der Brief und das Muster sind abrufbar unter https://www.bistum-muenster.de/corona/brief_des_generalvikars_mit_den_mustervorlagen_zur_rueckverfolgbarkeit_bei_veranstaltungen_anwesender_personen/

Arztbriefen, bei denen in der Patientenakte ein falscher behandelnder Arzt eingetragen war und der Entlassbericht daher auch an den falschen Arzt versendet wurde.

Sachverhalte in diesem Bereich haben oft eine besondere Brisanz, da die fehlgeleiteten Informationen als Gesundheitsdaten zu den besonderen Kategorien personenbezogener Daten gehören und einem besonderen Schutz unterliegen müssen.

Beschwerden zur Verarbeitung von Beschäftigtendaten

Aus dem Themenbereich des Beschäftigtendatenschutzes erreichten das Katholische Datenschutzzentrum im Berichtszeitraum beispielsweise Beschwerden über die Weitergabe von Bewerberdaten im Bewerbungsverfahren. Hier müssen die Einrichtungen darauf achten, dass Bewerberdaten nur an die im regulären Prozess der Bewerberauswahl direkt beteiligten Personen weitergegeben werden dürfen. An andere – auch interne – Stellen dürfen die Bewerberdaten nicht weitergegeben werden. Auch eine Nachfrage beim vorherigen oder aktuellen Arbeitgeber des Bewerbers beinhaltet schon eine Übermittlung personenbezogener Daten und kann daher nur mit Einwilligung des Bewerbers erfolgen.

Beschwerden zum Recht auf Auskunft

Als zentrales Betroffenenrecht ist das Recht auf Auskunft nach § 17 KDG oft Thema der Aufsichtstätigkeit des Katholischen Datenschutzzentrums.

Bei den hierzu im Berichtszeitraum eingegangenen Beschwerden wurden von den Beschwerdeführern unterschiedliche Punkte moniert. Insgesamt zeigt sich jedoch weiterhin, dass sich der datenschutzrechtlich korrekte Umgang und damit die Gewährleistung des Rechts auf Auskunft durch die kirchlichen Verantwortlichen oftmals als schwierig darstellt und daher nur eine unzureichende und verspätete Beantwortung des Auskunftsersuchens erfolgt. Gerade die Einhaltung der Monatsfrist (vgl. § 14 Absatz 3 Satz 1 KDG mit der Möglichkeit zur Verlängerung nach Satz 2) war oftmals ein Beschwerdegrund. Dabei ist darauf zu achten, dass eine Verlängerung der Bearbeitungszeit des Verantwortlichen zur Beantwortung der Auskunftsanfrage nur möglich ist, wenn innerhalb der Monatsfrist die Verspätung der Auskunft begründet dargelegt wird. Das Recht auf Beschwerde beim Katholischen Datenschutzzentrum nach § 48 Abs. 1 KDG wird schon dadurch ausgelöst, dass diese Fristen überschritten sind, es kann aber nicht schon vorab in Erwartung einer Überschreitung der Frist geltend gemacht werden.

In der Aufarbeitung der Beschwerden wurde oft deutlich, dass die Verantwortlichen nicht auf die Beantwortung von Auskunftsanfragen vorbereitet waren und keine internen Prozesse existierten, um das Auskunftsersuchen zeitlich und inhaltlich gesetzeskonform zu beantworten. Gerade im Falle von langjährigen Mitarbeitenden oder häufigen Kontakten über einen längeren Zeitraum (z. B. als Patient) ist dies eine nicht zu unterschätzende Aufgabe und sollte daher klaren Verfahrensvorgaben unterliegen, um Beschwerden und möglicherweise Bußgelder in diesem Bereich zu vermeiden.

Da das Gesetz über den Kirchlichen Datenschutz und somit das Recht auf Auskunft aus § 17 KDG nun seit mehr als zwei Jahren Anwendung findet, geht das Katholische Datenschutzzentrum bei der Bewertung etwaiger Beschwerden davon aus, dass die Verantwortlichen eben diese Prozessabläufe zur Sicherstellung einer gesetzeskonformen Beantwortung von Auskunftsanfragen mittlerweile implementiert haben (sollten).

3.7 Meldungen

Im Berichtszeitraum erreichten das Katholische Datenschutzzentrum weiterhin eine hohe Anzahl von Meldungen von Datenschutzverletzungen nach § 33 KDG. Im Vergleich zum Vorjahr hat sich die Zahl der Meldungen von Datenschutzverletzung im Berichtszeitraum nochmals um weit über 50 % erhöht. Im Vergleich zum Jahr 2018 hat das KDSZ im Jahr 2020 fast fünf Mal mehr Meldungen über Datenschutzverletzungen erhalten.

Bei den eingereichten Meldungen waren oft Nachfragen notwendig, da die Meldungen nicht alle notwendigen Informationen enthielten. Hier erleichterte es die Bearbeitung für beide Seiten, wenn die auch im Meldeformular schon abgefragten Informationen direkt bereitgestellt wurden.

Trotz der hohen Anzahl dieser in vielen Fällen leicht zu vermeidenden Datenschutzverletzungen konnte das Katholische Datenschutzzentrum in vielen Einrichtungen positiv feststellen, dass diese in ihren Häusern die Integration eines Datenschutz-Managementsystems vorangetrieben haben und die Sensibilisierung der Mitarbeitenden in Bezug auf den Datenschutz weiter vorangeschritten ist. Positiv sind auch die Maßnahmen hervorzuheben, die die Einrichtungen zur Vermeidung weiterer Datenschutzverletzungen vornehmen.

3.7.1 Stichwort: Meldewege

„In der Praxis ist es ratsam, die Meldung schriftlich an das KDSZ zu richten."

Liegt eine Verletzung des Schutzes personenbezogener Daten vor, muss die verantwortliche Stelle dies gemäß § 33 KDG unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung an die Aufsicht melden. Eine Überschreitung der 72-Stunden-Frist muss in der Meldung begründet werden.

Grundsätzliche Fragen zu der Erstellung einer Meldung, den notwendigen Unterlagen oder dem Ablauf der Bearbeitung einer Meldung können telefonisch im Rahmen der Beratung durch das Katholische Datenschutzzentrum beantwortet werden. Für die Meldung selbst ist keine besondere Form vorgesehen. In der Praxis ist es ratsam, die Meldung schriftlich an das KDSZ zu richten.

Zur Erleichterung des Meldevorgangs stellt das Katholische Datenschutzzentrum unterschiedliche Wege zur Meldung einer Datenschutzverletzung zur Verfügung. So hat das KDSZ ein Formular auf der Home-

page eingerichtet. Hier können alle wichtigen Informationen sicher an die Aufsicht übermittelt werden. Bei Meldungen per E-Mail ist darauf zu achten, dass personenbezogene Daten nicht auf unsicherem Weg versandt werden. Für eine sichere Datenübertragung an das KDSZ kann eine gesicherte E-Mail per DE-Mail oder durch Nutzung unseres S/MIME-Zertifikates gesendet werden.

3.7.2 Unvollständige und vorläufige Meldungen

Im Allgemeinen werden durch das Meldeformular die wichtigsten Informationen abgefragt und der Meldende wird auf die Notwendigkeit bestimmter Informationen hingewiesen. Es kommt jedoch häufig vor, dass bei der Beschreibung des Datenschutzvorfalls, der ergriffenen Maßnahmen sowie der Folgen der Datenschutzverletzung nicht alle wesentlichen Informationen mitgeteilt werden.

Einer der Schritte der Datenschutzaufsicht im Rahmen der Bearbeitung von Meldungen von Datenschutzverletzungen ist es, das Risiko für die Betroffenen zu bewerten. Anhand dieser Bewertung kann dann im nächsten Schritt die Angemessenheit der ergriffenen Maßnahmen beurteilt werden. Ziel des Instruments der Meldung von Datenschutzverletzungen nach § 33 KDG ist es, durch das frühzeitige Einleiten von Gegenmaßnahmen eventuelle Schäden bei den Betroffenen zu vermeiden oder zumindest zu minimieren.

Damit eine Meldung diese Funktion erfüllen kann, werden daher zunächst alle wesentlichen Tatsachen bezüglich der eigentlichen Datenschutzverletzung benötigt. So reicht z. B. die grundsätzliche Mitteilung der Tatsache eines Einbruchs ohne weitere Angaben nicht aus. Entscheidend ist vielmehr, dass im Meldungstext mitgeteilt wird, welche personenbezogenen Daten genau innerhalb der Einrichtung nachweislich betroffen sind oder betroffen sein könnten. Darüber hinaus sind zur Abschätzung des Risikos Informationen bezüglich der Anzahl der möglicherweise oder nachweislich betroffenen Personen notwendig.

Es ist daher aus Sicht der Datenschutzaufsicht wichtig, dass sämtliche relevanten Tatsachen in der Meldung mitgeteilt werden.

Liegen dem Verantwortlichen zum Zeitpunkt der Meldung der Datenschutzverletzung noch nicht sämtliche Tatsachen vor, d. h. dem Verantwortlichen ist es noch nicht möglich, alle Informationen bereits zum Zeitpunkt der Meldung zusammenzutragen, muss dennoch im Rahmen der Regelung des § 33 KDG die Meldung bereits abgegeben werden. Diese Meldung ist dann als "vorläufig" zu kennzeichnen. Weitere Informationen sind dann gemäß § 33 Abs. 4 KDG im Nachgang zur Verfügung zu stellen. Hierbei müssen die Informationen in dem Rahmen, in dem sie ermittelt werden, schrittweise ohne unangemessene Verzögerungen mitgeteilt werden. Der Grund hierfür liegt erneut in der Aufgabe der Schadensminimierung für die durch die Datenschutzverletzungen betroffenen Personen. Dies bedeutet auch, dass es sich hierbei um eine Bringpflicht des Verantwortlichen handelt. Es ist nicht die Aufgabe der Datenschutzaufsicht, hier die noch fehlenden Informationen in wiederkehrenden Intervallen abzufragen.

Im Rahmen der Bearbeitung etlicher Meldungen im Berichtszeitraum hat das Katholische Datenschutzzentrum festgestellt, dass in vielen Einrichtungen der Meldeprozess in Bezug auf die (vorläufigen) Meldungen noch nicht klar definiert ist. Dies führte in vielen Fällen zu einer Überprüfung des Meldeprozesses und dem Erlass entsprechender Anordnungen von Seiten der Datenschutzaufsicht zur gesetzeskonformen Gestaltung des Prozesses.

3.7.3 Nutzung offener E-Mail-Verteiler

Bei den im Berichtszeitraum eingegangenen Meldungen fallen die Meldungen zur Nutzung offener E-Mail-Verteiler auf. Diesen Meldungen liegen Vorgänge zugrunde, bei denen an eine große Anzahl von Empfängern eine E-Mail verschickt wird und alle Adressen im An- oder CC-Feld eingetragen sind. Damit sind die Adressen aber für alle Empfänger sichtbar, was – bis auf wenige Ausnahmefälle - eine Übermittlung von Daten an die anderen Empfänger der E-Mail darstellt, für die im Regelfall keine Rechtsgrundlage vorliegt.

Während zu Beginn des Jahres eine durchschnittliche Anzahl an Meldungen mit diesem Hintergrund verzeichnet wurden, gab es einen sprunghaften Anstieg in den Monaten des harten Lockdowns aufgrund der Corona-Pandemie. Gerade zu Beginn des jeweiligen Lockdowns im März und Dezember 2020 stiegen die Zahlen deutlich an. Dies lässt sich wahrscheinlich auf die erhöhte Zahl von Informationen zurückführen, die zu diesen Zeitpunkten z. B. an Eltern, Schüler, Kursteilnehmer oder Patienten per E-Mail versandt wurden. Bei dem Versand kam es dann, auch wohl aufgrund der neuen Situation, zu unbeabsichtigten Sendungen mit offenen Email-Verteilern.

Bei E-Mail-Adressen handelt es sich um personenbezogene Daten gemäß § 4 Nr. 1 KDG. Die Verwendung eines offenen E-Mail-Verteilers ist datenschutzrechtlich unzulässig, wenn die Inhaber der E-Mail-Adressen dazu nicht ihre Einwilligung erklärt haben. Bei Eintragung der E-Mail-Adressen in das An- oder CC-Feld sehen sowohl die unmittelbaren Empfänger (An-Feld) als auch die Empfänger der Kopien (CC-Feld) dieser E-Mail, an wen diese sonst noch geschickt wurde. Nur bei Eintragung der E-Mail-Adressen in das BCC-Feld wird die Übertragung der E-Mail-Adressen an die Empfänger unterdrückt, so dass niemand erkennen kann, an wen diese E-Mail sonst noch verschickt wurde. Durch die unbefugte und nicht notwendige Offenlegung der E-Mail-Adressen, werden diese den anderen Adressaten bekannt. Ein Missbrauch ist zumindest nicht auszuschließen, so dass regelmäßig von einem meldepflichtigen Vorgang auszugehen ist.

3.7.4 Unbefugte Offenlegung von Daten durch fehlerhaften Postversand

Ein großer Teil der in 2020 eingegangenen Meldungen betraf den Fehlversand von personenbezogenen Daten. Hierbei kam es vermehrt zum Fehlversand von Gesundheitsdaten und Gehaltsabrechnungen per Post.

Gesundheitsdaten

Bei Gesundheitsdaten handelt es sich um personenbezogene Daten der besonderen Kategorie gemäß § 4 Nr. 2 KDG i. V. m. § 4 Nr. 17 KDG. Besondere Kategorien personenbezogener Daten unterliegen einem erhöhten Schutzniveau und sind gemäß § 13 KDG-DVO der Datenschutzklasse III zuzuordnen. Dementsprechend ist der Umgang mit medizinischen Befunden durch organisatorische und technische Schutzmaßnahmen so abzusichern, dass diese höheren Anforderungen an den Schutz der Gesundheitsdaten erfüllt werden können.

Die dem Katholischen Datenschutzzentrum gemeldeten Fehlversendungen hatten verschiedene Ursachen, wobei zwei Konstellationen dabei häufiger auftraten.

In der ersten Variante wurden bei der Kuvertierung der Schreiben Dokumente mehrerer Empfänger in einen Umschlag gesteckt und damit neben einem Dokument, das an den richtigen Empfänger gesandt wurde, auch noch ein Dokument eines anderen Empfängers in den Umschlag gesteckt, welches durch die gemeinsame Versendung beider Dokumente bei dem falschen Empfänger ankam. In der zweiten Variante wurden Inhalte vertauscht. Dies kann durch eine falsche Zuordnung des Patienten zu einem überweisenden Arzt oder Hausarzt im Krankenhausinformationssystem erfolgen, so dass der Brief zwar an den angegebenen Empfänger gesendet wird, dieser Empfänger aber die Informationen eigentlich gar nicht bekommen dürfte. Teilweise wurden Schreiben eines Patienten auch Anlagen eines anderen Patienten zugeordnet und damit fälschlich zusammen verschickt. Diese Konstellation ähnelt vom Ablauf her der oben beschriebenen ersten Variante (zwei Briefe in einem Umschlag).

Als Ursache für den Fehlversand konnte festgestellt werden, dass beim Verpackungsvorgang oder bei der Zuordnung Patient-Hausarzt im System beziehungsweise Brief und Anlage zum Brief Fehler gemacht wurden.

In den meisten Fällen waren zusätzliche Maßnahmen für die Sicherstellung der Prozesssicherheit notwendig. Aufgrund des für Gesundheitsdaten geltenden besonders hohen Schutzniveaus ist es erforderlich, dass der korrekte Versand bereits auf Prozess- und Ablaufebene sichergestellt wird, um das Fehlerpotenzial bei der Durchführung der Tätigkeit auf ein Mindestmaß zu reduzieren. Die tatsächlich zu ergreifenden Maßnahmen sind abhängig von den spezifischen Gegebenheiten vor Ort. Welche konkreten technischen und organisatorischen Maßnahmen zu ergreifen sind, um die Sicherheit des Versands zu gewährleisten, liegt beim Verantwortlichen. Entscheidend für die Bewertung ist hier die Sicherstellung des Schutzniveaus in der Gesamtschau.

Von der grundsätzlichen Pflicht zur Meldung der Datenschutzverletzung an die Datenschutzaufsicht, an die § 33 KDG nur geringe Voraussetzungen stellt, ist die weitergehende Pflicht zur Information der von der Datenschutzverletzung betroffenen Personen nach § 34 KDG zu unterscheiden. Hier sieht das Gesetz eine höhere Hürde vor, bevor diese Verpflichtung greift. Die Verantwortlichen haben die in § 34 KDG vorgesehene Risikoabschätzung zu treffen und nachvollziehbar zu dokumen-

tieren. In der Praxis waren die Entscheidungen der Verantwortlichen, die Betroffenen nicht zu informieren, da aus Sicht des Verantwortlichen kein hohes Risiko für die persönlichen Rechte und Freiheiten der Personen bestand, für die Datenschutzaufsicht mangels ausreichender Dokumentation nicht immer nachvollziehbar.

Gehaltsabrechnungen

Gehaltsdaten fallen an sich zwar nicht in die Gruppe der besonderen Kategorien personenbezogener Daten, unterfallen jedoch gemäß § 13 KDG-DVO dem Schutzniveau der Klasse III. Darüber hinaus werden Gehaltsdaten in vielen Fällen durch Dienstleister als Auftragsverarbeiter bearbeitet, so dass für die Verantwortlichen zusätzliche Kontrollpflichten entstehen.

Bei den an das KDSZ gemeldeten Fällen von Fehlversand von Gehaltsdaten handelte es sich mehrfach um Fehler auf Seiten des Auftragsverarbeiters. Hierbei wurden entweder mehrere Einzel-Abrechnungen in einem Brief versendet oder die gesammelten Gehaltsabrechnungen gingen insgesamt im Versand an eine unzuständige Stelle.

Kritisch zu bewerten war oftmals die Durchlässigkeit des Meldeprozesses zwischen Auftragsverarbeiter und Verantwortlichem. Hier kam es mehrfach zur Überschreitung der Frist von § 33 Abs. 1 KDG, so dass eine grundsätzliche Überarbeitung der betroffenen Prozesse angeordnet werden musste. Hier müssen Auftragsverarbeiter und Verantwortlicher auf die Einhaltung ihrer jeweiligen Pflichten achten. Für Auftragsverarbeiter bedeutet dies unter anderem, dass der Verantwortliche nach § 33 Abs. 2 KDG unverzüglich von einer Datenschutzverletzung zu informieren ist.

Gleichfalls kritisch zu bewerten war, dass in vielen Fällen der verantwortlichen Stelle nicht klar war, welche Maßnahmen hinsichtlich der falsch verwendeten Irrläufer zu ergreifen waren. So musste in diesen Fällen besonders darauf hingewiesen werden, dass Maßnahmen zu ergreifen sind, um die Irrläufer dem unberechtigten Zugriff zu entziehen und sicherzustellen, dass die in den Schreiben enthaltenen Informationen nicht weitergetragen werden.

