Tätigkeitsbericht des Datenschutzbeauftragten für Kirche und Diakonie*

vorgelegt gemäß § 41 EKD-Datenschutzgesetz – DSG-EKD:

der Kirchenleitung der Ev.-Luth. Landeskirche Sachsens

dem Vorstand und dem Diakonischen Rat des Diakonischen Werkes der Ev.-Luth. Landeskirche Sachsens e. V.

der Kirchenleitung der Evangelischen Landeskirche Anhalts

dem Vorstand und dem Diakonischen Rat des Diakonischen Werkes Evangelischer Kirchen in Mitteldeutschland e. V.

für den Berichtszeitraum
2020 und 2021

*Aufsichtsbehörde für den Datenschutz gemäß Kirchengesetz zur Durchführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (Datenschutz-Durchführungsgesetz) vom 16. April 2018 (ABl. 2018 S. A 62), gemäß dem Beschluss der Landessynode der Evangelisch-Lutherischen Landeskirche Sachsens

Der Datenschutzbeauftragte für Kirche und Diakonie
Reichenbrander Str. 4 ▪ 09117 Chemnitz
Tel.: 0351-4692-460 ▪ Fax 0351-4692-469
E-Mail: Datenschutzbeauftragter@evlks.de
WEB-Site: www.dsbkd.de

Offizielle Druckversion vom 22.06.2022

Hinweis zum Sprachgebrauch in diesem Bericht:

Soweit im Bericht die männliche oder weibliche Form verwendet wird, geschieht das zur besseren Lesbarkeit und Textverständlichkeit, der Sachverhalt bezieht sich aber ausdrücklich auf alle Geschlechter. Sofern eine Personifizierung vorhanden war, wird die entsprechende Form verwendet. Leserin bzw. Leser sollen sich bitte auch von der andersgeschlechtlichen Bezeichnung angesprochen fühlen, geht es doch vordergründig um den fachlichen Sachverhalt.

Übergeordnete Bezeichnungen, die eine geschlechtliche Ausdrucksform durch Worterweiterung nicht zulassen (z. B. Person, Kind, Mensch, Mitarbeitende) zu verwenden, wären eine Möglichkeit. Dies kann den Sachverhalt jedoch weit vom tatsächlich vorliegenden Fall entfernen, was einer Betrachtung der Problemfälle auf „Augenhöhe“ und damit einem Erkennen eigener Pflichten eher hinderlich ist.

Inhaltsverzeichnis

Vorwort

Datenschutz ist immer noch ein Thema, welches schwer zu verstehen und noch schwerer umzusetzen ist!

Die Jahre 2020 und 2021 waren durch besondere Faktoren in Gesellschaft und Kirche geprägt.

So spielte die weltweit grassierende Corona-Pandemie eine große Rolle. Die Corona-Pandemie zwang viele verantwortliche Stellen, sowohl im Bereich der verfassten Kirchen als auch in den Diakonischen Werken nach gangbaren und verantwortbaren organisatorischen und technischen Lösungen zur Erfüllung ihrer Aufgaben und ihres Auftrages zu suchen.

Insbesondere die Herausforderung zur Umsetzung der gesetzlichen Pflicht zum Homeoffice, den Abstands- und Hygieneregeln sowie vieler weiterer Aspekte machten technische Lösungen, wie z.B. Videokonferenzsysteme und die technische Realisierung der Arbeit an gemeinsamen Dokumenten jenseits des originalen Arbeitsplatzes notwendig. Hier wurde die Aufsichtsbehörde immer wieder für Beratungen angefragt. Natürlich blieben Meldungen von Datenpannen nicht aus. Zeitweise war dadurch mehr als die Hälfte der vorhandenen Arbeitskapazität der Aufsichtsbehörde gebunden.

Bedingt durch neue technische und technologische Lösungen bestand zu vielen Zeitpunkten die Gefahr der Einschränkung der gesetzlich garantierten Persönlichkeitsrechte. Dabei war auch für uns als Aufsichtsbehörde das spannungsgeladene Feld der gesetzlichen Anforderungen (z. B. Bestimmungen des Infektionsschutzgesetzes) einerseits und den gebotenen Einschränkungen mit Blick auf die körperliche Unversehrtheit der Mitarbeiter in den kirchlichen und diakonischen Dienststellen andererseits eine Herausforderung.

Die Entwicklung der Corona-Warn-App stellte einen solchen grundlegenden ausführlichen und damit aber auch langwierigen Prozess deutlich vor Augen.

Das überarbeitete kirchliche Datenschutzrecht (das Kirchengesetz der Evangelischen Kirche in Deutschland – DSG-EKD) im Einklang mit der Datenschutz-Grundverordnung der Europäischen Union hat sich bisher bewährt.

Die Aufsichtsbehörde des Datenschutzbeauftragten für Kirche und Diakonie hat sich im zurückliegenden Berichtszeitraum 2020 und 2021 auf allen Ebenen ihres gesetzlichen Auftrags weiterentwickelt und ihre Tätigkeit im Rahmen der bestehenden materiellen und personellen Ressourcen, systematisiert und gestaltet.

Schwerpunktmäßig stand, entsprechend den gesetzlichen Anforderungen des DSG-EKD, das große Aufgabenfeld der Beratung und Unterstützung der betrieblichen bzw. örtlichen Beauftragten für den Datenschutz verschiedenster Rechtsträger im Focus des Handelns.

Schulungen und Fortbildungen konnten im zurückliegenden Berichtszeitraum überwiegend digital vorbereitet und durchgeführt werden. Dies führte allerdings auch zu eingeschränkten Kontakten zu den jeweils verantwortlichen Personenkreisen für den Datenschutz in den Dienststellen unseres Aufsichtsbereiches.

Aufsichtsrechtlich wurden wir mit zahlreichen Meldungen von Verletzungen des Datenschutzes und Beschwerden betroffener Personen konfrontiert. Mit Blick auf Beanstandungen, die wir als Aufsichtsbehörde aussprechen mussten, gab es immer einen gesetzeskonformen und praktikablen Konsens mit den verantwortlichen Stellen.

Eine wichtige Aufgabe eines örtlichen/betrieblichen Datenschutzbeauftragten und ebenso der Aufsichtsbehörde ist die Anwaltschaft für die Betroffenen. In dieser Funktion wird unsere Aufsichtsbehörde zunehmend in Anspruch und wahrgenommen. Das spiegelt sich in zahlreichen E-Mail-Anfragen, Telefonaten und auch postalischen Anfragen und Beschwerden wider. In diesem Zusammenhang haben die zumeist aufwendigen Beratungen in den zurückliegenden Berichtsjahren stark zugenommen. Insbesondere im Bereich der Datenverarbeitung in Kindertageseinrichtungen und der verfassten Kirche sind diese Anfragen vermehrt aufgetreten.

Die von der Datenverarbeitung betroffenen Personen wenden sich vermehrt auch mit Beschwerden an die Aufsichtsbehörde. Allen an uns

gerichteten Beschwerden konnten wir im zurückliegenden Berichtzeitraum außergerichtlich abhelfen.

Leider ist in diesem Zusammenhang auch ein Trend festzustellen, der sich darin widerspiegelt, dass Problemstellungen des Datenschutzes dazu benutzt werden, um anderen Ansprüchen gegenüber der verantwortlichen Stelle Nachdruck zu verleihen. Sehr oft ist es deshalb nicht einfach, deutliche Grenzen zwischen den verschiedenen Rechtsgebieten zu ziehen, die sich einerseits im Bereich der Schweigepflicht, des Dienstrechts und der Geheimhaltung und andererseits der originären Problematik des Datenschutzes bewegen.

Das Urteil des Europäischen Gerichtshofes vom Juli 2020 (initiiert durch eine Klage des Rechtsanwaltes Max Schrems) befasste die Aufsichtsbehörde in den zurückliegenden beiden Jahren stark, war doch das Privacy-Shield-Abkommen der EU mit den USA mit sofortiger Wirkung für unwirksam erklärt worden.