3.7.5 Verschlüsselungs- und Erpressungstrojaner

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Dezember 2020 in einem Lagebild[48] festgestellt, dass die COVID-19-Pandemie erhebliche Auswirkungen auf die IT-Sicherheitslage in Deutschland hat. So sei z. B. seit März 2020 ein erheblicher Anstieg von versuchten und auch gelungenen Angriffen mit Verschlüsselungs- und Erpressungstrojanern zu verzeichnen. Die Behörde stellt dabei auch eine erhöhte Aggressivität der Erpressungsmethoden sowie immer mehr Fälle des „Big-Game Hunting“ (deutsch: „Großwildjagd“) fest, bei denen vermeintlich zahlungskräftige Organisationen von den Kriminellen ins Visier genommen werden.

[48] Deutsch-französisches IT-Sicherheitslagebild Vol. 3 - Dezember 2020, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DE-FR-Lagebild/de-fr_Lagebild_2020.html?

Aus dem Bereich der durch das KDSZ beaufsichtigten Einrichtungen wurden ihm im Jahr 2020 mehrere Datenschutzverletzungen gemeldet, die ursächlich in dem Befall der IT-Systeme mit einem Erpressungstrojaner begründet waren.

Bei den gemeldeten Vorfällen handelt es sich oft um eine Schadsoftware, die sich im kompletten Netzwerk der betroffenen Einrichtung ausbreitet, in allen erreichbaren Verzeichnissen alle Dateien verschlüsselt und anschließend einen „Erpresserbrief" z. B. als Textdatei hinterlässt, der zur Kontaktaufnahme mit den Kriminellen auffordert. Nicht nur die Benutzerdaten und E-Mail-Konten waren betroffen, sondern auch Backup-Dateien, die in vermeintlich „versteckten" Bereichen des Dateisystems abgelegt waren. Gegen Zahlung eines „Lösegeldes" wird die komplette Entschlüsselung der Dateien versprochen.

Während das Schutzziel der Verfügbarkeit offensichtlich in jedem dieser Fälle berührt wird, ist meistens unklar, ob auch Daten an den Angreifer abgeflossen sind und damit auch das Schutzziel der Vertraulichkeit betroffen ist. Aufklärung kann dann oft nur durch Spezialisten (IT-Forensiker) erfolgen, wenn diese frühzeitig eingeschaltet werden.

In der Regel dringt der Schädling über das Öffnen von infizierten Dateianhängen oder das Anklicken von Weblinks in E-Mails in die Netzwerke ein. Dazu werden zuvor – je nach Umfang der Vorbereitung des Angriffs – durchaus echte und existierende E-Mail-Kontakte und E-Mail-Kommunikationen ausgespäht und abgefangen, um dann unter Nachbildung einer auf den ersten Blick plausibel erscheinenden E-Mail-Antwort den Empfänger zum Öffnen des präparierten Datei-Anhangs oder zum Aufruf des Web-Links aufzufordern. In einem weiteren Schritt wird dann weitere Schadsoftware, etwa ein Verschlüsselungsprogramm, nachgeladen.

Das Katholische Datenschutzzentrum empfiehlt allen kirchlichen Einrichtungen, ihre Mitarbeitenden für die Erkennung solcher Phishing-Mails zu sensibilisieren und die Hilfestellungen des BSI zur Vorbeugung eines Angriffs zu befolgen. Außerdem sollten die kirchlichen Einrichtungen die Situation zum Anlass nehmen, die für den Schutz personenbezogener Daten notwendigen technischen und organisatorischen Schutzmaßnahmen auf ihre Wirksamkeit zu prüfen.

Bei der Eindämmung der Folgen eines Befalls mit Schadsoftware sind Backups ein sehr wichtiger Bestandteil. Um eine wirksame Option zur Wiederherstellung der Daten sein zu können, sollte sichergestellt sein, dass die Backups für die Schadsoftware nicht über das Netzwerk der Einrichtung erreichbar sind, sie regelmäßig erstellt werden und dass diese auch wiederherstellbar sind. Dazu sind regelmäßige Tests des Wiederherstellungsverfahrens notwendig. Sind im Falle eines Angriffs auf die Einrichtung Daten verschlüsselt worden, es liegen aber aktuelle Backups vor, die zurückgespielt werden können und auf deren Basis die Arbeit nahtlos fortgesetzt werden kann, ist trotz des Trojaner-Befalls das Schutzziel der Verfügbarkeit nicht gefährdet.

Bei Entdeckung einer Schadsoftware sollten die IT-Verantwortlichen der Einrichtung unverzüglich gemäß den in der Einrichtung für solche

Fälle vorhandenen Notfallplänen agieren. Die Polizei in NRW hat eine zentrale Stelle „Cybercrime" eingerichtet, die in diesen Fällen ebenfalls weiterhelfen kann.

3.7.6 Umgang mit Papierakten

Auch wenn immer mehr Prozesse auf eine rein digitale Verarbeitung von Daten umgestellt werden, basieren die Abläufe z. B. in Krankenhäusern, Schulen, Kindertageseinrichtungen und Verwaltungen oft noch auf der Nutzung von Papier. Personenbezogene Daten finden sich also nicht nur in den elektronischen Systemen, sondern auch auf beinahe jedem Schriftstück, das in den Einrichtungen bearbeitet wird.

Der Schutz für den Datenträger Papier ist deshalb sorgfältig zu planen und durchzuführen. Er muss sich über die komplette Lebensdauer der aufgezeichneten Daten erstrecken. Diese beginnt z. B. bei der Erstellung der Ausdrucke, erstreckt sich über die zweckbestimmte Verwendung, Aufbewahrung und Weitergabe bis zur physischen Löschung.

Beim Umgang mit den Papierakten gibt es viele Prozessschritte, bei denen Fehler passieren, die manchmal zu meldepflichtigen Datenschutzverletzungen führen können. Im Berichtsjahr 2020 wurde dem Katholischen Datenschutzzentrum eine nennenswerte Anzahl solcher Datenschutzverletzungen gemeldet.

Dabei können Fehler in allen Phasen der Verarbeitung der Daten zu diesen Schutzverletzungen führen:

Beim Drucken

Ein Drucker in einem eigenen Druckerraum ist gut für einen emissionsarmen Arbeitsplatz, aber nicht das ideale Werkzeug für den Ausdruck sensibler Personaldaten von der Gehaltsabrechnung bis zum Kündigungsschreiben, wenn dieser Druckerraum für alle Mitarbeitenden zugänglich ist. Zeitgemäße Großdrucker verfügen über Autorisierungsfunktionen wie PIN oder Token, mit denen sichergestellt wird, dass nur der berechtigte Absender des Druckjobs das Papier in Empfang nehmen kann. Nebenbei lassen sich über solche Identifizierungssysteme die Druckausgaben auch an jedem anderen so ausgestatteten Drucker im Netzwerk abrufen (FollowMe-Funktion).

Bei der Aufbewahrung

Für die Aufbewahrung der Papierakten sind dem Inhalt der Akten entsprechende Schutzmaßnahmen zu ergreifen. Je sensibler die aufbewahrten Daten sind, desto höher sind die Anforderungen an eine Aufbewahrung. So kann statt einem einfachen, abschließbaren Schrank je nach Risiko auch die Aufbewahrung in einem Stahlschrank oder einem besonders gesicherten Raum notwendig sein.

Sehr oft mussten Einrichtungen melden, dass bei einem Einbruchdiebstahl nicht nur PCs und Kameras gestohlen, sondern auch Aktenschränke geöffnet und Akten augenscheinlich eingesehen wurden. Je nach Art der dort verzeichneten Daten kann alleine die Einsicht in die Daten schon meldepflichtig sein.

Bei der Weitergabe beziehungsweise dem Transport

Auch bei der Weitergabe beziehungsweise dem Transport der personenbezogenen Daten sind diese Daten entsprechend ihrer Sensibilität und dem gewählten Transportweg zu schützen.

Die Meldung einer Datenschutzverletzung an das Katholische Datenschutzzentrum, bei der Gesundheitsakten beim Transport auf einem Fahrrad-Gepäckträger verloren wurden, zeigt auch hier noch den Bedarf an Aufklärung und der Einführung weiterer Schutzmaßnahmen.

Bei der Vernichtung

Die Vernichtung von Papierdokumenten ist der Prozessschritt beim Umgang mit Papierakten, bei dem im Berichtszeitraum die meisten Datenschutzverletzungen in diesem Bereich gemeldet wurden. Die Meldungen betrafen meist auch mehrere Betroffene, da Papierakten oft in größeren Mengen gemeinsam entsorgt werden.

So wurde ein Fall gemeldet, in dem „Datenmüll" im normalen Hausmüll entsorgt wurde, was letztlich nur dem Entsorger zufällig auffiel. In einem anderen Fall waren die mit sensiblen Daten bedruckten Papiermengen anscheinend so groß, dass sie nicht in die Entsorgungsbehälter passten und deshalb einfach neben den Altpapiercontainer gestellt wurden. In einem weiteren Fall fanden sich Daten auf Papier in einem offenen Sperrmüllcontainer.

In all diesen Fällen haben es die Verantwortlichen unterlassen, die sachgemäße Vernichtung der Papiere zu organisieren beziehungsweise zu beauftragen und damit nicht die notwendigen technischen und organisatorischen Schutzmaßnahmen ergriffen.

Bei der Entsorgung von „Datenmüll" gibt die DIN 66399 hilfreiche Vorgaben zu allen Arten von Datenträgern (z. B. Papier, Festplatten oder CD/DVD) und für verschiedene Schutzklassen der Daten.

3.7.7 Verlust beziehungsweise Diebstahl von elektronischen Geräten mit darauf gespeicherten Daten

Die Meldung einer Datenschutzverletzung durch Verlust oder Diebstahl eines elektronischen Gerätes, auf dem die personenbezogenen Daten gespeichert sind, war auch in diesem Berichtszeitraum einer der häufigsten Meldegründe.

Die Schwelle zur Meldepflicht ist überschritten, wenn auf dem elektronischen Gerät personenbezogene Daten gespeichert sind, die nunmehr unbefugten Dritten gegenüber zugänglich sind und die Verletzung des datenschutzrechtlichen Schutzziels Vertraulichkeit eine Gefährdung für die Rechte und die Freiheiten der betroffenen Personen darstellt.

Im Zuge der Bearbeitung dieser Meldungen musste festgestellt werden, dass die zur Sicherung des Schutzziels Vertraulichkeit notwendigen technischen und organisatorischen Maßnahmen nicht im ausrei-

chenden Maß vorhanden waren. Auffällig war, dass selbst einfache technische Maßnahmen zur Sicherung der Daten in vielen Fällen nicht ergriffen waren. Bereits bei personenbezogenen Daten ab der Schutzklasse II sollten die Daten gemäß § 12 Abs. 2 lit. d) KDG-DVO auf zentralen Systemen gespeichert werden. Eine dezentrale Speicherung ist nach dieser Vorgabe nur mit einem ausreichenden Zugriffsschutz möglich. Besonders schwerwiegend ist das Fehlen von Sicherungsmaßnahmen, wenn Daten der Schutzklasse III betroffen sind. Hier schreibt § 13 Absatz 2 lit. a) KDG-DVO ausdrücklich vor, dass diese Daten auf mobilen Geräten nur verschlüsselt gespeichert werden dürfen.

„Bei den gemeldeten Datenschutzverletzungen fällt auf, dass die Vorgaben der KDG-DVO nicht immer bei der Auswahl der erforderlichen Maßnahmen berücksichtigt werden."

Bei den gemeldeten Datenschutzverletzungen fällt auf, dass die Vorgaben der KDG-DVO nicht immer bei der Auswahl der erforderlichen Maßnahmen berücksichtigt werden. Die Tragweite der gesetzlichen Verpflichtung, die aus den Regelungen der KDG-DVO resultieren, werden entweder nicht erkannt oder die Regelungen werden fälschlicherweise nur als unverbindliche Handlungsempfehlungen gewertet.

3.8 Beratung und Anfragen

Die Zahl der an das Katholische Datenschutzzentrum gerichteten Anfragen und Beratungswünsche war im Berichtszeitraum weiterhin auf einem sehr hohen Niveau. Thematisch spiegelten sich in den Anfragen und Beratungen (ohne kurze telefonische Auskünfte) im Berichtszeitraum die Themenschwerpunkte wieder, die das Jahr 2020 thematisch beherrscht haben: Corona, das Schrems II-Urteil des EuGH, die Ausübung von Betroffenenrechten und viele kleinere Schwerpunkte.

3.8.1 Stichwort: Beratung durch das Katholische Datenschutzzentrum

Gemäß § 44 Abs. 3 lit. b) KDG hat eine Datenschutzaufsicht im Rahmen ihres Zuständigkeitsbereichs insbesondere auch die Aufgabe, kirchliche Einrichtungen und Gremien über Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung derer Daten zu beraten. Die Beratung von Verantwortlichen, betrieblichen Datenschutzbeauftragten und Privatpersonen stellt einen wichtigen Schwerpunt der Arbeit des Katholischen Datenschutzzentrums dar.

Anfragen können auf verschiedenen Wegen an das KDSZ herangetragen werden. Neben der telefonischen Kontaktaufnahme können Fragestellungen oder Fallgestaltungen per E-Mail oder über das geschützte Kontaktformular gesendet werden.

Bei der Einzelfallberatung kann allerdings nur auf allgemeine Fragestellungen aus Sicht der Datenschutzaufsicht eingegangen werden. Konkrete Rechts- oder Vertragsberatungen, die eine rechtliche Bewertung eines Einzelfalles zum Gegenstand haben, sind außerhalb der gesetzlich definierten Ausnahmefälle nicht Teil der Aufgabe des Katholischen Datenschutzzentrums.

3.8.2 Thematische Schwerpunkte in der Beratung

Auch bei den Beratungen und Anfragen lag im Berichtszeitraum ein Schwerpunkt bei allen Fragen rund um die Corona-Pandemie.

Wie schon in Abschnitt 3.1 dieses Jahresberichts ausführlich dargestellt, gab es bei der datenschutzrechtlichen Beratung zum Umgang mit der Corona-Pandemie einige Fragen, die immer wieder an das Katholische Datenschutzzentrum gerichtet wurden.

Während des ersten Lockdowns und des damit verbundenen Verbots der Durchführung von Gottesdiensten mit Besuchern erreichten das KDSZ viele Anfragen rund um die Voraussetzung für die Übertragung von Gottesdiensten im Internet. Mit der an vielen Stellen für die Mitarbeitenden kurzfristig geschaffenen Möglichkeit von Zuhause aus zu arbeiten, kamen datenschutzrechtliche Fragen rund um das mobile Arbeiten und den damit notwendigen technischen Schutzmaßnahmen für die Daten und im Speziellen zur Nutzung von Videokonferenztools.

Mit der im weiteren Verlauf der Pandemie wieder eröffneten Möglichkeit zur Feier von Gottesdiensten mit Besuchern hatte das Katholische Datenschutzzentrum Anfragen rund um die datenschutzkonforme Gestaltung der jetzt notwendigen Besucherlisten im Rahmen der gesetzlich vorgeschriebenen Kontaktnachverfolgung zu beantworten. Da die Kontaktnachverfolgung nicht nur für die Gottesdienste vorgeschrieben ist, betrafen die Fragestellungen zur Gestaltung und zum Umgang mit Besucherlisten ebenso Tagungshäuser, Treffen kirchlicher Gruppen und alle kirchlichen Aktivitäten, bei denen mehrere Personen zusammenkamen und damit die im Gesetz geforderte Kontaktnachverfolgung notwendig wurde.

Im Bereich des Beschäftigtendatenschutzes hatte das KDSZ – wie oben beschrieben – vor allem Anfragen rund um die Erhebung von Gesundheitsdaten durch die Dienstgeber zu beantworten.

Neben Anfragen zu den anderen dargestellten Schwerpunktthemen erhielt das Katholische Datenschutzzentrum Anfragen aus allen Einrichtungstypen und zu nahezu allen Themen der Verarbeitung personenbezogener Daten im kirchlichen Bereich. Bei diesen Anfragen sind auch viele Themenbereiche enthalten, die in diesem Bericht in anderem Zusammenhang, z. B. bei Beschwerden oder der Meldung von Datenschutzverletzungen, schon dargestellt worden sind.

3.9 Neue Vorgaben des BSI zum Wechsel von Passwörtern

Mit dem jährlichen Update des IT-Grundschutz-Kompendiums des BSI zum 01.02.2020 (Edition 2020) änderte das BSI seine Vorgaben zum Wechsel von Passwörtern.

Während das BSI bisher die Vorgabe im IT-Grundschutz herausgegeben hatte, ein regelmäßiger Wechsel von Passwörtern sei das beste Mittel, um unberechtigten Datenzugriff - etwa mit Hilfe ausgespähter Passwörter - zu verhindern, vertritt das BSI in der aktuellen Ausgabe des Kompendiums (Baustein ORP.4: Identitäts- und Berechtigungsmanagement) nun die Auffassung, dass eine rein zeitgesteuerte Aufforderung zum Wechsel des Passworts vermieden werden sollte. Dahinter steht die Erkenntnis, dass ein zu häufiger Zwang zum Ändern des Passworts beim Anwender häufig zu ausweichendem Verhalten führt, bei dem z. B. nur eine Monatszahl an das Stamm-Passwort angehängt wird.

Wird auf den regelmäßigen Wechsel des Passworts verzichtet, soll die Passwortsicherheit durch andere Schutzmaßnahmen sichergestellt werden. Der IT-Grundschutz fordert jetzt statt der rein zeitgesteuerten Änderung des Passworts vom Verantwortlichen eine differenzierte Vorgehensweise bei der Einrichtung und Pflege von Zugriffskontrollen.

Der Verantwortliche hat daher …

- … zu prüfen, ob die alleinige Verwendung eines Passworts den Schutzbedarf hinreichend erfüllt oder evtl. eine Mehrfaktor-Authentifizierung eingeführt werden sollte.
- … Vorgaben von Mindestqualitäten für Passwörter (Länge, Komplexität) zu machen.
- … regelmäßig zu prüfen, ob Passwörter kompromittiert sein könnten (z. B. über Online-Dienste, die regelmäßig die veröffentlichten Passwort-Leaks zur Überprüfung für jedermann bereitstellen).
- … ein konsequentes Benutzermanagement einzurichten, bei dem auch vorübergehend ausgeschiedene Nutzer zeitnah in den Systemen deaktiviert werden.

Sofern die genannten Vorkehrungen nicht umgesetzt werden können, sollen doch zeitgesteuerte Wechsel von Passwörtern geprüft werden.

Soweit die Einrichtung den IT-Grundschutz umsetzt oder sich bei der Umsetzung der IT-Sicherheit an dem IT-Grundschutz orientiert, kann der betriebliche Datenschutzbeauftragte bei der Umsetzung der Vorgaben des IT-Grundschutzes in den Eirichtungen unterstützen.

3.10 Überarbeitung der Meldeprozesse für betriebliche Datenschutzbeauftragte und Datenschutzverletzungen

Seit Inkrafttreten des KDG im Mai 2018 stellt das Katholische Datenschutzzentrum den Einrichtungen eine Online-Plattform zur Verfügung, auf der die vorgeschriebenen Meldungen der Benennung eines betrieblichen Datenschutzbeauftragten nach § 36 Abs. 4 KDG beziehungsweise einer Datenschutzverletzung nach § 33 Abs. 1 KDG in einfacher und intuitiver Weise vorgenommen werden können.