Alle kirchlichen und diakonischen Stellen hatten ihre Verarbeitungen daraufhin zu überprüfen und mussten Lösungen erarbeiten und implementieren.

Auch wenn in den kirchlichen und diakonischen Stellen in der Regel mit den unterschiedlichsten Fachanwendungen gearbeitet wird, konzentrierten sich die Anfragen an die Aufsichtsbehörde nach Bekanntwerden des Urteils auf den Einsatz von Videokonferenzsystemen US-amerikanischer Anbieter und von Software und Diensten des Herstellers Microsoft.

Der Datenschutzbeauftragte für Kirche und Diakonie ist Mitglied in einem Arbeitskreis der Konferenz der Beauftragten für den Datenschutz in der EKD, wo zum Einsatz von Microsoft Anwendungen und Diensten Hinweise für die Praxis erarbeitet werden. Den vorläufigen Stand der internen Arbeit und Einschätzung unserer Behörde veröffentlichen wir in diesem Bericht mit einem eigenen Schwerpunkt.

Einen weiteren Schwerpunkt behandeln wir mit dem Thema Alexa, Siri & Co. Der zunehmende Einsatz dieser elektronischen, sprachgesteuerten „Helferlein“ stellt kirchliche und diakonische Stellen und insbesondere die in der Pflege tätigen Mitarbeiter vor besondere Herausforderungen, wenn die Überwachung möglich ist und auf einmal die zu pflegenden Menschen oder auch deren Angehörige zu verantwortlichen Personen im Sinne des geltenden Datenschutzrechts werden. Eine bereits 2021 für den Bereich der Diakonie Sachsen erstellte Handreichung wird mit diesem Bericht aktualisiert für den gesamten Zuständigkeitsbereich unserer Behörde veröffentlicht.

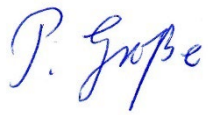
Die Aufsichtsbehörde hat im zurückliegenden Berichtszeitraum ein Datenschutz-Systemaudit in einer der großen Einrichtungen in ihrem Verantwortungsbereich durchgeführt. Im Rahmen eines begrenzten Systemaudits wurde die zum Prüfzeitpunkt etablierte Datenschutzorganisation und die Form der Umsetzung der Verarbeitungen personenbezogener Daten in jeweils spezifischen Arbeitsfeldern analysiert und geprüft. Im Ergebnis wurden Hinweise zur Verbesserung gegeben, die nun umgesetzt und durch unsere Behörde beratend begleitet werden.

Mit dem vorgelegten Tätigkeitsbericht will unsere Behörde den bisher vorgelegten 1. Tätigkeitsbericht weiterentwickeln und detailliert aufzeigen, wie sich die rechtskonforme Datenverarbeitung in unserem Aufsichtsbereich in den zurückliegenden Berichtsjahren weiterentwickelt hat.

Neu ist der Bereich der anonymisierten Darstellung der verschiedenen Praxisfelder.

Ich wünsche allen, die diesen Bericht lesen, eine fruchtbare Lektüre und viele wertvolle Impulse für ihre eigene Tätigkeit bei der personenbezogenen Datenverarbeitung.