Die bereits mehrere tausend Male verwendeten Online-Formulare, die gemeinsam mit den anderen deutschen katholischen Datenschutzaufsichten betrieben werden, wurden nutzerfreundlich angelegt.

Um missbräuchliche Meldungen im Namen anderer Personen zu vermeiden, wird in dem Meldeprozess die Authentizität des Absenders/Erfassers verifiziert. Dazu hat das Katholische Datenschutzzentrum einen Prozessablauf vorgesehen, in dem der Erfasser eine Bestätigungs-E-Mail mit einem Link erhält, den er innerhalb einer gewissen Zeitspanne bestätigen muss. Erst dadurch werden die gemeldeten Daten für eine Bearbeitung durch das KDSZ beziehungsweise die anderen angeschlossenen kirchlichen Datenschutzaufsichten freigeschaltet.

Leider kam es in der Vergangenheit in mehreren Fällen dazu, dass der Link in der Bestätigungs-E-Mail bereits vor Auslieferung an den Erfasser durch IT-Systeme auf der Empfängerseite getestet und damit aktiviert wurde. Damit war die Meldung bestätigt, ohne dass der Meldende die Bestätigung bewusst ausgelöst hatte. Wurde die Bestätigungs-E-Mail dann anschließend zugestellt, verursachte das Klicken des Links eine Fehlermeldung, da die Bestätigung längst im Hintergrund erfolgt war. In anderen Fällen wurde die E-Mail nur mit sehr großer Verzögerung ausgeliefert, weil IT-Systeme auf der Empfängerseite den Inhalt (den Link) als potentiell gefährlich bewerteten. Der Zeitraum, innerhalb dessen die Bestätigung erfolgen musste, war in diesen Fällen zum Zeitpunkt der späteren Zustellung manchmal bereits abgelaufen.

Im Dezember 2020 wurden die technischen Verfahren zur Meldung von betrieblichen Datenschutzbeauftragten und von Datenschutzverletzungen deshalb durch einen zusätzlichen Schritt abgesichert und transparenter gestaltet. Nachdem die meldende Person die Daten vollständig eingegeben und abgesendet hat, erhält sie wie bisher einen Link zur Bestätigung per E-Mail.

Wird der Link angeklickt, öffnet sich eine neue Seite, auf der alle eingegebenen Daten angezeigt werden. Am Fuß der Seite muss die meldende Person dann über eine Bestätigungs-Schaltfläche die Daten nochmal ausdrücklich freigeben.

Nach der Bestätigung werden die Daten ein weiteres Mal angezeigt und die meldende Person hat die Möglichkeit, über eine andere Schaltfläche zu drucken.

Mit dieser Änderung wird sowohl eine bewusste Bestätigung durch die meldende Person erreicht als ihr auch die Möglichkeit gegeben, die Daten einschließlich der Bearbeitungsnummer für die eigenen Unterlagen auszudrucken.

Mit diesen technischen Anpassungen des Meldeprozesses konnten die vereinzelt bestehenden Schwierigkeiten bei Meldungen über die Meldeplattform beseitigt werden.

3.11 Hinweis auf Änderungsbedarf im Impressum von Internetseiten

Der am 07.11.2020 in Kraft getretene Medienstaatsvertrag (MStV) ersetzt den bisher angewendeten Rundfunkstaatsvertrag (RStV) und regelt u. a. Rechte und Pflichten der Medienanbieter in Deutschland neu.

Die Internetseiten kirchlicher Einrichtungen und Stellen, die redaktionell-journalistische Inhalte anbieten, müssen – wie bisher auch schon – im Impressum einen inhaltlich Verantwortlichen benennen. Die alte Regelung „Verantwortlicher im Sinne des § 55 Abs. 2 RStV" ist nun aufgrund der neuen Gesetzeslage durch die Angabe „Verantwortlicher gemäß § 18 Abs. 2 MStV" zu ersetzen.

Diese Pflicht gilt auch für Blogs oder Social-Media-Accounts, soweit über diese auch redaktionell-journalistische Inhalte bereitgestellt werden. Auch der eigene Internetauftritt des Katholischen Datenschutzzentrums wurde an die neue Gesetzeslage angepasst.

3.12 Nutzung privater IT zu dienstlichen Zwecken (insbesondere im Schulbereich)

Die Nutzung privater IT-Systeme zu dienstlichen Zwecken ist aus datenschutzrechtlicher Sicht nicht unproblematisch. In diesen Fällen werden dienstliche personenbezogene Daten auf den privaten Systemen verarbeitet. Da die kirchliche Einrichtung als Verantwortlicher im datenschutzrechtlichen Sinne auch in diesen Fällen für eine gesetzeskonforme Verarbeitung der Daten verantwortlich ist, muss sie z. B. sicherstellen, dass nach der Verarbeitung keine Reste von dienstlichen Daten auf dem privaten System zurückbleiben oder während und nach der Verarbeitung kein unberechtigter Zugriff auf die Daten stattfinden kann.

Um den notwendigen Schutz der Daten auch auf den privaten Geräten sicherstellen zu können, muss die kirchliche Einrichtung die für ihre dienstlichen Geräte geltenden technischen und organisatorischen Schutzmaßnahmen auch auf die privaten Geräte übertragen können. Dies wird in der Regel aber einen administrativen Zugriff auf die privaten Geräte erfordern und kann z. B. bei mobilen Geräten wie Smartphones bis hin zur Einrichtung der Möglichkeit einer Fernlöschung der Daten auf dem Smartphone gehen, damit im Falle des Verlustes des

Smartphones die dienstlichen personenbezogenen Daten datenschutzgerecht gelöscht werden können.

Da die Vereinbarung und Umsetzung notwendiger technischer und organisatorischer Schutzmaßnahmen für private Endgeräte vor diesem Hintergrund nicht unproblematisch sind, hat sich der Gesetzgeber dazu entschieden, in § 20 Abs. 1 KDG-DVO die Nutzung privater IT-Systeme zu dienstlichen Zwecken grundsätzlich zu verbieten. Nur in Ausnahmefällen und unter den in § 20 KDG-DVO genannten Voraussetzungen darf ein privates IT System überhaupt zu dienstlichen Zwecken genutzt werden.

Diese allgemeine Regelung für alle kirchlichen Einrichtungen wird im Schulbereich durch eine Spezialregelung ergänzt. Der Einsatz digitaler Endgeräte, also z. B. Laptop oder Smartphone durch Lehrkräfte an kirchlichen Schulen wird in den nordrhein-westfälischen (Erz-)Diözesen durch die „Anordnung über den Kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Trägerschaft" (KDO-Schulen) geregelt. Die KDO-Schulen orientiert sich dabei wesentlich an den „Verordnungen über die zur Verarbeitung zugelassener Daten von Schülerinnen, Schülern und Eltern" (VO-DV I) beziehungsweise „der Lehrerinnen und Lehrer" (VO-DV II) des Landes NRW. Sowohl die weltlichen Verordnungen als auch die kirchliche Anordnung setzen als Regel den Einsatz dienstlicher Endgeräte voraus, da nur so eine umfassend sichere Datenverarbeitung eingerichtet werden kann.

Jeder Einsatz privater IT-Systeme bedarf als Ausnahme einer schriftlichen Genehmigung durch die Schulleitung, die neben der Erforderlichkeit zur Erfüllung schulischer Aufgaben auch die Einhaltung eines Mindeststandards an technischer Absicherung prüfen muss. Die Landesregierung NRW hat dazu ein Formular herausgegeben, in welchem der Antragsteller (Lehrerin/Lehrer) die Notwendigkeit begründet und technische Schutzmaßnahmen dokumentiert. Erst nach Prüfung aller Voraussetzungen erteilt die Schulleitung über dieses Formular die Genehmigung, das private Endgerät einzusetzen. Nach Auffassung des Katholischen Datenschutzzentrums kann dieses Formular eine gute Vorlage auch für die bischöflichen Schulverwaltungen sein.

Im Rahmen seiner Tätigkeit hat das KDSZ feststellen müssen, dass die gelebte Praxis noch nicht den oben geschilderten Vorgaben entspricht. Immer wieder trifft die Datenschutzaufsicht auf Situationen, in denen Lehrkräfte kirchlicher Schulen – unabhängig von den aktuellen Pandemie-Bedingungen – mit eigener IT-Ausstattung arbeiten (müssen).

Nach entsprechenden Hinweisen des Katholischen Datenschutzzentrums haben die fünf nordrhein-westfälischen (Erz-)Diözesen mittlerweile jeweils für ihren Bereich Lösungsansätze gefunden. Das KDSZ begrüßt die konsequente Umsetzung der gesetzlichen Vorgaben in diesem Bereich. Als Teil der Ausstattung mit dienstlichen Geräten sollten die (Erz-)Diözesen dann aber auch die IT-fachliche Betreuung der Personen organisieren.

Das Katholische Datenschutzzentrum wird die weiteren Entwicklungen zu diesem Thema datenschutzrechtlich begleiten.

3.13 Einsatz von Faxen zur Übermittlung personenbezogener Daten

Auch wenn das Faxgerät technisch gesehen schon eine „alte" Technologie ist, erfreut sich das Fax auch in einigen kirchlichen Einrichtungen, z. B. in Krankenhäusern, immer noch großer Beliebtheit.

Neben den allgemeinen Voraussetzungen und Vorkehrungen, die Verantwortliche bei jeder Form der Verarbeitung gemäß KDG und evtl. anderen speziellen Regelungen beachten müssen, hält die KDG-DVO in § 24 KDG-DVO noch eine spezielle Regelung für die Nutzung von Faxen zur Übermittlung personenbezogener Daten bereit.[49] Auf die Geltung der allgemeinen Regelungen weist § 24 Satz 1 KDG-DVO auch nochmals ausdrücklich hin, bevor spezielle, ergänzende Vorgaben für die Nutzung von Faxen aufgeführt werden. Insbesondere bei der Versendung von personenbezogenen Daten der Schutzklassen II und III sind gemäß § 24 Satz 1 Nr. 4 KDG-DVO noch zusätzliche Sicherheitsvorkehrungen einzurichten.

Welche technischen und organisatorischen Schutzmaßnahmen im Einzelfall notwendig und angemessen sind, ist unter Berücksichtigung des Risikos für die personenbezogenen Daten durch die Verarbeitung und die möglichen Folgen für den Betroffenen im konkreten Nutzungsszenario abzuwägen.

In einem Beschluss[50] vom 22.07.2020 hat sich das OVG Lüneburg mit der Frage der Rechtswidrigkeit der Versendung personenbezogener Daten per Telefax durch eine Behörde beschäftigt. In seiner Entscheidung kommt der Senat zu dem Ergebnis, dass eine Behörde bei der Übermittlung von personenbezogenen Daten per Fax zur Gewährleistung des Grundrechts auf informationelle Selbstbestimmung des Betroffenen Sicherungsvorkehrungen treffen muss. Nach Auffassung des Gerichts richtet sich das dabei einzuhaltende Schutzniveau nach der Sensibilität und Bedeutung der zu übermittelnden Daten sowie den potentiellen Gefahren bei der Faxübermittlung, dem Grad der Schutzbedürftigkeit des Betroffenen und dem mit den Sicherungsmaßnahmen verbundenen Aufwand.

Der Beschluss des Senats ist auch für kirchliche Einrichtungen von Bedeutung, da er grundsätzliche Ausführungen zum Umgang mit der Übermittlung personenbezogener Daten per Fax enthält. Diese treffen allgemeingültige Aussagen und sind daher auch bei dem Einsatz von Faxen durch kirchliche Stellen zu berücksichtigen.

Dem Beschluss liegt ein Sachverhalt zugrunde, bei dem eine Behörde – trotz eigener Erklärung, auf elektronischem Wege keine unverschlüsselte Übertragung der personenbezogenen Daten des Klägers vorzunehmen – in einem Gerichtsverfahren ihrem eigenen Prozessbevollmächtigten per Fax einen Bescheid (gerichtet an den Kläger) schickte. Dieser Bescheid enthielt unter anderem den Namen und die Anschrift des Klägers, sowie eine Fahrzeugidentifikationsnummer und das amtliche Kennzeichen dieses Fahrzeugs.

[49] Siehe hierzu auch die Kommentierung von Pau in Sydow, Kirchliches Datenschutzrecht, 1. Aufl. 2021 zu § 24 KDG-DVO.
[50] OVG Lüneburg, Beschluss vom 22.07.2020, Az. 11 LA 104/19.

Nachdem der Kläger dieses Vorgehen erfolglos bei der Behörde moniert hatte, fand er beim Verwaltungsgericht Osnabrück Unterstützung für seine Ansicht. Das Gericht stellte fest, dass die unverschlüsselte Übermittlung des Bescheides per Fax von der Behörde an ihren Prozessbevollmächtigten rechtswidrig war. Das VG Osnabrück hat dabei festgestellt, dass die Behörde wiederholt Schreiben mit personenbezogenen Daten des Klägers unverschlüsselt weitergegeben hat. Es hat weiter ausgeführt, dass die Behörde mit der Übermittlung eines unverschlüsselten Faxes das datenschutzrechtlich erforderliche Schutzniveau für den besonderen Gefahren ausgesetzten Kläger nicht gewahrt habe. Dieses Schutzniveau werde durch das zum Zeitpunkt der Übermittlung des Faxes anwendbare Niedersächsische Datenschutzgesetz näher vorgegeben. Auch wenn nach den Darstellungen des Verwaltungsgerichts das Gesetz kein Recht auf eine Implementierung bestimmter Schutzvorkehrungen vorsehe, müsse aber dennoch ein angemessenes Schutzniveau erreicht werden. Aufgrund der Besonderheiten der Tätigkeit des Klägers sei dieser im Falle seiner Identifizierung erheblichen Gefahren ausgesetzt. Daher müsse in besonderem Maße auf den Schutz seiner personenbezogenen Daten geachtet werden. Das VG Osnabrück kommt zu dem Ergebnis, dass in Anbetracht der mit einer unverschlüsselten Faxübertragung verbundenen abstrakten Risiken die Behörde entsprechend dem Stand der Technik das Fax nicht ohne Verschlüsselung hätte übermitteln dürfen. Das Gericht hat weiter ausgeführt, dass der Übermittlungsvorgang selbst noch zahlreiche andere Risiken berge, und festgestellt, dass deshalb auf eine Übersendung per Fax im konkreten Fall hätte verzichtet werden müssen. Das OVG Lüneburg hat sich auf die Beschwerde der Behörde der Ansicht des Verwaltungsgerichts und damit des Klägers angeschlossen.

Das OVG Lüneburg hat unter Bezug auf das Grundrecht auf informationelle Selbstbestimmung und das Niedersächsische Datenschutzgesetz ausgeführt, dass öffentliche Stellen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen haben, um eine den Vorschriften der datenschutzrechtlichen Regelungen entsprechende Verarbeitung personenbezogener Daten sicherzustellen. Dabei muss der Aufwand für diese Maßnahmen in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen und den Stand der Technik berücksichtigen. Das zum Zeitpunkt der Faxübermittlung geltende Datenschutzrecht sah vor, dass Maßnahmen zu treffen sind, die je nach Art der Daten und ihrer Verwendung geeignet sind zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Weiterhin war nach den Ausführungen des Gerichts die innerbehördliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Verwiesen hat das Gericht in diesem Zusammenhang auf Ausführungen des Landesbeauftragten für Datenschutz Niedersachsen, wonach eine Abwägung zwischen der Sensibilität und Bedeutung der Daten, den potentiellen Gefahren, dem Grad der Schutzbedürftigkeit und dem mit den Sicherungsmaßnahmen verbundenen Aufwand vorzunehmen ist.

Das OVG Lüneburg stellt in seinem Beschluss fest, dass gemessen an diesen Vorgaben die Behörde mit der nicht verschlüsselten Übermittlung des nicht anonymisierten Bescheides über ein Faxgerät an ihren Prozessbevollmächtigten nicht den gebotenen Schutz gewährleistet und dadurch den Kläger in seinem Grundrecht verletzt hat.

In seinem Beschluss betont das OVG Lüneburg die in der konkreten Situation bestehende besondere Schutzbedürftigkeit des Klägers. Es stimmt mit dem VG Osnabrück überein, dass der Kläger besonderen Risiken ausgesetzt ist. Daraus zieht das OVG Lüneburg die Schlussfolgerung, dass die Behörde bei der Übermittlung ein angemessenes Schutzniveau gewährleisten muss. Es hat dabei auch berücksichtigt, dass der Kläger bereits früher einer unverschlüsselten Übermittlung von personenbezogenen Daten widersprochen hatte. Auch hält das Gericht der Behörde die eigene Erklärung gegenüber dem Kläger vor, dass sie sich an die geltenden datenschutzrechtlichen Vorgaben halte und personenbezogene Daten nicht auf nicht verschlüsselten elektronischen Wegen übermitteln würde. Aus der Gesamtsituation folgt für das OVG Lüneburg, dass ein erhöhtes Schutzniveau im konkreten Fall einzuhalten war. Mit der unverschlüsselten Faxübermittlung ist nach Auffassung des Gerichts dieses Niveau unterschritten worden. Das OVG stimmt mit dem VG Osnabrück überein, dass bei einer Übermittlung per Fax kein Hindernis für die Wahrnehmung der Daten durch Unbefugte besteht und durch die offene Übertragung die Gefahr der Einsichtnahme in personenbezogene Daten durch unbefugte Dritte gegeben ist.

Das OVG Lüneburg kommt daher zu dem Ergebnis, dass aufgrund der Gefahren für den Kläger im konkreten Fall die Behörde den Risiken durch Sicherungsmaßnahmen bei der Übermittlung ihres Bescheides hätte begegnen müssen. Es zeigt als Alternativen für einen geeigneten Übertragungsweg den Postversand oder die Übermittlung per Boten auf. Die Benutzung von Telefaxgeräten sollte auf Ausnahmefälle beschränkt sein. Bei ihrem Einsatz sollten zur Verfügung stehende Sicherungen genutzt werden, etwa Verschlüsselungsgeräte. In seinem Beschluss betont das Gericht die Erforderlichkeit der Verwendung von Sicherungsmaßnahmen, wenn diese verfügbar sind und dem Stand der Technik entsprechen.

Die Rahmenbedingungen und Probleme bei der Faxübermittlung sind im außerkirchlichen wie im kirchlichen Bereich gleichartig. Kirchliche Stellen können sich daher bezüglich der Verwendung von Faxen an den Aussagen des OVG Lüneburg orientieren. Insbesondere sind die festgestellten Gefahrsituationen nicht von der Hand zu weisen. Die ungesicherte Übermittlung per Fax ist dem Risiko unbefugter Zugriffe ausgesetzt. Insofern ist die Situation mit der oft in diesem Zusammenhang zitierten Versendung einer Postkarte vergleichbar. Verantwortliche sollten sich der Risiken bewusst sein und ihre Übermittlungsoptionen entsprechend anpassen. Insbesondere bei sensiblen Daten und erhöhten Risiken sollten nur die möglichst sicheren Transportwege genutzt werden. Wenn die Nutzung von Faxen unvermeidbar sein sollte, müssen die erforderlichen Sicherungsmaßnahmen eingesetzt werden.

Dies ergibt sich auch schon aus den Regelungen des § 24 KDG-DVO. Die Einhaltung der allgemeinen Schutzmaßnahmen gemäß der §§ 5 ff. KDG-DVO, verbunden mit dem Hinweis in § 24 Satz 1 Nr. 4 KDG-DVO auf notwendige besondere Schutzmaßnahmen bei der Verarbeitung von Daten der Schutzklassen II und III, machen vor dem zukünftigen Einsatz von Faxübertragungen eine Risikobetrachtung des Verantwortlichen notwendig, ob in der konkreten Risikosituation der betroffenen personenbezogenen Daten und der Situation des Empfängers als Betroffenem angemessene technisch-organisatorische Maßnahmen zum Schutz der

Daten getroffen worden sind. Sofern dies nicht mit Sicherheit festgestellt werden kann, müssen entsprechende Maßnahmen nachgezogen werden oder es muss auf andere, risikoärmere Übermittlungswege zurückgegriffen werden.

3.14 Nachweis der Masernimpfung - datenschutzrechtliche Fragestellungen im Zusammenhang mit der Nachweispflicht für Beschäftigte

Zum 01.03.2020 ist die vom Bundestag beschlossene Masernimpfpflicht in Kraft getreten.[51] Ziel dieser Verpflichtung soll die Gesundheitsfürsorge sein, da es sich bei der Maserninfektion nicht nur um eine Kinderkrankheit, sondern um eine der ansteckendsten Infektionskrankheiten mit teilweise schweren Folgen bis zum Tod handelt.

Da neben den Nutzern der betroffenen Einrichtungen (z. B. den Kindern in den Kindertagesstätten oder den Schulen) auch die Beschäftigten einen Nachweis zu erbringen haben, ist aus datenschutzrechtlicher Sicht zu beachten, wie der Arbeitgeber den Impfstatus der Beschäftigten als personenbezogenes Datum der besonderen Kategorie rechtmäßig verarbeitet und das Prinzip der Datenminimierung beachtet.

Impfnachweis als Gesundheitsdatum

Legt der Mitarbeitende zum Nachweis seines Impfstatus seinen Impfausweis oder eine besondere ärztliche Bestätigung vor, verarbeitet der Arbeitgeber ein personenbezogenes Datum der besonderen Kategorie gemäß § 4 Nr. 2 KDG. Es handelt sich um die Verarbeitung von Gesundheitsdaten (vgl. § 4 Nr. 17 KDG).

Das Gesetz sieht vor, dass Beschäftigte in Gemeinschaftseinrichtungen oder medizinischen Einrichtungen ihren Impfschutz (oder ihre Immunität) gegenüber der Leitung nachzuweisen haben. Zu diesen Einrichtungen gehören vor allem Betreuungseinrichtungen für Minderjährige (wie z. B. Kindertageseinrichtungen oder Schulen). Wird eine Weiterbeschäftigung oder Neubeschäftigung ohne Impfschutz von der Einrichtung gestattet, ist dies in Zukunft als Ordnungswidrigkeit zu werten und bußgeldbewehrt. Außerdem kann das zuständige Gesundheitsamt ein Verbot gegenüber der betreffenden Person aussprechen.

Die bereits am 01.03.2020 in den genannten Einrichtungen tätigen Personen haben den Impfnachweis bis zum 31.07.2021 zu erbringen.

Auch betreute Personen in diesen Gemeinschaftseinrichtungen werden vom dem Gesetzesentwurf erfasst. Teilweise kann die zuständige Behörde vor Aufnahme der Betreuung den entsprechenden Nachweis gegenüber dem Gesundheitsamt verlangen, so dass dieser nicht von der Leitung eingeholt werden muss. Zum Nachweis verpflichtet sind die Personenfürsorgeberechtigten beziehungsweise der gesetzliche Betreuer.

[51] Siehe das Gesetz für den Schutz vor Masern und zur Stärkung der Impfprävention (Masernschutzgesetz) vom 10.02.2020, (BGBl. I 2020, S. 148).

Rechtmäßigkeit der Verarbeitung (Erhebung des Impfstatus durch den Arbeitgeber)

Der neue § 20 Abs. 8 IfSG fordert einen Nachweis der Impfung oder der Immunität von den betreuten Personen und von den Beschäftigten (unter den dort genannten Bedingungen). Die Vorlage des Nachweises darf beziehungsweise muss von der nach dem IfSG verpflichteten Stelle vermerkt werden. Es muss aber keine Kopie angefertigt werden. Es ist ausreichend, wenn vermerkt wird, wer was wann und wie vorgelegt hat. Die Notwendigkeit zur Dokumentation ergibt sich auch aus § 20 Abs. 9 IfSG, der die Einrichtung verpflichtet, Personen, die keinen Nachweis erbracht haben, durch Übermittlung personenbezogener Daten zu melden. Um dies tun zu können, muss die Einrichtung aber vermerken (dürfen), wer die Verpflichtung durch Vorlage eines Nachweises erfüllt hat.

Ist die Verarbeitung durch das IfSG vorgegeben, so liegt eine Rechtsgrundlage nach § 6 Abs. 1 lit. a) KDG beziehungsweise § 6 Abs. 1 lit. d) KDG vor. Die Verarbeitung besonderer Kategorien personenbezogener Daten wäre dann nach § 11 Abs. 2 lit. b) KDG erlaubt. Da das IfSG ein Verbot des Einsatzes von Personen in den Einrichtungen vorsieht, die keinen Nachweis vorgelegt haben, könnte als Rechtsgrundlage auch noch § 53 KDG herangezogen werden. Für die Verarbeitung der besonderen Kategorien personenbezogener Daten wäre aber auch in diesem Fall § 11 Abs. 2 lit. b) KDG heranzuziehen.

Umgang mit der Information über den Impfstatus

Haben die Beschäftigten ihren Impfstatus gegenüber dem Dienstgeber nachgewiesen, stellt sich die Frage, wie dieser die Information dokumentiert. Nach dem Prinzip der Datenminimierung aus § 7 Abs. 1 lit. c) KDG dürfte die Anforderung des § 20 Abs. 9 IfSG zur Vorlage eines Nachweises so auszulegen sein, dass bei Vorlage der Bescheinigung ein Vermerk in den Unterlagen des Dienstgebers ausreichend ist, um der Verpflichtung aus dem IfSG nachzukommen. Anders als bei der Vorlagepflicht eines (erweiterten) Führungszeugnisses oder einer Führerscheinkopie bei Nutzung von Dienstfahrzeugen, kommt es bei dem Nachweis der Impfpflicht wohl nicht zu Streitigkeiten mit Beweispflicht. Besonders weil der Impfschutz nicht erneuert werden muss.

3.15 Orientierungshilfe der DSK zur E-Mail-Sicherheit

Im März 2020 beschäftigte sich die Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder erneut mit dem Thema E-Mail und verabschiedete die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“[52]. Mit dem Papier greifen die Datenschutzaufsichten viele auch für die kirchlichen Einrichtungen unter der Geltung des KDG relevante Aspekte auf.

[52] Das Papier ist abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf (nachträglich aktualisiert).

In der Orientierungshilfe wird z. B. auf die Problematik der Absicherung dienstlicher E-Mails hingewiesen, wenn diese nicht über dienstliche E-Mails-Postfächer geleitet werden, sondern über private Postfachanbieter. Die Nutzung der Adresse Kirchenvorstand@webmail-provider.com macht aus einer E-Mail mit dienstlichem Bezug und aus dienstlichen Gründen versendeten Daten keine privaten Daten. Hier hat die kirchliche Einrichtung als Verantwortlicher immer noch die Verantwortung für die Verarbeitung der Daten, auch wenn die E-Mail bei einem privaten Web-Mail-Anbieter liegt. Auch die Nutzung der personalisierten Adresse max.mustermann@webmail-provider als Mitglied z. B. des Kirchenvorstandes macht aus der dienstlichen E-Mail keine Privatsache. Hier bietet es sich dringend an, die von den (Erz-)Diözesen bereitgestellten dienstlichen E-Mail-Adressen zu nutzen.

Das Papier gibt außerdem Hinweise zur Nutzung von Verschlüsselung und Signaturen für E-Mails. Gerade die Verschlüsselung von E-Mails stellt eine wirksame Schutzmaßnahme für die mit der E-Mail versendeten Daten dar. Die Orientierungshilfe nennt hier verschiedene Wege und gibt Empfehlungen.

4 Das Katholische Datenschutzzentrum

4.1 Zuständigkeitsbereich

Der Diözesandatenschutzbeauftragte und Leiter des Katholischen Datenschutzzentrums ist als Datenschutzaufsicht im Sinne des Art. 91 Abs. 2 DSGVO und der §§ 42 ff. KDG zuständig für die Erzdiözese Köln, die Erzdiözese Paderborn, die Diözese Aachen, die Diözese Essen und die Diözese Münster (nordrhein-westfälischer Teil). Diese sind von der Fläche deckungsgleich mit dem Bundesland Nordrhein-Westfalen. Hinzu kommen noch einzelne Gemeinden oder Teile von Gemeinden in Rheinland-Pfalz, die zur Erzdiözese Köln gehören, und in Niedersachsen und Hessen, die zur Erzdiözese Paderborn gehören. In diesem Gebiet leben ca. 6,7 Millionen Menschen römisch-katholischen Glaubens (Stand 2019).

Neben den fünf (Erz-)Bischöflichen Generalvikariaten als den zentralen Verwaltungsbehörden der (Erz-)Diözesen werden die vielen Pfarreien vor Ort vom Katholischen Datenschutzzentrum betreut. Hinzu kommen fünf Caritasverbände auf Diözesanebene und 89 Orts- und Kreisverbände der Caritas mit ihren Beratungsangeboten und Beratungsstellen (Stand 2018)[53]. Daneben gibt es in den fünf (Erz-)Diözesen noch über 140 Schulen in kirchlicher Trägerschaft, über 2600 katholische Kindergärten, rund 200 katholische Krankenhäuser, über 1200 Altenpflegeeinrichtungen und rund 390 Einrichtungen der Jugendhilfe, für die der Diözesandatenschutzbeauftragte (DDSB) zuständig ist (Stand 2018)[54]. Darüber hinaus fallen noch diverse Vereine, Verbände und Stiftungen im kirchlichen Bereich sowie auch die Bundesverbände kirchlicher Vereinigungen, die ihren Sitz in Nordrhein-Westfalen haben, in die Zuständigkeit des DDSB.

Seit dem 01.01.2018 ist der Diözesandatenschutzbeauftragte zusätzlich als Datenschutzaufsicht für den Verband der Diözesen Deutschlands[55] zuständig. Der VDD ist Rechtsträger der Deutschen Bischofskonferenz. Er wurde 1968 als Körperschaft des öffentlichen Rechts gegründet. Im VDD sind die 27 rechtlich und wirtschaftlich selbstständigen (Erz-)Diözesen zusammengeschlossen. Neben dem Sekretariat der Deutschen Bischofskonferenz in Bonn gehören unter anderem die Geschäftsstelle des VDD in Bonn, das Kommissariat der deutschen Bischöfe – Katholisches Büro in Berlin und weitere Einrichtungen des VDD zum Zuständigkeitsbereich.

[53] https://www.caritas-nrw.de/magazin/2018/artikel/ein-starker-Teil-von-Kirche
[54] Daten aus der Zentralstatistik der Caritas Stand 31.12.2018.
[55] Die Datenschutzaufsicht heißt dort „Verbandsdatenschutzbeauftragter".

4.2 Aufbau der Einrichtung

Das Katholische Datenschutzzentrum ist eine eigenständige Körperschaft des öffentlichen Rechts, die von den Erzdiözesen Köln und Paderborn und den Diözesen Aachen, Essen und Münster gegründet wurde.

In den Verwaltungsrat des Katholischen Datenschutzzentrums haben die (Erz-)Bischöfe ihre jeweiligen Generalvikare entsandt. Der Vertreter der Erzdiözese Paderborn, Herr Generalvikar Hardt, wurde vom Verwaltungsrat zum Vorsitzenden des Gremiums gewählt, die Geschäftsführung wurde dem Leiter des Katholischen Datenschutzzentrums übertragen.

Die Leitung des Katholischen Datenschutzzentrums nimmt der gemeinsame Diözesandatenschutzbeauftragte der fünf Mitgliedsdiözesen wahr. Er vertritt die Körperschaft nach außen.

Dem DDSB sind eine Vertreterin/ein Vertreter, Referentinnen und Referenten, Sachbearbeiterinnen und Sachbearbeiter und eine Sekretärin zur Seite gestellt, die auch vom KDSZ selbst angestellt sind. Es sind im Berichtszeitraum elf Stellen vorgesehen, von denen zum Jahresende zehn besetzt sind.

Die Stelle der stellvertretenden Leitung war zum 31.12.2020 nicht besetzt. Die Funktion der stellvertretenden Diözesandatenschutzbeauftragten und der stellvertretenden Leitung des Katholischen Datenschutzzentrums wird seit 01.01.2021 kommissarisch durch eine Referentin wahrgenommen.

Durch die eigenständige Körperschaft des öffentlichen Rechts und das im eigenen Haus angestellte Personal wird die notwendige Unabhängigkeit des Diözesandatenschutzbeauftragten und seiner Mitarbeitenden gewährleistet.

	Soll	Ist
Diözesandatenschutzbeauftragter / Verbandsdatenschutzbeauftragter / Leiter KDSZ	1	1
Stellvertrentender Diözesandatenschutzbeauftragter / Stellvertretender Verbandsdatenschutzbeauftragter / Stellvertretender Leiter KDSZ	1	0
Referentinnen / Referenten	5	5
Sachbearbeiterinnen / Sachbearbeiter	3	3
Sekretariat	1	1
Gesamt	11	10

Abb.: Stellensoll des KDSZ und besetzte Stellen

Bei der Planung des Katholischen Datenschutzzentrums wurde konsequent auf die Umsetzung des Urteils des Europäischen Gerichtshofs vom 09.03.2010 zur Unabhängigkeit und Selbständigkeit der Datenschutzaufsichtsbehörden[56] geachtet. Auch die Veränderungen durch die Europäische Datenschutz-Grundverordnung beziehungsweise deren Umsetzung in kirchliches Recht wurden schon berücksichtigt.

Das KDSZ hat seinen Sitz in der Kommende Dortmund, dem Standort des Sozialinstituts der Erzdiözese Paderborn.

Nach der Übernahme der Aufgaben des Diözesandatenschutzbeauftragten der fünf (Erz-)Diözesen in NRW zum 01.09.2016 und der folgenden Aufbauphase des KDSZ war es im Jahr 2020 das Ziel, im Rahmen der schwierigen Rahmenbedingungen der Corona-Pandemie die gesetzlichen Aufgaben als Datenschutzaufsicht weiter erfolgreich umzusetzen.

Mit der Übernahme der Datenschutzaufsicht über den VDD und die angeschlossenen Einrichtungen wurde diese Aufgabe in die bestehenden Abläufe des Katholischen Datenschutzzentrums integriert und so die reibungslose Wahrnehmung der Datenschutzaufsicht auch für diese kirchlichen Stellen sichergestellt.

4.3 Der hl. Ivo – Schutzpatron des Katholischen Datenschutzzentrums

Mit der Gründung des Katholischen Datenschutzzentrums als der gemeinsamen Datenschutzaufsicht der fünf nordrhein-westfälischen (Erz-)Diözesen wurde dem KDSZ von den (Erz-)Diözesen auch ein Schutzpatron mitgegeben.

Der hl. Ivo lebte im 13. Jahrhundert in der Bretagne. Der Bischof von Tréguier ernannte den Priester, der auch Rechtswissenschaften studiert hatte, zu seinem Offizial. Dieses kirchliche Richteramt füllte er mit Mut und Unbestechlichkeit aus und setzte sich vor allem für Arme und Bedrängte vor weltlichen und kirchlichen Gerichten ein, was ihm den Ruf eines „Anwalts der Armen" einbrachte. Er wurde im 14. Jahrhundert heiliggesprochen. Sein Gedenktag ist der 19. Mai. Die Reliquien des heiligen Ivo werden in der Kathedrale von Tréguier aufbewahrt[57].

[56] Siehe hierzu auch Abschnitt 5.1.1 dieses Jahresberichts.

[57] Ausführlich zum Leben und Wirken des hl. Ivo: Michael Streck / Annette Rieck, St. Ivo (1247-1303) - Schutzpatron der Richter und Anwälte, 2007; Artikel „Ivo Hélory" auf Wikipedia (https://de.wikipedia.org/wiki/Ivo_Hélory). In dem Beitrag bei Wikipedia wird auch erwähnt, dass der hl. Ivo das Siegel des Katholischen Datenschutzzentrums ziert.

Das Bildnis des hl. Ivo ziert auch das Siegel des Katholischen Datenschutzzentrums, so dass der Schutzpatron auch in der täglichen Arbeit immer gegenwärtig ist.

Abb.: Darstellung des Siegels des KDSZ im Amtsblatt der Erzdiözese Paderborn

4.4 Aufgabenkatalog

Die Aufgaben des Diözesandatenschutzbeauftragten beziehungsweise des Verbandsdatenschutzbeauftragten des VDD als Datenschutzaufsicht sind im KDG beziehungsweise im KDG-VDD[58] beschrieben. Wer der Ansicht ist, dass bei der Verarbeitung von personenbezogenen Daten durch eine (katholische) kirchliche Stelle datenschutzrechtliche Regelungen verletzt worden sind, kann sich gemäß § 48 KDG an die Datenschutzaufsicht wenden. Diese prüft den Sachverhalt und hört dazu die betroffene kirchliche Stelle an, soweit ein Verstoß gegen datenschutzrechtliche Regelungen vorliegen könnte. Wichtig ist dabei das Benachteiligungsverbot des § 48 Abs. 3 KDG: „Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an die Datenschutzaufsicht gewendet hat."

Das Überwachen der Einhaltung datenschutzrechtlicher Vorgaben gehört nicht nur im Rahmen der Beschwerdebearbeitung, sondern als allgemeine Kernaufgabe zu den Tätigkeiten der Datenschutzaufsicht (vgl. § 44 Abs. 1 KDG).

§ 44 Abs. 3 lit. g) KDG ergänzt § 44 Abs.1 KDG. Danach soll die Datenschutzaufsicht „Untersuchungen über die Anwendung dieses Gesetzes durchführen, auch auf Grundlage von Informationen einer anderen Datenschutzaufsicht oder einer anderen Behörde."

Auf Basis dieser Regelung kann und muss die Datenschutzaufsicht Überprüfungen auf Grundlage der bei ihr eingehenden Beschwerden und Hinweise vornehmen. Sie kann aber auch ohne einen konkreten Bezug anlasslos prüfen, ob die Einrichtungen datenschutzrechtliche Vorgaben richtig anwenden[59].

[58] Im Folgenden wird nicht immer explizit auf die gleichlautende Vorschrift des KDG-VDD verwiesen.

[59] Siehe auch Hense in Sydow, Kirchliches Datenschutzrecht, 1. Aufl. 2021, KDG § 44 Rn. 26f.; zur Auslegung der inhaltsgleichen Vorschrift des Art. 57 Abs. 1 lit. h) DSGVO vgl. Selmayr in Ehmann/Selmayr, Kommentar DSGVO, 2. Aufl. 2018, Art. 57 Rn. 9 und Kugelmann/Buchmann in Schwartmann u. a., Heidelberger Kommentar DSGVO / BDSG, 2. Aufl. 2020, Art. 57 Rn. 74.