Chemnitz im Juni 2022



Pierre Große

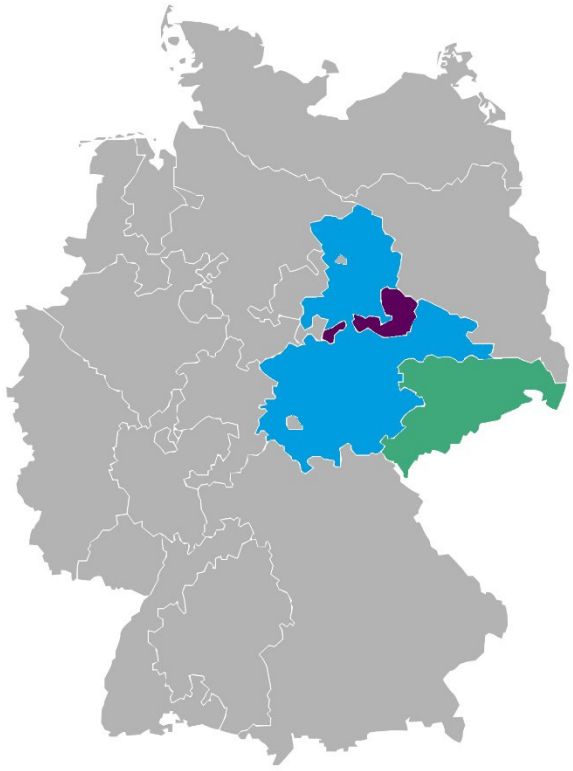
Der Datenschutzbeauftragte
für Kirche und Diakonie

Der Datenschutzbeauftragte als eine unabhängige Behörde für den Datenschutz in Kirche und Diakonie

Zuständigkeitsbereich

Der Datenschutzbeauftragte für Kirche und Diakonie, vertreten durch den behördlichen Beauftrgaten Herrn Pierre Große, ist die Aufsichtsbehörde für den Datenschutz für

- die Ev.-Luth. Landeskirche Sachsens
- das Diakonische Werk der Ev.-Luth. Landeskirche Sachsens e. V.
- die Evangelische Landeskirche Anhalts und
- das Diakonische Werk Evangelischer Kirchen in Mitteldeutschland e. V.



Zweck und Ziel der Datenschutzaufsicht

Die Aufsichtsbehörden haben nicht ausschließlich, jedoch insbesondere die einheitliche Anwendung und Durchsetzung des kirchlichen Datenschutzrechts im Zuständigkeitsbereich zu überwachen und sicherzustellen (§ 43 Abs. 1 DSG-EKD).

Die Erfahrungen aus unserer Arbeitspraxis zeigen, dass dies zu erreichen ist, wenn kirchliche Stellen aktiv ihre Verantwortung für den Schutz der Menschen mit ihren Rechten übernehmen.

Die erfolgreiche Praxis seit Beginn unserer Tätigkeit im Mai 2018 zeigt, dass die Zusammenarbeit kirchlicher Aufsichtsbehörden im Diskurs und im Rahmen der Datenschutzkonferenz förderlich ist beim Einsatz für den Datenschutz.

Sensibilisierung, Information und Beratung so viel wie möglich

Jede Verarbeitung personenbezogener Daten ist in der Logik des europäischen, des deutschen und nicht zuletzt auch des kirchlichen Rechts ein Grundrechtseingriff.

So formuliert das EKD-Datenschutzgesetz den Schutzweck in § 1 damit, „die einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird."

Der Datenschutzbeauftragte für Kirche und Diakonie will vornehmlich durch Sensibilisierung, Information und Beratung die Durchsetzung der geltenden Rechte unterstützen.

Kontrolle und Ausübung aufsichtsrechtlicher Befugnisse so viel wie nötig

Jede Verarbeitung personenbezogener Daten ist ein Risiko für die Rechte und Freiheiten von Menschen.

Die Folgen unsachgemäßer oder unrechtmäßiger Datenverarbeitung können von persönlichen Unannehmlichkeiten über Rufschädigung und Diskriminierung bis hin zu Gefahren für Leib und Leben reichen. Aufsichtstätigkeiten dienen einzig dazu, Betroffenen zu ihrem Recht zu verhelfen.