Für kirchliche Stellen im Sinne des § 3 Abs. 1 KDG macht § 44 Abs. 2 KDG nochmals deutlich, dass diese die Arbeit der Datenschutzaufsicht durch Auskünfte und das Ermöglichen von Einsichtnahme in Akten und Räume zu unterstützen und Untersuchungen und Prüfungen zuzulassen haben. Den Anweisungen der Datenschutzaufsicht ist nach § 44 Abs. 2 lit. a) KDG Folge zu leisten.

Hierzu führt die Datenschutzaufsicht anlassbezogen, aufgrund der bei ihr eingehenden Beschwerden oder Hinweise, oder ohne Anlass – im Rahmen regelmäßiger Kontrollen – Prüfungen zur Verbesserung des Datenschutzes durch. Hierbei spielt die Einhaltung der rechtlichen Vorgaben (Datenschutzrecht) ebenso eine Rolle wie die Umsetzung der notwendigen technischen und organisatorischen Schutzmaßnahmen gemäß den datenschutzrechtlichen Vorgaben (Datensicherheit). Beide Komponenten, die Umsetzung der rechtlichen Vorgaben und der technisch-organisatorischen Schutzmaßnahmen, müssen beachtet werden, damit Datenschutz wirksam werden kann und die betroffenen Personen den gesetzlich vorgesehenen Schutz genießen können.

Kommt die Datenschutzaufsicht im Rahmen einer Prüfung oder der Bearbeitung einer Beschwerde oder eines Hinweises zu dem Ergebnis, dass ein bestimmter von der kirchlichen Stelle durchgeführter oder unterlassener Vorgang bei der Verarbeitung personenbezogener Daten zu beanstanden ist, wird dies dokumentiert und dem Verantwortlichen schriftlich mitgeteilt. Je nach Schwere des Verstoßes gegen die datenschutzrechtlichen Vorgaben kann das Katholische Datenschutzzentrum verschiedene Maßnahmen ergreifen, die bis zu einer Untersagung der konkreten Datenverarbeitung und der Verhängung eines Bußgeldes reichen können.

Um datenschutzrechtlichen Verstößen vorzubeugen steht das Team des Katholischen Datenschutzzentrums im Rahmen seiner Aufgaben beratend zur Verfügung, um über die Anforderungen der datenschutzrechtlichen Regelungen zu informieren. Die Datenschutzaufsicht kann als Referent oder mit schriftlichen Informationen allgemeine Hinweise zur Umsetzung des Datenschutzes geben oder im Wege der Beratung im Einzelfall weiterhelfen.

„Um datenschutzrechtlichen Verstößen vorzubeugen steht das Team des Katholischen Datenschutzzentrums im Rahmen seiner Aufgaben beratend zur Verfügung …“

4.5 Finanzen

Das Katholische Datenschutzzentrum wird von den fünf (Erz-)Diözesen als Mitgliedern der Körperschaft des öffentlichen Rechts getragen. Wie in § 43 Abs. 4 KDG beschrieben stellen sie die für die Erfüllung der Aufgaben des Diözesandatenschutzbeauftragten angemessene Personal- und Sachausstattung zur Verfügung. Außerdem verfügt der DDSB über einen eigenen jährlichen Haushalt.

Für das Kalenderjahr 2020 hat der Verwaltungsrat des Katholischen Datenschutzzentrums auf Vorschlag des Diözesandatenschutzbeauftragten den Haushaltsplan in Höhe von 1.375.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben bewilligt. Für das Folgejahr 2021 wird sich das genehmigte Budget leicht auf 1.390.000 Euro erhöhen.

4.6 Mitarbeit in Gremien und Arbeitsgruppen

Das Katholische Datenschutzzentrum bringt seine Kenntnisse und Erfahrungen aus der Praxis der Datenschutzaufsichten auch in die Arbeit von kirchlichen Gremien und Arbeitsgruppen ein. Die Beratung der Gremien und Arbeitsgruppen ist Teil des gesetzlichen Auftrags der Datenschutzaufsichten.

Im Berichtszeitraum unterstützte das Katholische Datenschutzzentrum als Verbandsdatenschutzbeauftragter die Arbeit des Verbandes der Diözesen Deutschlands. So war der Verbandsdatenschutzbeauftragte zusammen mit einer Referentin aus dem KDSZ an der Erarbeitung des Verwaltungsverfahrensgesetzes für die Datenschutzaufsichten in der dafür eingerichteten Arbeitsgruppe der Unterkommission Datenschutz- und Melderecht/IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands beteiligt. Daneben wurde das Katholische Datenschutzzentrum als Datenschutzaufsicht für den Verband der Diözesen Deutschlands mehrfach um Einschätzungen und datenschutzrechtlichen Bewertungen zu Gesetzentwürfen oder Einzelfragen gebeten, die im Rahmen der kirchlichen Gesetzgebungsverfahren aufkamen. Dabei kann die Datenschutzaufsicht ihre Expertise als unabhängiger Berater einbringen.

Als zuständige Datenschutzaufsicht beraten der Verbandsdatenschutzbeauftragte und das Katholische Datenschutzzentrum den VDD und die angeschlossenen Einrichtungen darüber hinaus auch in datenschutzrechtlichen Fragen, die in der täglichen Arbeit aufkommen oder in Gremien beraten werden.

Bei der Weiterentwicklung der diözesanen Gesetze und der Diskussion von grundsätzlichen Rechtsfragen sind die Justitiare der fünf (Erz-)Diözesen und der Justitiar des Katholischen Büros NRW in Düsseldorf die ersten Ansprechpartner des Katholischen Datenschutzzentrums. Das KDSZ hält daher einen regelmäßigen Kontakt zu den Rechtsabteilungen der Generalvikariate und zum Katholischen Büro NRW.

In der ökumenischen Projektgruppe zur Umsetzung des Standard-Datenschutzmodells im kirchlichen Bereich ist das KDSZ mit dem Diözesandatenschutzbeauftragten, der die Projektgruppe seit deren Einrichtung 2019 zusammen mit dem Beauftragten für den Datenschutz der EKD leitet, und einem Referenten vertreten.[60]

Im Arbeitskreis Grundsatz der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder vertritt der Diözesandatenschutzbeauftragte die Konferenz der Katholischen Datenschutzaufsichten in Deutschland und nimmt als Gast an den Sitzungen des Arbeitskreises der DSK teil.

[60] Siehe Abschnitt 1.7 dieses Jahresberichts zur ökumenischen Projektgruppe.

4.7 Vernetzung

4.7.1 Vernetzung mit kirchlichen Stellen

Die fünf Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen stehen untereinander und mit den Gemeinsamen Ordensdatenschutzbeauftragten der Deutschen Ordensobernkonferenz in ständigem Austausch zu aktuellen Fragen und grundsätzlichen Themen. Die Besprechungen und Telefon- oder Videokonferenzen dienen diesem Austausch und der Vorbereitung und Verabschiedung gemeinsamer Positionen[61].

Der Beauftragte für den Datenschutz der EKD hat neben seinem Hauptsitz in Hannover noch vier Außenstellen. Die Außenstelle in Dortmund ist u. a. für die Landeskirchen und Diakonien in Nordrhein-Westfalen zuständig. Im Berichtszeitraum ist der regelmäßige Austausch sowohl mit dem Beauftragten für den Datenschutz der EKD selbst, als auch mit der Außenstelle Dortmund intensiv fortgesetzt worden.

Das Katholische Datenschutzzentrum unterstützt im Rahmen seiner zeitlichen Möglichkeiten Arbeitskreise betrieblicher Datenschutzbeauftragter kirchlicher Einrichtungen. Hierbei steht es für kurze Vorträge und allgemeinen Erfahrungsaustausch zur Verfügung. Von diesem Angebot wurde im Berichtszeitraum, bedingt durch die Corona-Pandemie, nur vereinzelt Gebrauch gemacht.

So hat das KDSZ z. B. mit den IT-Sicherheitsbeauftragten der (Erz-)Diözesen oder den IT-Verantwortlichen der Generalvikariate verschiedene Gesprächskreise aufgebaut, die dem regelmäßigen Austausch dienen und es ist regelmäßiger Gast bei den Treffen der betrieblichen Datenschutzbeauftragten der Generalvikariate.

Auch im Arbeitskreis Technik der Konferenz der Diözesandatenschutzbeauftragten arbeitet das KDSZ aktiv mit. Im Berichtszeitraum nahm der Vertreter des Katholischen Datenschutzzentrums auch die jährlich wechselnde Leitung des Arbeitskreises wahr.

4.7.2 Vernetzung mit staatlichen Stellen

Der Kontakt und der Austausch mit dem Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten als staatlichen Datenschutzaufsichtsbehörden ist nach § 46 KDG Bestandteil der Aufgaben des Diözesandatenschutzbeauftragten. Im Berichtszeitraum gab es vielfältige regelmäßige Kontakte in Grundsatzfragen und bei der Bearbeitung von konkreten Datenschutzproblemen.

Diese Kontakte zu den staatlichen Stellen helfen, vergleichbare Auslegungen der Gesetze bei vergleichbaren Vorgängen und damit ein vergleichbares Datenschutzniveau im kirchlichen Bereich bei Anwendung des KDG und im außerkirchlichen Bereich bei Anwendung der DSGVO sicherzustellen.

[61] Siehe Abschnitt 5.1.2 dieses Jahresberichts zur Konferenz der Diözesandatenschutzbeauftragten.

§ 18 Abs. 1 Satz 4 Bundesdatenschutzgesetz sieht eine Beteiligung der kirchlichen Datenschutzaufsichten bei Sachverhalten vor, die vom Europäischen Datenschutzausschuss beraten werden, wenn die kirchlichen Datenschutzaufsichten von dieser Frage betroffen sind. Auch nach dem Beschluss vom 13.05.2019 („Beschluss zur Beteiligung der spezifischen Aufsichtsbehörden gem. § 18 Abs. 1 Satz 4 BDSG an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der EU“)[62] der in der DSK zusammengeschlossenen unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder sind die Einzelheiten zur Anwendung dieser Vorschrift zwischen den staatlichen Datenschutzaufsichten und den Datenschutzaufsichten der Rundfunkanstalten und der Kirchen weiterhin in der Diskussion.

4.8 Öffentlichkeitsarbeit

Das kirchliche Datenschutzrecht stellt - ebenso wie die Datenschutz-Grundverordnung - die Bedeutung der Information der Öffentlichkeit, der kirchlichen Stellen und der Verantwortlichen für die Datenverarbeitungen über Rechte und Pflichten beim Umgang mit personenbezogenen Daten besonders heraus. Der Aufgabenkatalog der Datenschutzaufsichten in § 44 Abs. 3 KDG betont dieses Thema gleich mehrfach.[63]

Das Katholische Datenschutzzentrum macht daher auf vielfältige Weise auf seine Arbeit und den Datenschutz in der katholischen Kirche aufmerksam und informiert die kirchlichen Einrichtungen, die betroffenen Personen und die interessierte Öffentlichkeit darüber.

4.8.1 Internetauftritt

Über die Internetpräsenz **www.katholisches-datenschutzzentrum.de** stellt das Katholische Datenschutzzentrum vielfältige Informationen rund um den kirchlichen Datenschutz und die Arbeit der Datenschutzaufsicht zur Verfügung. Diese Informationen sind als Internetseiten online verfügbar oder stehen dort als Infoblätter und Broschüren zum Download bereit. Hierbei reicht das Spektrum von den einschlägigen Gesetzestexten für die jeweilige (Erz-)Diözese über Hilfestellungen bis hin zu Mustern und Vorlagen. Die angebotenen Informationen reichen von Erläuterungen zu Grundlagen des Datenschutzes über Hilfestellungen für Datenschutzfachleute bis hin zu aktuellen rechtlichen und technischen Entwicklungen und Neuigkeiten.

[62] Siehe Abschnitt 5.3.1 des Jahresberichts 2019.

[63] So sollen die Datenschutzaufsichten gemäß § 44 Abs. 3 lit. a) KDG die „Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären“, wobei „spezifische Maßnahmen für Minderjährige“ besondere Beachtung finden sollen. Weiterhin sollen die Datenschutzaufsichten „kirchliche Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten“ (§ 44 Abs. 3 lit. b) KDG), „die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz entstehenden Pflichten sensibilisieren“ (§ 44 Abs. 3 lit. c) KDG) und „auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes zur Verfügung stellen“ (§ 44 Abs. 3 lit. d) KDG).

Teil der Internetseite des Katholischen Datenschutzzentrums ist auch ein gesichertes Kontaktformular. Über diese Kontaktmöglichkeit will das KDSZ jedem Beteiligten eine gesicherte Kontaktaufnahme ermöglichen. Auf der Internetseite ist ebenfalls der öffentliche Schlüssel für die zentrale E-Mail-Adresse des Katholischen Datenschutzzentrums hinterlegt, so dass auch eine verschlüsselte Kommunikation per E-Mail möglich ist. Als weitere Möglichkeit der gesicherten Kommunikation hat das KDSZ eine DE-Mail-Adresse eingerichtet.

Das Katholische Datenschutzzentrum verschickt zudem einen Newsletter, der in unregelmäßigen Abständen über neue Informationen auf der Internetseite informiert. Der Newsletter kann über die Internetseite abonniert werden.

4.8.2 Vorträge

Wie schon in den Vorjahren war auch im Berichtszeitraum die Nachfrage nach Vorträgen durch das Katholische Datenschutzzentrum hoch, wenn auch mit Fortschreiten der Pandemie die Vortragstätigkeit ruhiger wurde. Während im Jahr 2018 Vorträge sehr stark gefragt waren, die einen allgemeinen Überblick über die neuen, ab Mai 2018 geltenden gesetzlichen Regelungen geben sollten, gab es in der nachfolgenden Zeit eine differenziertere Nachfrage.

Bei Informationsveranstaltungen ist das Katholische Datenschutzzentrum als Referent zugegen, organisiert die Veranstaltungen aber nicht selbst. Aufgrund der pandemiebedingten Einschränkungen wurden neue Formate für Vorträge erarbeitet und angeboten. Mit diesen Vorträgen konnten erneut viele Multiplikatoren und Verantwortliche erreicht werden.

Auf Präsenzveranstaltungen wurde im Berichtszeitraum weitestgehend verzichtet, viele Anfrage und Angebote wurden und werden wohl in das Folgejahr verlegt.

Das Katholische Datenschutzzentrum stellt auch vor dem Hintergrund der Pandemiesituation einen weiterhin hohen Informationsbedarf der kirchlichen Stellen, der betroffenen Personen und der Öffentlichkeit zum kirchlichen Datenschutz fest. Dieser Bedarf kann derzeit nur nicht allein mit den klassischen Instrumenten eines Präsenztermins bedient werden.

4.8.3 Informationen/Broschüren/Arbeitshilfen/Muster

Neben den Auskünften auf der Internetseite stellt das Katholische Datenschutzzentrum auch weitergehende Informationen in Form von Informationsblättern, Broschüren, Arbeitshilfen, Mustern oder Checklisten bereit.

In diesen Publikationen behandelt das KDSZ grundsätzliche oder aktuelle Themen, bei denen durch vermehrte Anfragen oder Beschwerden zu einem Thema ein erhöhter Informationsbedarf deutlich wird. Das

Angebot an Informationen wurde auch im Berichtszeitraum weiter ausgebaut.

Ergänzt wird dies durch Gastbeiträge für Fachzeitschriften (z. B. „Kompakt" für Kindertageseinrichtungen der Caritas in der Erzdiözese Köln), mit denen allgemein oder auch sehr zielgruppenspezifisch über Datenschutzthemen informiert wird.

4.9 Bußgelder

Das KDG sieht, anders als noch die frühere Anordnung über den kirchlichen Datenschutz, für die Diözesandatenschutzbeauftragten als Datenschutzaufsicht über die kirchlichen Stellen die Möglichkeit vor, bei Verstößen gegen das KDG eine Geldbuße zu verhängen. Diese kann im Einzelfall bis zu 500.000 Euro betragen.

Gemäß § 51 KDG kann die Datenschutzaufsicht eine Geldbuße gegen den Verantwortlichen oder Auftragsverarbeiter verhängen, wenn dieser vorsätzlich oder fahrlässig gegen Bestimmungen des KDG verstoßen hat. Bei der Möglichkeit der Verhängung einer Geldbuße handelt es sich um eine Ermessensvorschrift. Dies bedeutet, dass nicht jeder festgestellte Verstoß mit einer Geldbuße zu ahnden ist („Kann-Vorschrift"). Bei der Bemessung der Höhe einer Geldbuße sind vor allem die in § 51 Abs. 3 KDG aufgeführten Kriterien zu berücksichtigen. Dabei gilt es, sowohl mildernde als auch schärfende Umstände zu berücksichtigen und in die Abwägung einzubeziehen.

„Zwar erscheint die Geldbuße zunächst als die am Stärksten eingreifende Maßnahme der Datenschutzaufsicht, jedoch ist die Ahndung eines datenschutzrechtlichen Verstoßes mittels einer Anordnung … oftmals einschneidender für die Arbeit der kirchlichen Einrichtungen …"

Zwar erscheint die Geldbuße zunächst als die am Stärksten eingreifende Maßnahme der Datenschutzaufsicht, jedoch ist die Ahndung eines datenschutzrechtlichen Verstoßes mittels einer Anordnung nach § 47 Abs. 5 KDG oftmals einschneidender für die Arbeit der kirchlichen Einrichtungen, als die Zahlung einer Geldbuße. Gerade die in § 47 Abs. 5 lit. c) KDG normierte Anordnungsmöglichkeit, die Datenverarbeitung einzustellen[64], dürfte in den meisten Einrichtungen zu größerem (auch finanziellem) Aufwand führen. Dabei ist aber zu beachten, dass die Geldbuße einen begangenen Datenschutzverstoß ahnden soll, während die Maßnahmen nach § 47 Abs. 5 KDG zukünftige (weitere) Verstöße gegen datenschutzrechtliche Regelungen verhindern sollen.

Von den derzeit bei der Datenschutzaufsicht anhängigen Bußgeldverfahren wurde im Berichtszeitraum ein Verfahren mit einem Bußgeld gegen eine kirchliche Einrichtung abgeschlossen.

Das Bußgeld wurde wegen der mangelnden Beachtung von Betroffenenrechten (hier das Recht auf Berichtigung nach §§ 18, 21 KDG) verhängt. Gerade die gesetzlich normierten Betroffenenrechte, insbesondere das Recht auf Auskunft[65], sollten daher besonders sorgfältig von den Einrichtungen beachtet werden, um Bußgelder an dieser Stelle zu vermeiden.

[64] Im Berichtszeitraum hat die Datenschutzaufsicht auch mehrfach zum Mittel der Untersagungsverfügung gegriffen und bestimmte Verarbeitungen von personenbezogenen Daten in kirchlichen Einrichtungen vorübergehend oder endgültig untersagt.

[65] Siehe hierzu Abschnitt 3.4 dieses Jahresberichts.

4.10 Gerichtsverfahren mit Beteiligung des Katholischen Datenschutzzentrums

Das Gesetz über den Kirchlichen Datenschutz sieht für jede betroffene Person neben der Beschwerde bei der Datenschutzaufsicht auch das Recht auf gerichtlichen Rechtsbehelf (vgl. § 49 KDG) vor. Zuständiges Gericht für diese Antragsverfahren ist in erster Instanz das Interdiözesane Datenschutzgericht mit Sitz in Köln und in zweiter Instanz das Datenschutzgericht der Deutschen Bischofskonferenz mit Sitz in Bonn.[66]

In einem der im letzten Jahresbericht erwähnten Verfahren hat das Interdiözesane Datenschutzgericht die Entscheidung des Katholischen Datenschutzzentrums bestätigt.[67]

Im Berichtsjahr wurde ein Antrag beim Interdiözesanen Datenschutzgericht eingereicht, welcher den Bescheid des Katholischen Datenschutzzentrums in einem Beschwerdeverfahren zum Thema Einsichtnahme in Gottesdienstbesucherlisten während der Corona-Pandemie angreift. Das KDSZ hatte in dem Beschwerdeverfahren beschieden, dass alleiniger Zweck des Führens der Listen die Ermöglichung der Kontaktnachverfolgung durch die zuständigen Behörden ist und die Listen nur auf deren Aufforderung an diese ausgehändigt werden dürfen. Im konkreten Fall sah die Datenschutzaufsicht diesen Grundsatz durch die Einsichtnahme verletzt, da diese zu anderen Zwecken erfolgte. Gegen diesen Bescheid wendet sich die Antragstellerin.

[66] Nähere Informationen zu den beiden Gerichten inkl. der veröffentlichten Urteile sind abrufbar unter https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/

[67] Siehe Jahresbericht 2019, Abschnitt 4.10. Das zweite, dort erwähnte Verfahren ist noch nicht entschieden.

5 Dokumentation

5.1 Die Datenschutzaufsicht in der katholischen Kirche

5.1.1 Struktur der Aufsichtsstellen

Die Datenschutzaufsicht in der katholischen Kirche wird nicht von einer einzigen Stelle wahrgenommen. Vergleichbar den einzelnen Bundesländern mit eigener Gesetzgebung und jeweils eigenen Landesdatenschutzbeauftragten, hat auch jeder Diözesanbischof in Deutschland aufgrund seiner Gesetzgebungsgewalt das kirchliche Datenschutzrecht für die eigene (Erz-)Diözese in Kraft gesetzt und hat, wie im Gesetz vorgesehen, für den eigenen Wirkungskreis einen Diözesandatenschutzbeauftragten ernannt. Dieser DDSB nimmt die Funktion wahr, die im staatlichen Bereich der oder die Landesdatenschutzbeauftragte als Datenschutzaufsicht wahrnimmt.

Zur effektiven und effizienten Wahrnehmung der Aufgaben der Datenschutzaufsicht und in Umsetzung des Urteils des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsichtsbehörden aus dem Jahr 2010 haben jeweils mehrere (Erz-)Diözesen gemeinsame Diözesandatenschutzbeauftragte als Datenschutzaufsicht bestellt. Die Verteilung ist in der nachfolgenden Übersicht dargestellt:

Abb.: Struktur der Datenschutzaufsichten der (Erz-)Diözesen in Deutschland

Daneben gibt es noch eine eigene Datenschutzaufsicht für die katholische Militärseelsorge, die in Personalunion vom Diözesandatenschutzbeauftragten für die ostdeutschen (Erz-)Diözesen wahrgenommen wird. Außerdem besteht eine eigenständige Datenschutzaufsicht für den Verband der Diözesen Deutschlands und die nachgeordneten Ein-

richtungen. Diese Aufsichtsfunktion wird in Personalunion vom Diözesandatenschutzbeauftragten für die nordrhein-westfälischen (Erz-) Diözesen wahrgenommen.

Für den Bereich der Ordensgemeinschaften päpstlichen Rechts hat die Deutsche Ordensobernkonferenz (DOK), der Zusammenschluss der Höheren Oberen der Orden und Kongregationen in Deutschland, die Einrichtung der Gemeinsamen Ordensdatenschutzbeauftragten der DOK als Datenschutzaufsicht geschaffen.

5.1.2 Konferenz der Diözesandatenschutzbeauftragten

Zu den Aufgaben des DDSB gehört gemäß §§ 44 Abs. 3 lit. f) und 46 KDG das Hinwirken auf die Zusammenarbeit mit den anderen Diözesandatenschutzbeauftragten.

Um eine möglichst einheitliche Praxis bei der Auslegung des Gesetzes und bezogen auf Verfahrensabläufe der kirchlichen Stellen zu erreichen, tauschen sich die Diözesandatenschutzbeauftragten regelmäßig als Konferenz der DDSB aus. Neben den Diözesandatenschutzbeauftragten werden zu den Konferenzen auch die von der Deutschen Ordensobernkonferenz bestellten Ordensdatenschutzbeauftragten für die päpstlichen Ordensgemeinschaften als ständige Gäste eingeladen. Im Rahmen der Konferenzen ist ebenfalls ein jährlicher Austausch mit Vertretern des Verbandes der Diözesen Deutschlands, der Unterkommission Datenschutz- & Melderecht/IT-Recht der Rechtskommission des VDD, dem Katholischen Büro und der Deutschen Ordensobernkonferenz vorgesehen. Beratend können weitere Vertreter an den Tagungen teilnehmen.

Die Beratungen dienen dazu, gemeinsame Standpunkte zu verabschieden und gemeinsame Vorgehensweisen zu Themen zu finden. Ziel ist die möglichst einheitliche Auslegung des KDG in allen deutschen (Erz-) Diözesen durch die kirchlichen Datenschutzaufsichten.

Im Berichtszeitraum fanden fünf Konferenzen der Diözesandatenschutzbeauftragten statt, die aufgrund der Corona-Pandemie überwiegend als Videokonferenzen stattfanden. Gegenstand der Beratungen waren sowohl aktuelle Fragestellungen als auch Grundsatzfragen zum KDG, die sich bei der Umsetzung der Anforderungen des Datenschutzrechts für die kirchlichen Einrichtungen ergeben haben.

Auch zwischen den Konferenzen stehen die Diözesandatenschutzbeauftragten in regelmäßigem Austausch über aktuelle Fragen.

Zur Vorbereitung technischer Sachverhalte hat die Konferenz der DDSB einen Arbeitskreis Technik ins Leben gerufen. Die Leitung dieses Arbeitskreises wechselt jährlich zwischen den Datenschutzaufsichten.

Die katholischen und evangelischen Datenschutzaufsichten haben vor dem Hintergrund vergleichbarer Anforderungen und Fragestellungen beschlossen, sich regelmäßig über datenschutzrechtliche Themen auszutauschen und jährlich eine gemeinsame Sitzung der Kon-

ferenz der Diözesandatenschutzbeauftragten mit den evangelischen Datenschutzaufsichten durchzuführen. Leider konnte der Austausch aufgrund der Corina-Pandemie im Jahr 2020 nicht stattfinden.

5.1.3 FAQ zur Konferenz der Diözesandatenschutzbeauftragten

Zur Konferenz der Diözesandatenschutzbeauftragten werden immer wieder Fragen an das KDSZ herangetragen, die aus Sicht des Katholischen Datenschutzzentrums gerne beantwortet werden:

Auf welcher (Rechts-)Grundlage ist das Gremium der Konferenz der Diözesandatenschutzbeauftragen gebildet worden?

Das KDG gibt den Diözesandatenschutzbeauftragten in den §§ 44 Abs. 3 lit. f) und 46 KDG das Hinwirken auf die Zusammenarbeit mit den anderen Diözesandatenschutzbeauftragten vor. Ein formales Gremium sieht das Gesetz aber nicht vor.

Die „Konferenz der Diözesandatenschutzbeauftragten" ist die von den Diözesandatenschutzbeauftragten selbst gewählte formalisierte Form dieser Vorgabe des KDG zur Zusammenarbeit.

Kann ich als Gast an den Sitzungen teilnehmen?

Die Konferenz besteht aus den Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen.

Durch die Beauftragung einzelner Diözesandatenschutzbeauftragter durch mehrere (Erz-)Diözesen gibt es derzeit fünf Diözesandatenschutzbeauftragte.

Als ständige Gäste nehmen die von der Deutschen Ordensobernkonferenz bestellten Gemeinsamen Ordensdatenschutzbeauftragten für die Datenschutzaufsichten der päpstlichen Ordensgemeinschaften an den Sitzungen teil, um auch hier die enge Abstimmung sicherzustellen.

Gemäß der Absprache in der Konferenz können themenbezogen oder zu einzelnen Sitzungen weitere Gäste eingeladen werden. Es besteht aber kein Anspruch einzelner Verbände, Gremien oder Personen auf Teilnahme an den Sitzungen.

Welche Verbindlichkeit/Rechtswirkungen haben die Beschlüsse der Konferenz?

Da die Konferenz kein gesetzlich vorgesehenes Gremium mit gesetzlichen Aufgaben und Befugnissen ist, können die Beschlüsse auch keine direkte bindende Wirkung per Gesetz entfalten.

Die Beschlüsse der Konferenz sind eine gemeinsame Auslegung der datenschutzrechtlichen Vorschriften und deren Anwendung auf bestimmte Sachverhalte durch die Diözesandatenschutzbeauftragten.

Der Beschluss an sich ist daher für die kirchlichen Einrichtungen nicht verbindlich. Er entfaltet gegenüber den kirchlichen Stellen aber indirekt dadurch Wirkung, dass die eigene zuständige Datenschutzaufsicht den Beschluss zur Grundlage ihrer Entscheidung im konkreten Einzelfall machen wird, der dann für die Einrichtung verbindlich ist.

Der Wert der Beschlüsse ergibt sich daher aus Sicht des Katholischen Datenschutzzentrums daraus, dass es eine einheitliche Auslegung der Sachverhalte zwischen den Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen gibt. Für die kirchlichen Stellen bringen diese Beschlüsse dadurch ein großes Stück Berechenbarkeit der Datenschutzaufsichten, da sich die Einrichtungen anhand der Beschlüsse auf die Entscheidung ihrer zuständigen Datenschutzaufsicht im konkreten Einzelfall besser einstellen können.

Welche Funktion hat die Sprecherin oder der Sprecher der Konferenz?

Die Konferenz wählt aus ihrer Mitte jährlich eine Sprecherin beziehungsweise einen Sprecher. Ihre/Seine Aufgabe ist die Vorbereitung und Leitung der Sitzungen der Konferenz. Außerdem nimmt sie/er als Gast an der Unterkommission Datenschutz- und Melderecht/IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands teil und nimmt andere Termine für die Konferenz wahr.

Wie kann ich mich direkt an die Konferenz wenden?

Die Konferenz der Diözesandatenschutzbeauftragten hat zur leichteren Erreichbarkeit eine „Geschäftsstelle" eingerichtet. Diese befindet sich beim Katholischen Datenschutzzentrum in Dortmund. Sie erreichen die Konferenz postalisch unter der Adresse des Katholischen Datenschutzzentrums in Dortmund oder per E-Mail unter ddsb@kdsz.de.

5.2 Veröffentlichungen des Katholischen Datenschutzzentrums - Auszug -

5.2.1 Infoblatt mobiles Arbeiten

Katholisches Datenschutzzentrum

Mobiles Arbeiten und Datenschutz in Zeiten der Corona-Pandemie

In der aktuellen Corona-Pandemie werden die Unternehmen und Einrichtungen von der Regierung aufgefordert, zur Vermeidung unnötiger sozialer Kontakte den Beschäftigten möglichst eine Erledigung der täglichen Arbeit von zu Hause aus zu ermöglichen.

Normalerweise ist die Einrichtung einer Arbeitsmöglichkeit zu Hause mit einigem organisatorischen Vorlauf verbunden, damit bei der Arbeit zu Hause der Datenschutz im gleichen Maße gewährleistet werden kann wie bei der Arbeit im Büro. In der derzeitigen Situation der Corona-Pandemie findet der Wechsel vom Büro zum heimischen Arbeitsplatz meist ohne lange Vorbereitungszeit statt. Das Katholische Datenschutzzentrum gibt zur Umsetzung des Datenschutzes auch in dieser Situation folgende Hinweise:

Telearbeit – Homeoffice – mobiles Arbeiten
Unter dem Begriff Telearbeit werden häufig alle Arbeitsformen zusammengefasst, bei denen Mitarbeiter einen Teil der Arbeit außerhalb der Gebäude des Arbeitgebers verrichten - unabhängig davon, ob die Arbeit von einem fest eingerichteten Arbeitsplatz oder von unterwegs (mobil) erfolgt. Die gesetzliche Definition unterscheidet jedoch zwischen Telearbeit im engeren Sinne und „mobilem Arbeiten“: Mit der Novellierung der Arbeitsstättenverordnung (ArbStättV) im November 2016 wurde der Begriff der Telearbeit erstmals gesetzlich definiert und damit auch von einer generellen Zulässigkeit ausgegangen. Die Verordnung definiert einen Telearbeitsplatz als einen durch den Arbeitgeber fest eingerichteten Bildschirmarbeitsplatz im Privatbereich des Arbeitnehmers und formuliert arbeitsrechtliche und arbeitssicherheitstechnische Mindeststandards. Erst wenn sowohl die Ausstattung geliefert und installiert als auch die arbeitsrechtliche Vereinbarung geschlossen ist, kann der Telearbeitsplatz in Betrieb gehen.

Im Gegensatz dazu ist mobiles Arbeiten (auch als Remote Work oder Mobile Office bezeichnet) bisher nicht gesetzlich definiert. Das mobile Arbeiten baut zwar - ebenso wie die Telearbeit - auf einer Verbindung zum Betrieb per Informations- und Kommunikationstechnik auf. Diese Arbeitsform zeichnet sich jedoch dadurch aus, dass sie weder an das Büro, noch an den häuslichen Arbeitsplatz gebunden ist. Die Mitarbeiter und Mitarbeiterinnen können von beliebigen anderen Orten mithilfe von Laptop, Tablet oder Smartphone über das mobile Netz ihre Arbeit unabhängig von festen Arbeitszeiten und festen Arbeitsplätzen erledigen. Auch ist nicht unbedingt geregelt, dass die Ausstattung durch den Arbeitgeber gestellt wird.

In der aktuellen Situation wird es also meistens um „temporäres mobiles Arbeiten“ gehen, auch wenn der Begriff „Home Office“ gerne verwendet wird. Die jetzt geschaffenen Möglichkeiten zum Arbeiten zu Hause sollen in der Regel nur einen temporären Charakter haben. Die dauerhafte Einrichtung von Home-Office-Arbeitsplätzen (offiziell: „Telearbeitsplätzen“ nach ArbStättV) kann nur unter erweiterten Voraussetzungen (z.B. Dienstvereinbarung und arbeitsvertragliche Vereinbarungen, Einhaltung der Vorgaben für einen Arbeitsplatz nach der ArbStättV) erfolgen.

Informationsblätter

Seite 1 katholisches-datenschutzzentrum.de Rev. 1.0 / 03.04.2020

Katholisches Datenschutzzentrum

Auch unter datenschutzrelevanten Aspekten unterscheiden sich die Anforderungen an einen Telearbeitsplatz von den Voraussetzungen für ein datenschutzkonformes temporäres mobiles Arbeiten.

Einsatz dienstlicher Endgeräte:
Auch beim mobilen Arbeiten muss die kirchliche Einrichtung als Verantwortliche im Sinne des Datenschutzes für die datenschutzkonforme Verarbeitung der personenbezogenen Daten sorgen.

Diesen Schutz wird der Verantwortliche beim Einsatz dienstlicher Endgeräte, die er selbst konfiguriert hat, einfacher sicherstellen können, als beim Einsatz privater Endgeräte.

Der Einsatz privater Geräte zu dienstlichen Zwecken muss nach § 20 KDG-DVO gesondert begründet werden.

In jedem Fall sollte den Beschäftigten eine Ansprechperson für technische Probleme zur Seite stehen. Außerdem müssen auch im häuslichen Umfeld die nötigen Sicherheitsmaßnahmen gewährleistet sein (z. B. sind das System und der Virenschutz mit Updates und Patches auf dem aktuellem Stand zu halten).

Sichere Datenverbindung:
Der Zugriff auf die Firmendaten und evtl. die Firmenanwendungen muss über eine „mithörsichere" verschlüsselte Verbindung erfolgen. Hierzu bietet sich z.B. eine VPN (Virtual Private Network) – Verbindung an, die auf eine normale unverschlüsselte Internetverbindung aufgesetzt wird. Eine VPN-Verbindung benötigt Einstellungen auf dem Router oder der Firewall des Unternehmens und auf dem Endgerät, welches für das mobile Arbeiten genutzt werden soll. Eine andere Möglichkeit ist das Arbeiten in speziellen webbasierten Oberflächen wie z.B. CITRIX, wobei nicht nur die Daten, sondern auch die Anwendungen zentral auf den Servern des Unternehmens bleiben.

Lokale Daten auf dem Endgerät:
Dokumente in Bearbeitung und Arbeitsergebnisse werden am besten auf Datenträgern im Netz des Unternehmens bzw. der Einrichtung gespeichert So kann auch die regelmäßige Datensicherung (Backup) gewährleistet werden und die Daten sind keinem zusätzlichen Risiko durch alleinige lokale Speicherung ausgesetzt.

Auch wenn eine lokale Ablage von Daten auf dem Endgerät also möglichst vermieden oder reduziert werden sollte, lässt sich diese Ablage der Daten nicht ganz verhindern.

Der Datenspeicher des Endgerätes (z.B. die Festplatte) sind daher zu verschlüsseln, damit die Daten auf dem Gerät auch im Falle des Verlustes des Endgerätes geschützt sind.

Wenn z.B. mit CITRIX unter Einsatz eines privaten Endgerätes gearbeitet wird, muss CITRIX so konfiguriert werden, dass auf lokale Laufwerke (z.B. „C:\") nicht zugegriffen werden kann. Sollte es aus technischen Gründen nicht möglich sein, den Zugriff zu unterbinden, müssen entsprechende Bestimmungen per Dienstanweisung kommuniziert werden.

Informationsblätter

Katholisches Datenschutzzentrum

Verhinderung des Zugriffs durch Dritte bei dienstlichen Endgeräten:
Das dienstliche Endgerät mit den darauf evtl. befindlichen Daten oder dem Zugang auf die dienstlichen Server ist vor dem Zugriff Dritter zu schützen.

Eine Mitnutzung des Rechners durch Familie oder Freunde, weil z.B. der eigene private Rechner gerade besetzt ist, ist durch eine Anweisung an die Beschäftigten zu untersagen. Auch wenn der Nachwuchs nur mal eben was im Internet nachschauen will, kann nicht sichergestellt werden, dass er bei der Nutzung des Endgerätes nicht doch Kenntnis von schützenswerten dienstlichen Daten erhalten kann.