EU-Recht und kirchliches Recht sind Grundlage für die Praxis der Aufsicht

Der Anwendungsbereich europäischen Rechts

Wie Prof. Dr. Gernot Sydow, Herausgeber des im Jahr 2020 im Nomos Verlag erschienenen Handkommentars „Kirchliches Datenschutzrecht", in der Einführung erläutert, greift das kirchliche Datenschutzrecht, welches gemäß Art. 91 Abs. 1 DS-GVO „in Einklang" mit den Regelungen der DS-GVO gebracht wurde, soweit der Anwendungsbereich des Europäischen Unionsrechts eröffnet ist. Im Bereich der Diakonie erscheint dies mit Blick auf deren Aktivitäten unstrittig. Die Herausnahme und

Zulässigkeit eigenen kirchlichen Datenschutzrechts wurde mit Art. 91 DS-GVO europarechtlich verankert. Dennoch bleibt, so Prof. Sydow, eine richtlinienartige Bedeutung der DS-GVO zumindest für kirchliche Aktivitäten, die in den Kompetenzbereich der EU fallen.

Der (allein) kirchliche Anwendungsbereich

Bei der überwiegenden Anzahl von Verarbeitungen in der verfassten Kirche liegt keine EU-Regelungskompetenz vor. Das Recht der Mitgliedstaaten greift. Der deutsche Gesetzgeber verzichtet auf entsprechende Regelungen und überlässt es den Kirchen, auch den Datenschutz als eine eigene Angelegenheit im Rahmen des den Kirchen verfassungsrechtlich garantierten Rechts selbstständig zu ordnen und zu verwalten.

Diakonie gilt als Wesens- und Lebensäußerung der Kirche. In den Einrichtungen der Diakonie, wo der kirchliche Auftrag mit vielfältigen Aktivitäten für alle Menschen in einem weit verstandenen Sinn verwirklicht wird, ist Kirche. Dies gilt fortdauernd auch mit Kenntnis der Tatsache, dass nichtkirchliche Akteure in weitgehender Übereinstimmung gleiche Aktivitäten entfalten.

Kein Ermessensspielraum für die kirchlich konstituierten Aufsichtsbehörden

Die Anforderung in Art. 91 Abs. 2 DS-GVO verlangt für die Rechtmäßigkeit spezifischer (kirchlicher) Aufsichtsbehörden, dass für sie die in Kapitel VI DS-GVO niedergelegten Bedingungen erfüllt sind.

Für den allein kirchlichen Anwendungsbereich könnten die Kirchen eigene Aufsichtsbehörden mit einem je eigenen Regelungskatalog errichten. Im Bereich kirchlicher Aktivitäten, die (auch) der EU-Regelungskompetenz unterliegen, ist das nicht möglich. Art. 91 Abs. 2 DS-GVO ist hier eindeutig.

Unabhängigkeit der Datenschutzaufsicht

Das Erfordernis der völligen Unabhängigkeit (§ 40 Abs. 1 DSG-EKD, Art. 52 DS-GVO) von Aufsichtsbehörden für den Datenschutz ergibt sich, soziologisch und in der Folge politisch betrachtet, aus dem strukturellen Ungleichgewicht der Kräfte zwischen Organisationen, die Personendaten für ihre Zwecke verarbeiten wollen und den einzelnen Personen, in deren Grundrecht so eingegriffen wird. Die Verwendung des Wortes „völlige“ im Gesetzestext erscheint zunächst wie eine unnötige Betonung. Der Gesetzgeber hat damit jedoch jede irgendwie eingeschränkte Unabhängigkeit von vorneherein ausgeschlossen.

Aufsichtsbehörden sollen unabhängig vom Einfluss der sie errichtenden und finanzierenden Institutionen ihren Auftrag für alle Betroffenen in Kirche und Diakonie wahrnehmen können.

Aufsichtsbehörden gemäß DSG-EKD in den Landeskirchen der EKD

Das kirchliche Datenschutzrecht, wie es mit Zustimmung der Gliedkirchen der EKD beschlossen wurde, erlaubt es den Gliedkirchen und auch den gliedkirchlichen Zusammenschlüssen, jeweils eigene unabhängige Aufsichtsbehörden für ihren Bereich einzeln oder gemeinschaftlich zu errichten.

Damit berücksichtigt das Kirchengesetz die Verfasstheit der evangelischen Landeskirchen und der Evangelischen Kirche in Deutschland.