Vermeiden von Papier:
Der Arbeitsablauf sollte so gestaltet werden, dass keine Ausdrucke durch den Arbeitnehmer zu Hause nötig werden und dass auch keine schriftlichen Unterlagen für die Arbeit benötigt werden. Der notwendige „Dateninput" kann z.B. über E-Mail oder Intranet verfügbar gemacht werden. Werden dennoch schriftliche Unterlagen mit personenbezogenen Daten bei der mobilen Arbeit benötigt, müssen diese in geeigneter Weise bei Transport und Aufbewahrung im häuslichen Umfeld gesichert werden. Welche Maßnahmen hier im Einzelfall notwendig sind, richtet sich nach der Sensibilität der personenbezogenen Daten.

Telefon- und Videokonferenzen:
Bei der Auswahl von Anbietern von Konferenzdiensten ist auf eine datenschutzkonforme Gestaltung der Systeme zu achten. Auch hier gilt in der Regel der z.B. von Messengerdiensten bekannte Grundsatz, dass die Dienste entweder mit Geld oder mit Daten bezahlt werden. Vor der Nutzung der Dienste sollte daher überprüft werden, inwieweit diese Dienste Zugriff auf die Inhalts- oder Metadaten der Kommunikation haben (wollen). Zur Wahrung der Vertraulichkeit müssen intelligente Lautsprecher (z.B. Amazon-Echo, Google-Assistent oder Cortana), die das gesprochene Wort aus dem Wohnzimmer über das Internet an den Hersteller übertragen, während der Konferenzen ausgeschaltet sein.

Organisation der Arbeit zu Hause
Bei der Arbeit zu Hause sollte der Arbeitsplatz so organisiert sein, dass dienstliche und private Daten nicht gemischt werden. Wird der Arbeitsplatz verlassen, ist der Kennwortschutz zu aktivieren, damit ein unberechtigter Zugriff auf die Daten ausgeschlossen werden kann. Auch Papierakten müssen dann angemessen gesichert werden.

Bei der Arbeit mit dienstlichen Computern sollten keine privaten USB-Sticks oder andere private Hardware genutzt werden, um die Gefahr eines Befalls der dienstlichen Geräte mit Schadsoftware zu verringern. Sofern doch einmal der Verdacht besteht, dass ein Befall mit Schadsoftware vorliegen könnte, ist sofort die Einrichtung zu verständigen.

Werden Ausdrucke oder Notizen nicht mehr benötigt, dürfen diese nicht einfach in den privaten Papiermüll entsorgt werden. Auch bei der Entsorgung ist der Datenschutzeinzuhalten (z.B. durch Vernichtung mit einem privat vorhandenen Aktenvernichter oder durch Sammlung der Dokumente und Entsorgung bei der nächsten Möglichkeit im Büro).

Informationsblätter

Katholisches Datenschutzzentrum

Rückkehr in den Normalbetrieb
Alle Maßnahmen sind unter Beachtung der Schutzziele des Datenschutzes so zu gestalten, dass die temporäre mobile Arbeitsweise jederzeit reibungslos und unterbrechungsfrei in den Normalbetrieb zurückgeführt werden kann.

Stand: 26.03.2020

Informationsblätter

5.2.2 Infoblatt MAVO-Änderung

Katholisches Datenschutzzentrum

Einsatz neuer Informations- und Kommunikationstechnologien bei Sitzungen der Mitarbeitervertretungen in Zeiten der Corona-Pandemie

Bisher sah das Mitarbeitervertretungsrecht eine Präsenzpflicht der Mitglieder bei Sitzungen der Mitarbeitervertretung vor. Dies war die Voraussetzung für das Fassen wirksamer Beschlüsse. Vor dem Hintergrund der Corona-Pandemie und der damit verbundenen Schwierigkeiten, Sitzungen der Mitarbeitervertretungen als Präsenz-Sitzung durchzuführen, wurde Anfang April 2020 der § 14 Abs. 4 Mitarbeitervertretungsordnung (MAVO) um folgende Sätze ergänzt:

> „Kann die Sitzung der Mitarbeitervertretung wegen eines unabwendbaren Ereignisses nicht durch die körperliche Anwesenheit eines oder mehrerer Mitglieder durchgeführt werden, kann die Teilnahme einzelner oder aller Mitglieder an der Sitzung auch mittels neuer Informations- und Kommunikationstechnologien erfolgen, wenn sichergestellt ist, dass Dritte vom Inhalt der Sitzung keine Kenntnis nehmen können. Im Hinblick auf die Beschlussfähigkeit gelten die an der virtuellen Sitzung teilnehmenden Mitglieder als anwesend im Sinne des Abs. 5 S. 1."

Damit haben die (Erz-)Diözesen in Nordrhein-Westfalen auf die veränderten Bedingungen reagiert und die Möglichkeit geschaffen, Sitzungen der Mitarbeitervertretungen mittels neuer Informations- und Kommunikationswege abzuhalten.

Die neuen Möglichkeiten dürfen aber nur genutzt werden, wenn „*Dritte vom Inhalt der Sitzung keine Kenntnis nehmen können*". Damit hat die Mitarbeitervertretung auch bei Nutzung der erweiterten Möglichkeiten zur Teilnahme an der Sitzung der Mitarbeitervertretung (MAV) den Datenschutz sicherzustellen.

Bei der Vorbereitung und Durchführung der Sitzungen der MAV unter Nutzung der neuen Möglichkeiten sollten daher folgende Hinweise beachtet werden:

Anforderungen an den Ort, von dem aus Sie an der Konferenz teilnehmen
Stellen Sie an dem Ort, von dem aus Sie an der Sitzung der MAV per Telefon- oder Videokonferenz teilnehmen wollen, eine datenschutzkonforme Situation sicher.

Bei der Arbeit zu Hause sollte der Arbeitsplatz so organisiert sein, dass dienstliche und private Daten nicht vermischt werden. Wird der Arbeitsplatz verlassen, ist ein unberechtigter Zugriff auf dienstliche Daten auszuschließen. Auch Papierakten müssen dann angemessen gesichert werden.

Werden Ausdrucke oder Notizen nicht mehr benötigt, dürfen diese nicht einfach in den privaten Papiermüll entsorgt werden. Auch bei der Entsorgung ist der Datenschutz einzuhalten (z.B. durch Vernichtung mit einem privat vorhandenen Aktenvernichter oder durch Sammlung der Dokumente und Entsorgung bei der nächsten Möglichkeit im Büro).

Während der Teilnahme an der MAV-Sitzung per Telefon- oder Videokonferenz hat das MAV-Mitglied sicherzustellen, dass andere Personen (z.B. Familie, Freunde oder Nachbarn) vom Inhalt der Sitzung keine Kenntnis nehmen können. Ein Mithören oder Mitansehen der Sitzung durch andere Personen ist daher auszuschließen. Zur Wahrung der Vertraulichkeit müssen auch intelligente Lautsprecher (z.B. Amazon-

Informationsblätter

Katholisches Datenschutzzentrum

Echo, Google-Assistent oder Cortana), die das gesprochene Wort aus dem Wohnzimmer über das Internet an den Hersteller übertragen, während der Konferenzen ausgeschaltet sein.

Anforderungen an die Telefon- und Videokonferenzsysteme
Bei der Auswahl der Anbieter von Konferenzdiensten ist auf eine datenschutzkonforme Gestaltung der Systeme zu achten. Auch hier gilt in der Regel der z.B. von Messengerdiensten bekannte Grundsatz, dass die Dienste entweder mit Geld oder mit Daten bezahlt werden. Vor der Nutzung der Dienste sollte daher überprüft werden, inwieweit diese Dienste Zugriff auf die Inhalts- oder Metadaten der Kommunikation haben (wollen).

Anforderungen an die benutzten Endgeräte
Für die Teilnahme an den Telefon- oder Videokonferenzen sollten soweit möglich dienstliche Endgeräte, also dienstliche Telefone oder Computer, verwendet werden.

Durch die Verwendung der dienstlichen Geräte kann auch beim mobilen Arbeiten der technische und organisatorische Schutzstandard angewendet werden, der bei der Nutzung der Geräte in der Einrichtung eingerichtet ist. Derjenige, der verantwortlich für den Schutz der Daten ist, muss auch in der Situation des mobilen Arbeitens sicherstellen, dass der Schutz der personenbezogenen Daten gewährleistet ist.

Werden Vorlagen für die MAV-Sitzung oder die Protokolle auf private Computer heruntergeladen, so hat der Verantwortliche keine Kontrolle darüber, ob und wie die Daten der MAV auf diesen Geräten vor dem Zugriff Unbefugter geschützt sind.

Nutzen Sie daher möglichst Geräte, Programme und Kommunikationswege, die von Ihrer Einrichtung oder Ihrer MAV eingerichtet und/oder freigegeben worden sind, um die Vertraulichkeit der MAV-Daten auch vor, während und nach einer Teilnahme an einer MAV-Sitzung per Telefon- oder Videokonferenz sicherzustellen. Bei der Nutzung privater Geräte beachten Sie bitte die Vorgaben des § 20 KDG-DVO.

Schweigepflicht gilt auch bei mobilem Arbeiten
Auch in dieser Ausnahmesituation der Pandemie gelten die Verschwiegenheitspflichten der MAV-Mitglieder weiter. Schützen Sie daher Informationen besonders, die der Schweigepflicht nach § 20 MAVO unterliegen. Bei den durch die MAV verarbeiteten Daten handelt es sich in der Regel um Daten der Schutzklasse III gemäß § 13 KDG-DVO. Die für den Schutz der Daten relevanten Anforderungen gelten auch außerhalb der Einrichtungsinfrastruktur und müssen auch in dieser Situation sichergestellt werden.

So sollten z.B. keine MAV-Vorlagen auf private Computer oder andere Endgeräte heruntergeladen werden, da damit z.B. bei Computern, die auch von anderen Familienmitgliedern genutzt werden, die Möglichkeit besteht, dass diese unberechtigterweise von den heruntergeladenen Daten Kenntnis nehmen können.

Weiterführende Hinweise zu mobilem Arbeiten während der Corona-Pandemie
Weitere Hinweise zum mobilen Arbeiten in der derzeitigen Ausnahmesituation hat das Katholische Datenschutzzentrum im Informationsblatt „Mobiles Arbeiten und Datenschutz in Zeiten der Corona-Pandemie“ zusammengefasst.

Stand: 15.04.2020

Informationsblätter

5.3 Entschließungen und Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder im Jahr 2020 - Auszug -

5.3.1 Orientierungshilfe vom 13.03.2020: Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail

Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail[1]

Orientierungshilfe des Arbeitskreises
„Technische und organisatorische Datenschutzfragen"

Stand: 13. März 2020

1 Zielstellung

Die vorliegende Orientierungshilfe zeigt auf, welche Anforderungen an die Verfahren zum Versand und zur Entgegennahme von E-Mail-Nachrichten durch Verantwortliche, ihre Auftragsverarbeiter und öffentliche E-Mail-Diensteanbieter[2] auf dem Transportweg zu erfüllen sind. Diese Anforderungen richten sich nach den Vorgaben des Art. 5 Abs. 1 lit. f, 25 und 32 Abs. 1 DS-GVO. Die Orientierungshilfe nimmt den Stand der Technik zum Veröffentlichungszeitpunkt als Ausgangspunkt für die Konkretisierung der Anforderungen.

Verantwortliche und Auftragsverarbeiter[3] sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Sie müssen hierbei Art, Umfang, Umstände und Zwecke ihrer Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Diese Orientierungshilfe behandelt ausschließlich die Risiken, die mit einer Verletzung von Vertraulichkeit und Integrität personenbezogener Daten verbunden sind. Sie setzt voraus, dass die Verantwortlichen bzw. ihre Auftragsverarbeiter einschätzen, welche Schäden aus einem Bruch von Vertraulichkeit und Integrität resultieren können.

Die Orientierungshilfe geht von typischen Verarbeitungssituationen aus. Sie bestimmt hierbei ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail Anforderungen an die Maßnahmen, die Verantwortliche und Auftragsverarbeiter zur ausreichenden Minderung der Risiken zu treffen haben. Die Verantwortlichen und Auftragsverarbeiter sind verpflichtet, die Besonderheiten ihrer Verarbeitungen, darunter insbesondere den Umfang, die Umstände und die Zwecke der vorgesehenen Übermittlungsvorgänge zu berücksichtigen, die ggf. in abweichenden Anforderungen resultieren können. Dabei müssen sie berücksichtigen, dass die vorliegende Orientierungshilfe ausschließlich Risiken betrachtet, die sich auf dem Transportweg ergeben. Risiken, denen ruhende Daten wie bereits empfangene E-Mails ausgesetzt sind oder die durch eine Weiterverarbeitung wie z. B. automatische Weiterleitungen entstehen, werden in dieser Orientierungshilfe nicht betrachtet und können weitere Maßnahmen oder eine andere Gewichtung der im Folgenden aufgeführten Maßnahmen notwendig

[1] Die Orientierungshilfe wurde durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme Bayerns beschlossen.

[2] Diensteanbieter, die eigene oder fremde E-Mail Dienste zur öffentlichen Nutzung bereithalten

[3] Auftragsverarbeiter ausschließlich im Hinblick auf ihre Pflichten nach Art. 32 DS-GVO.

1

machen. Können die Anforderungen an eine sichere Übermittlung per E-Mail nicht erfüllt werden, so muss ein anderer Kommunikationskanal gewählt werden[4].

2 Anwendungsbereich und Grundsätze

Der gesetzlich gebotene Schutz personenbezogener Daten im Zuge der Übermittlung von E-Mail-Nachrichten erstreckt sich sowohl auf die personenbezogenen Inhalte als auch die Umstände der Kommunikation, soweit sich aus letzteren Informationen über natürliche Personen ableiten lassen[5]. Dieser Schutz muss abseits des Blickwinkels dieser Orientierungshilfe ergänzt werden durch Maßnahmen zum Schutz der beteiligten Systeme und zur Minimierung, Speicherbegrenzung und Zweckbindung der auf diesen Servern verarbeiteten Verkehrsdaten.

Diese Orientierungshilfe thematisiert den Vertraulichkeitsschutz der personenbezogenen Inhalte der E-Mail-Nachrichten lediglich insoweit, wie diese nicht bereits vorab (z. B. anwendungsspezifisch) gemäß dem Stand der Technik so verschlüsselt wurden, dass nur der Empfänger sie entschlüsseln kann.

Sowohl Ende-zu-Ende-Verschlüsselung als auch Transportverschlüsselung mindern für ihren jeweiligen Anwendungszweck Risiken für die Vertraulichkeit der übertragenen Nachrichten. Daher müssen Verantwortliche beide Verfahren in der Abwägung der notwendigen Maßnahmen berücksichtigen.

Der durchgreifendste Schutz der Vertraulichkeit der Inhaltsdaten wird durch Ende-zu-Ende-Verschlüsselung erreicht, wofür derzeit die Internet-Standards S/MIME (RFC 5751) und OpenPGP (RFC 4880) i.d.R. in Verbindung mit PGP/MIME (RFC 3156) zur Verfügung stehen. Ende-zu-Ende-Verschlüsselung schützt nicht nur den Transportweg, sondern auch ruhende Daten. Bei Ende-zu-Ende-Verschlüsselung kann die Verarbeitung unverschlüsselter Inhaltsdaten auf besonders geschützte Netzsegmente bzw. auf solche Teile des Netzes beschränkt werden, die ausschließlich zur Nutzung durch Befugte (wie eine Personalabteilung oder einen Amtsarzt) vorgesehen sind.

Der Einsatz von Transportverschlüsselung bietet einen Basis-Schutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. In Verarbeitungssituationen mit normalen Risiken wird dabei bereits durch die Transportverschlüsselung eine ausreichende Risikominderung erreicht.

Die Transportverschlüsselung reduziert die Erfolgswahrscheinlichkeit passiver Abhörmaßnahmen Dritter auf dem Transportweg auf ein geringfügiges Maß. Um auch gegen Dritte zu bestehen, die aktiv in den Netzverkehr eingreifen, muss sie in qualifizierter Weise durchgeführt und durch Maßnahmen zur kryptografischen Absicherung der Angaben der Empfänger über die zur Entgegennahme der Nachrichten berechtigten Geräte flankiert werden.

Eine Darstellung der Anforderungen an die einfache und an die qualifizierte obligatorische Transportverschlüsselung sowie an die Ende-zu-Ende-Verschlüsselung und die Signatur von E-Mail-Nachrichten ist in Abschnitt 5 niedergelegt.

[4] Für die Kommunikation mit betroffenen natürlichen Personen (z. B. mit Kunden) kann ein Kommunikationsweg in der Bereitstellung eines Webportals bestehen.

[5] Informationen über die Umstände der Kommunikation lassen sich verschiedenen Verarbeitungsprozessen entnehmen, die mit Versand und Empfang von E-Mail-Nachrichten in Verbindung stehen (vom Abruf von Angaben aus dem DNS bis zur Protokollierung der Kommunikation auf verschiedenen Geräten). Diese Orientierungshilfe thematisiert lediglich den Schutz der in den Kopfzeilen einer E-Mail-Nachricht enthaltenen Angaben während des Transports der Nachricht.

3 Die Inanspruchnahme von E-Mail-Diensteanbietern

3.1 Grundlegende technische Anforderungen an die Erbringung von E-Mail-Diensten

Zum Schutz der Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten müssen öffentliche E-Mail-Diensteanbieter die Anforderungen der TR 03108-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI) einhalten.

Dies bedeutet, dass sie verpflichtend die in dieser Technischen Richtlinie niedergelegten Voraussetzungen für einen geschützten Empfang von Nachrichten schaffen und bei dem Versand von Nachrichten in Bezug auf die Anwendung von kryptografischen Algorithmen und die Überprüfung der Authentizität und Autorisierung der Gegenstelle den unter den gegebenen Bedingungen auf Empfängerseite bestmöglichen mit verhältnismäßigen Mitteln erreichbaren Schutz erzielen müssen.

3.2 Sorgfaltspflicht bei der Inanspruchnahme von E-Mail-Diensteanbietern

Verantwortliche, die öffentliche E-Mail-Diensteanbieter in Anspruch nehmen, müssen sich davon überzeugen, dass die Anbieter hinreichende Garantien für die Einhaltung der Anforderungen der DS-GVO und insbesondere der genannten Technischen Richtlinie bieten. Dies schließt auch die sichere Anbindung eigener Systeme und Endgeräte an die Diensteanbieter ein.

Darüber hinaus müssen die Verantwortlichen die Risiken sorgfältig einschätzen, die mit dem Bruch der Vertraulichkeit und Integrität von E-Mail-Nachrichten verbunden sind, die sie versenden oder gezielt empfangen. In Abhängigkeit von diesen Risiken können sich die im Folgenden dargestellten zusätzlichen Anforderungen ergeben, deren Erfüllung sie durch Weisung an den Diensteanbieter (z. B. durch Vornahme geeigneter Konfigurationseinstellungen, soweit solche von dem Diensteanbieter angeboten werden) durchsetzen müssen.

4 Fallgruppen

4.1 Gezielte Entgegennahme von personenbezogenen Daten in den Inhalten von E-Mail-Nachrichten

Verantwortliche, die gezielt personenbezogene Daten per E-Mail entgegennehmen, z. B. durch explizite Vereinbarung des Austauschs personenbezogener Daten per E-Mail oder die Aufforderung auf der Homepage, personenbezogene Daten per E-Mail zu übermitteln, haben die im Folgenden beschriebenen Verpflichtungen zu erfüllen.

4.1.1 Verpflichtungen bei normalen Risiken[6]

Der Schutz von Vertraulichkeit und Integrität von personenbezogenen Daten bei der Übermittlung von E-Mail-Nachrichten setzt voraus, dass Sender und Empfänger zusammenarbeiten. Die Verantwortung für den einzelnen Übermittlungsvorgang liegt bei dem Sender. Wer jedoch gezielt personenbezogene Daten per E-Mail entgegennimmt, ist verpflichtet, die Voraussetzungen für den sicheren Empfang von E-Mail-Nachrichten über einen verschlüsselten Kanal zu schaffen. Das bedeutet, dass der Empfangsserver mindestens den Aufbau von TLS-Verbindungen (direkt per SMTPS oder nach Erhalt eines STARTTLS-Befehls über SMTP) ermöglichen muss und hierbei ausschließlich die in der BSI TR 02102-2 aufgeführten Algorithmen verwenden darf. Um den Aufbau verschlüsselter Verbindungen zu erleichtern, sollte der Verantwortliche für Verschlüsselung und Authentifizierung ein möglichst breites Spektrum an qualifizierten Algorithmen anbieten.

Um die Authentizität und Integrität der empfangenen E-Mail-Nachrichten zu überprüfen, sollten Verantwortliche DKIM-Signaturen prüfen und signierte Nachrichten, bei denen die Prüfung fehlschlägt,

[6] Zur Einstufung von Risiken s. das Kurzpapier Nr. 18 der unabhängigen Datenschutzbehörden des Bundes und der Länder „Risiko für die Rechte und Freiheiten natürlicher Personen", abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/kurzpapiere/DSK_KPNr_18_Risiko.pdf.

markieren oder, bei entsprechender Festlegung des Absenders über einen DMARC-Eintrag im DNS, zurückweisen.

4.1.2 Verpflichtungen bei hohen Risiken

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei denen der Bruch der Vertraulichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er sowohl qualifizierte Transportverschlüsselung (s. u. Nr. 5.2) als auch den Empfang von Ende zu Ende verschlüsselter Nachrichten ermöglichen.

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei den der Bruch der Integrität ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er bestehende (PGP- oder S/MIME-) Signaturen qualifiziert prüfen (s. u. Nr. 5.4).

4.2 Versand von E-Mail-Nachrichten

4.2.1 Verpflichtungen bei normalen Risiken

Alle Verantwortliche, die E-Mail-Nachrichten mit personenbezogenen Daten versenden, bei denen ein Bruch der Vertraulichkeit (des Inhalts oder Umstände der Kommunikation, soweit sie sich auf natürliche Personen beziehen) ein Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, sollten sich an der TR 03108-1 orientieren und müssen eine obligatorische Transportverschlüsselung sicherstellen.

4.2.2 Versand von E-Mail-Nachrichten bei hohem Risiko

Verantwortliche, die E-Mail-Nachrichten versenden, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, müssen regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung vornehmen. Inwieweit entweder auf die Ende-zu-Ende-Verschlüsselung oder die Erfüllung einzelner Anforderungen an diese (s. Kap. Ende-zu-Ende-Verschlüsselung) oder an die qualifizierte Transportverschlüsselung (z. B. DANE oder DNSSEC) verzichtet werden kann, hängt von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und ggf. getroffenen kompensierenden Maßnahmen ab.

4.2.3 Versand von E-Mail-Nachrichten mit geheim zu haltenden Inhalten bei hohen Risiken

Verantwortliche, die aufgrund von § 203 StGB zur Geheimhaltung von Kommunikationsinhalten verpflichtet sind, müssen über die unter 4.2.1 bzw. 4.2.2 aufgeführten Anforderungen hinaus durch Verschlüsselung sicherstellen, dass nur Stellen eine Entschlüsselung vornehmen können, an die die Inhalte der Nachrichten offenbart werden dürfen.

5 Anforderungen an die Verschlüsselungs- und Signaturverfahren

5.1 Obligatorische Transportverschlüsselung

Durch eine obligatorische Transportverschlüsselung soll eine unverschlüsselte Übermittlung der Nachrichten ausgeschlossen werden. Sie kann über das Protokoll SMTPS oder durch Aufruf des SMTP-Befehls STARTTLS und den nachfolgenden Aufbau eines mit dem Protokoll TLS verschlüsselten Kommunikationskanals realisiert werden, wobei die Anforderungen der TR 02102-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu erfüllen sind.

Bei dem letztgenannten Verfahren (STARTTLS) kann die obligatorische Transportverschlüsselung durch entsprechende Konfiguration des sendenden MTA (Mail Transfer Agent) erreicht werden – die entsprechenden Konfigurationseinstellungen werden (En)Forced TLS, Mandatory TLS o. ä. genannt. Unterstützt die Gegenstelle kein TLS, dann wird der Verbindungsaufbau abgebrochen. Einige MTA ermöglichen eine domänenspezifische oder regelbasierte Spezifizierung dieses Verhaltens.

5.2 Qualifizierte Transportverschlüsselung

Transportverschlüsselung erreicht unter folgenden Voraussetzungen einen ausreichenden Schutz gegen aktive Angriffe von Dritten, die in der Lage sind, den Netzwerkverkehr auf der Übermittlungsstrecke zu manipulieren:

1. Die eingesetzten kryptografischen Algorithmen und Protokolle entsprechen dem Stand der Technik: Sie erfüllen die Anforderungen der Technischen Richtlinie BSI TR-02102-2 und garantieren Perfect Forward Secrecy.
2. Die Bezeichnung der zum Empfang autorisierten Mailserver und ihre IP-Adressen wurden auf Empfängerseite per DNSSEC signiert. Die Signaturen der DNS-Einträge werden auf Senderseite überprüft. Alternativ kann die Bezeichnung der zum Empfang autorisierten Mailserver auch durch Kommunikation mit dem Empfänger verifiziert werden.
3. Der empfangende Server wird im Zuge des Aufbaus der verschlüsselten Verbindung entweder zertifikatsbasiert authentifiziert oder anhand eines öffentlichen oder geheimen Schlüssels, der über einen anderen Kanal zwischen Sender und Empfänger abgestimmt wurde.
4. Erfolgt die Authentifizierung zertifikatsbasiert, so führt der Empfänger die Authentizität des Zertifikats auf ein vertrauenswürdiges Wurzelzertifikat bzw. einen via DANE publizierten Vertrauensanker zurück.

Die Einhaltung dieser Anforderungen muss nachgewiesen werden.

5.3 Ende-zu-Ende-Verschlüsselung

Durch eine Ende-zu-Ende-Verschlüsselung mit den Verfahren S/MIME und OpenPGP ist es möglich, die Inhalte einer E-Mail-Nachricht durchgreifend gegen unbefugte Kenntnisnahme zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Um diese Wirksamkeit zu erreichen, sind folgende Voraussetzungen einzuhalten:

1. Der Verantwortliche muss die öffentlichen Schlüssel der Empfänger auf die Einhaltung hinreichender Sicherheitsparameter (insbesondere einer hinreichenden Schlüssellänge) überprüfen, sie durch Verifikation der Zertifikate bzw. Beglaubigungen authentisieren, vor jedem Versand bzw. Signaturprüfung auf Gültigkeit überprüfen und zuverlässig verwalten.
2. Die Überprüfung der Authentizität eines Schlüssels kann regelmäßig durch Verifikation eines Zertifikats eines vertrauenswürdigen Zertifikatsdienstanbieters (S/MIME) oder Beglaubigung anderer vertrauenswürdiger und nachweislich zuverlässiger Dritter (OpenPGP) erfolgen. Es sei ausdrücklich darauf hingewiesen, dass die Veröffentlichung eines Schlüssels auf einem OpenPGP-Schlüsselserver kein Indiz für die Authentizität dieses Schlüssels ist. Die Überprüfung des Fingerprints eines OpenPGP-Keys ist für die Überprüfung der Authentizität eines Schlüssels ausreichend, sofern der Fingerprint mit einer sicheren kryptografischen Hashfunktion (s. BSI TR-02102) ermittelt und die Authentizität des Vergleichswerts z. B. durch direkte Kommunikation mit dem Empfänger über einen anderen Kanal überprüft wurde.
3. Die Authentizität eines über Web Key Directory (WKD) bereitgestellten öffentlichen Schlüssels ist äquivalent zu der Authentizität des bereitstellenden Webservers. Für die Überprüfung gelten die Anforderungen an die Überprüfung der Authentizität des empfangenden Mailservers entsprechend.
4. Diese Anforderung kann auch nachträglich in Bezug auf Schlüssel erfüllt werden, die zunächst opportunistisch ausgetauscht wurden (z. B. per Autocrypt). Hierzu ist eine Verifikation der Authentizität über einen anderen Kanal erforderlich.

5. Die Überprüfung der Gültigkeit eines S/MIME-Schlüssels vor seinem Einsatz soll durch Abruf von Gültigkeitsinformationen bei dem Zertifikatsdiensteanbieter (Abruf von CRL via http, OCSP) erfolgen. Die Überprüfung der Gültigkeit eines OpenPGP-Schlüssels ist nur möglich, wenn der Eigner bekannt gegeben hat, wo er ggf. Revokationszertifikate zu veröffentlichen beabsichtigt. Dies kann z. B. ein OpenPGP-Schlüsselserver oder die Webseite des Schlüsseleigners sein. Sofern es an einer solchen Abrufmöglichkeit fehlt, müssen Garantien dafür bestehen, dass alle Nutzer eines Schlüssels unverzüglich informiert werden, wenn dieser seine Gültigkeit – insbesondere aufgrund einer Kompromittierung des zugehörigen privaten Schlüssels – verliert.

Wer Nachrichten Ende zu Ende verschlüsselt, sollte beachten, dass Perfect Forward Secrecy durch Ende-zu-Ende-Verschlüsselung allein nicht gegeben ist, so dass eine Kompromittierung des privaten Schlüssels eines Empfängers alle Nachrichten gefährdet, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden. E-Mail-Nachrichten, die von Dritten abgefangen werden, können von diesen aufbewahrt und bei Offenlegung des privaten Schlüssels eines der Empfänger zu einem späteren Zeitpunkt entschlüsselt werden.

5.4 Signatur

Durch eine Signatur mit den Verfahren S/MIME und OpenPGP ist es möglich, die Integrität der Inhalte einer E-Mail-Nachricht nachhaltig gegen unbefugte Beeinträchtigung zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Um diese Wirksamkeit zu erreichen, sind folgende Voraussetzungen einzuhalten:

Sender müssen die eigenen Signaturschlüssel mit hinreichenden Sicherheitsparametern erzeugen, die privaten Schlüssel sicher speichern und nutzen; soweit kein direkter Abgleich der Schlüssel zwischen Sender und Empfänger stattfindet, die korrespondierenden öffentlichen Schlüssel von zuverlässigen und vertrauenswürdigen Dritten zertifizieren lassen und sie ihren Kommunikationspartnern zur Verfügung stellen. Empfänger sollen in Abhängigkeit von den Authentizitäts- und Integritätsrisiken die in Kap. Ende-zu-Ende-Verschlüsselung aufgeführten Maßnahmen auf die Überprüfung und das Management der Schlüssel der Sender in entsprechender Weise anwenden.

5.3.2 Entschließungvom03.04.2020:Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 03.04.2020

Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

Die Corona-Pandemie stellt eine der größten Bewährungsproben für die europäischen Gesellschaften seit Jahrzehnten dar. Alle Mitgliedstaaten der Europäischen Union haben gegenwärtig extreme Herausforderungen zu bewältigen, um die Gesundheit ihrer Bevölkerung zu gewährleisten. Angesichts der bereits getroffenen Maßnahmen wird gleichzeitig der Wert der Freiheitsrechte erlebbar, zu denen auch das Grundrecht auf informationelle Selbstbestimmung gehört.

Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden.

Was die Rechtfertigung der Verarbeitung personenbezogener Daten nach Maßgabe der europäischen Datenschutz-Grundverordnung anbelangt, stellt sie insbesondere in ihrem Artikel 5 **europaweit einheitliche Grundsätze** bereit, die als Leitfaden für staatliches Handeln auch gerade in Krisenzeiten dienen können, einer effektiven Bekämpfung der Corona-Pandemie nicht entgegenstehen und zugleich einen grundrechtsschonenden Umgang mit personenbezogenen Daten gewährleisten.

Im Zusammenhang mit der Bewältigung der Corona-Krise weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder daher auf **folgende wesentliche Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten** hin:

- Krisenzeiten ändern nichts daran, dass die **Verarbeitung** personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen hat. Das bedingt insbesondere, dass die mit einer Verarbeitung verfolgten Zwecke möglichst genau bezeichnet werden.

- Die **geplanten Maßnahmen** müssen zudem kritisch auf ihre **Eignung** überprüft werden, um etwa Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es in Notfalllagen beispielsweise eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die Gesundheitsversorgung zuständigen Behörden zu melden. Hingegen bestehen erhebliche Zweifel an der Eignung etwa von Maßnahmen, die allein mithilfe von Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.

- Die geplanten Maßnahmen müssen erforderlich sein. Stehen **ebenfalls geeignete Maßnahmen zur Zweckerreichung** zur Verfügung, die **weniger**, oder - wie eine vorherige Anonymisierung - sogar gar nicht in die Rechte der Menschen eingreifen, müssen diese vorrangig umgesetzt werden. Zudem darf die Verarbeitung der personenbezogenen Daten **nicht** – wie die präventive Überwachung ausnahmslos der gesamten Bevölkerung – **außer Verhältnis zum angestrebten legitimen Zweck** stehen. Daraus folgt, dass besonders stark freiheitseinschränkende Maßnahmen auch an besondere Voraussetzungen geknüpft werden müssen – etwa an die formelle Feststellung einer Gesundheitsnotlage, wie sie nach dem Infektionsschutzrecht in einigen Ländern bereits erfolgt ist.

- Zur verhältnismäßigen Ausgestaltung der Verarbeitung von sensiblen Daten gehört es schließlich, dass die speziell zur Bewältigung der Corona-Pandemie getroffenen Maßnahmen umkehrbar in dem Sinne gestaltet werden, dass sie nach Krisenende wieder zurückgenommen werden können und, wenn sie dann unverhältnismäßig sind, sogar müssen. So sind **nicht mehr für die benannten Zwecke benötigte** personenbezogene Daten **unverzüglich** zu **löschen**. Generell sollten zudem **alle Maßnahmen befristet** werden. Dies gilt insbesondere für solche gesetzlichen Maßnahmen, die in besonderem Maße in die Grundrechte der betroffenen Personen eingreifen.

- Gesundheitsdaten zählen zu den besonders sensiblen Daten, weil ihre Verwendung für die betroffenen Personen besondere Risiken nicht zuletzt in ihrem gesellschaftlichen Umfeld begründen können. Das europäische Datenschutzrecht verlangt deshalb geeignete Garantien zum Schutz der betroffenen Personen. **Technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit von Gesundheitsdaten** sind nicht nur **rechtlich geboten**, sondern auch **notwendig**, um eine missbräuchliche Verwendung von Daten zu verhindern und Fehlern in der Verarbeitung entgegenzuwirken. Wichtig ist es auch, im Sinne des Datenschutz-Grundsatzes der Transparenz die betroffenen Personen in verständlicher Weise über die Verarbeitung ihrer Daten zu informieren.

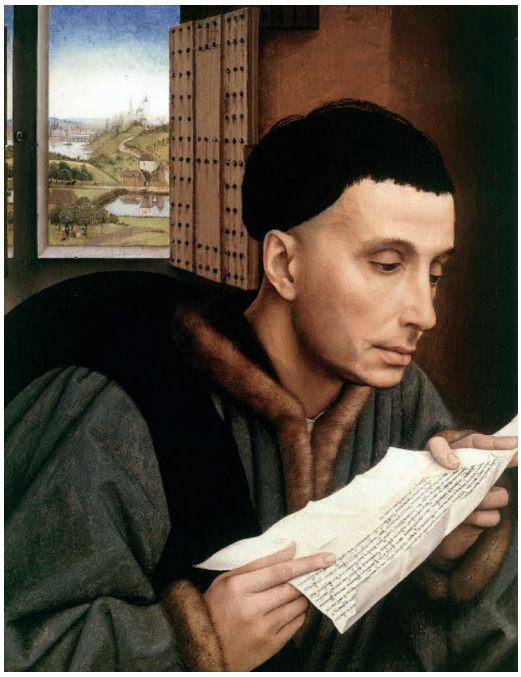
Datenschutz-Grundsätze bieten gerade auch in Krisenzeiten hinreichende Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten. Ihre Einhaltung leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft.

2

Abkürzungsverzeichnis

BGBl	Bundesgesetzblatt
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDU	Christlich Demokratische Union Deutschlands
DDSB	Diözesandatenschutzbeauftragte(r)
DOK	Deutsche Ordensobernkonferenz
DSG-EKD	Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz)
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder (Datenschutzkonferenz)
EDSA	Europäischer Datenschutzausschuss
EKD	Evangelische Kirche in Deutschland
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
FDP	Freie Demokratische Partei
GRCh	Charta der Grundrechte der Europäischen Union
IDSG	Interdiözesanes Datenschutzgericht
IfSG	Infektionsschutzgesetz
IT	Informationstechnik
KDG	Gesetz über den Kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum KDG
KDG-VDD	KDG für den Verband der Diözesen Deutschlands
KDM	Kirchliches Datenschutzmodell
KDO	Anordnung über den kirchlichen Datenschutz
KDO-Schule	KDO für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Trägerschaft
KDS-VwVfG	Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz
KDSZ	Katholisches Datenschutzzentrum
KHGG NRW	Krankenhausgestaltungsgesetz des Landes Nordrhein-Westfalen
MAV	Mitarbeitervertretung
MAVO	Mitarbeitervertretungsordnung
MStV	Medienstaatsvertrag
OVG	Oberverwaltungsgericht
PatDSG	Gesetz zum Schutz von Patientendaten
PatDSO	Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern
RStV	Rundfunkstaatsvertrag

SDM	Standard-Datenschutzmodell
Seelsorge-PatDSG	PatDSG bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens
USA	Vereinigte Staaten von Amerika
VDD	Verband der Diözesen Deutschlands
VG	Verwaltungsgericht
VO-DV I	Verordnungen über die zur Verarbeitung zugelassener Daten von Schülerinnen, Schülern und Eltern
VO-DV II	Verordnungen über die zur Verarbeitung zugelassener Daten der Lehrerinnen und Lehrer
§ 29-KDG-Gesetz	Gesetz zur Regelung des Rechtsinstruments nach § 29 Gesetz über den Kirchlichen Datenschutz (KDG)



Hl. Ivo

Der heilige Ivo ist der Schutzpatron des Katholischen Datenschutzzentrums.
Er lebte im 13. Jahrhundert im heutigen Frankreich und setzte sich dort unter anderem für Arme und Bedrängte vor weltlichen und kirchlichen Gerichten ein.
Das Bildnis des heiligen Ivo ziert auch das Siegel des Katholischen Datenschutzzentrums. Sein Gedenktag ist der 19. Mai.

Bild: Joachim Schäfer – www.heiligenlexikon.de

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de