Das EKD-Datenschutzgesetz (DSG-EKD) gibt den Aufsichtsbehörden für den Datenschutz in § 44 DSG-EKD weitreichende Befugnisse, mittels Verwaltungsakt in Datenverarbeitungen durch kirchliche Stellen einzugreifen, wenn dies zur Durchsetzung des kirchlichen Datenschutzrechts erforderlich ist.

Diese gesetzlichen Befugnisse schließen ein, dass die Aufsichtsbehörden verlangen können, dass die verantwortlichen Stellen sie bei der Erfüllung ihrer Aufgaben unterstützen. So ist ihnen auf Verlangen Auskunft sowie Einsicht in alle Unterlagen und Akten über die Verarbeitung personenbezogener Daten zu geben. Weiterhin sind alle diesbezüglichen Informationen bereitzustellen, insbesondere über die gespeicherten Daten und über die eingesetzten Datenverarbeitungsprogramme. Ihnen ist jederzeit Zutritt zu allen Diensträumen, einschließlich aller Verarbeitungsanlagen und -geräte zu gewähren, um Untersuchungen und Überprüfungen vorzunehmen (§ 44 Abs. 1 Satz 1-3 DSG-EKD).

Dienst des Datenschutzbeauftragten für Kirche und Diakonie

Tätigkeit der Geschäftsstelle und der Referenten an ihren Arbeitsorten

In der Geschäftsstelle der Aufsichtsbehörde in Chemnitz sind neben dem regelmäßigen Arbeitsplatz des Beauftragten, der gleichzeitig Leiter der Behörde ist, weitere Arbeitsplätze für die Sachbearbeitung sowie die auswärtigen Referenten eingerichtet, wenn diese zu Beratungen zum Dienstsitz nach Chemnitz kommen. Die auswärtigen Referenten arbeiten regelmäßig in Leipzig und in Halle und an Orten zu vereinbarten Terminen.

Zur Sicherstellung der Verwaltungsordnung werden sämtliche Postein- und Postausgänge zentral über die Geschäftsstelle verwaltet. In der Geschäftsstelle laufen alle Vorgänge, mit denen sich die Aufsichtsbehörde befasst, zusammen. Die Akten werden in der Geschäftsstelle hybrid verwaltet. Das heißt, dass alle elektronisch eingehenden Vorgänge meist elektronisch weiterbearbeitet werden. Lediglich Dokumente, die aus rechtlichen Gründen eine Papierform zwingend erfordern, werden in Papierform vorgehalten.

Alle vom Datenschutzbeauftragten beaufsichtigten und beratenen kirchlichen Stellen werden über ein einheitliches Aktensystem verwaltet.

In der Geschäftsstelle finden interne Beratungen als auch Gespräche und Beratungen mit Vertretern aus kirchlichen Stellen statt. Die Geschäftsstelle ist die zentrale Anlaufstelle sowohl für Anfragende als auch für die Beratungen kirchlicher Stellen und für die Entgegennahme von Meldungen an die Aufsichtsbehörde, beispielsweise im Fall der gemäß Datenschutzgesetz meldepflichtigen Verletzungen des Datenschutzes.

Über die Geschäftsstelle erfolgt die Koordination aller Vorgänge entsprechend der jeweiligen Sachgebiete. Die Online-Kommunikation innerhalb der Aufsichtsbehörde zwischen der Geschäftsstelle und den Referenten an ihren Arbeitsorten als auch die Kommunikation im Fall der durch die Behörde organisierten Online-Termine, -Beratungen und -Veranstaltungen erfolgt über das Open-Source-Tool BigBlueButton.

Beratung, Weiterbildung, Aufsicht

Der gesetzliche Auftrag sieht im Kern die Überwachung und Sicherstellung der Einhaltung der rechtlichen Anforderungen des Datenschutzes durch kirchliche Stellen vor.

Beratung, Sensibilisierung, Information

Viele Anfragen im Berichtszeitraum betrafen den Umgang mit den sich anfangs fast wöchentlich ändernden Regeln zur Bekämpfung und Beherrschung der Corona-Pandemie. Dazu gehörten nicht zuletzt Anfragen im Zusammenhang mit digital unterstützter Kommunikation und Arbeit, z. B. im Homeoffice.

Die meisten Anfragen wurden einzelfallbezogen bearbeitet. Einige schwerpunktbezogene Anfragen flossen in die Erarbeitung von Handreichungen ein, wie beispielsweise zum datenschutzkonformen Einsatz von Online-Videokonferenzsystemen.

Aus- und Weiterbildung

Das Weiterbildungsangebot für örtliche Beauftragte für den Datenschutz konnte mit den Einschränkungen der Corona-Pandemie über fast den gesamten Berichtszeitraum nicht mehr in Präsenz stattfinden. Vermehrt wurde online in Formaten mit wenigen Teilnehmenden gearbeitet.

Die Weiterbildungsarbeit zum Datenschutz im Rahmen der Verwaltungsausbildung in der Ev.-Luth. Landeskirche Sachsens wurde ebenfalls online fortgesetzt.

Unterstützt wurde die Bildung eines überregionalen Erfahrungsaustauschkreises (Erfa-Kreis) über die Aktionsräume der Diakonie Sachsens, als auch der Diakonie Mitteldeutschlands hinweg. Dieser fand bisher auch nur online statt.

Aufsicht, Überwachung, Sicherstellung

Die aufsichtlichen Tätigkeiten erfolgten im Berichtszeitraum überwiegend anlassbezogen auf Basis eingegangener Beschwerden von Betroffenen und Meldungen über Datenschutzverletzungen.

Einen vergleichsweise großen zeitlichen Umfang nahm die erstmalige umfassendere Prüfung einer zentralen kirchlichen Stelle mittels eines Datenschutz-Systemaudits ein, worauf im nächsten Abschnitt näher eingegangen wird.

Erstes Datenschutz-Systemaudit durch die Aufsichtsbehörde in einer zentralen kirchlichen Stelle

Im Zeitraum von Februar 2021 bis Februar 2022, hat die Aufsichtsbehörde in einer der verantwortlichen kirchlichen Stellen in ihrem Zuständigkeitsbereich ein Datenschutz-Systemaudit durchgeführt.

Die Entscheidung für ein Audit als Systemaudit hatte zum Ziel, den Status des Datenschutzniveaus der betrachteten Bereiche zu ermitteln.

§ 43 Abs. 1 DSG-EKD „Überwachen“

Diese Kernaufgabe der Datenschutzaufsicht wurde in der auditierten kirchlichen Stelle durch Sichten und Prüfen von Dokumenten einschließlich Webseiten, durch Kontrollieren des Ablaufs und der Wirksamkeit von Verfahren und Maßnahmen, die dem Datenschutz dienen sollen, sowie durch Befragen von Mitarbeitern der verantwortlichen Stelle zur Kontrolle des Wissenstands und des Grades ihrer Sensibilität für den Datenschutz in ihrem Wirkungskreis und den mit ihren Aufgaben verbundenen Tätigkeiten durchgeführt.

Überwachen durch die Aufsichtsbehörde bedeutete in dem Datenschutz-Systemaudit konkret:

- Anlasslose Kontrollen durch Stichproben, um Verarbeitungen und Vorgänge zu betrachten, die in Dokumenten unterrepräsentiert sind
- Anlassbezogene Kontrollen mit dem Fokus auf gemeldete Fälle, die Verletzungen des gesetzlich garantieren Schutzes des Persönlichkeitsrechts Betroffener darstellen könnten
- Kontrolle der Fähigkeit, die gesetzliche Rechenschaftspflicht zu erfüllen:
  - gem. § 5 Abs. 2 DSG-EKD über die Einhaltung der Grundsätze,
  - gem. § 11 Abs. 1 DSG-EKD über den Nachweis gültiger Einwilligungen,
  - gem. § 27 Abs. 1 DSG-EKD über den Nachweis angemessener technisch-organisatorischer Maßnahmen,
  - gem. § 34 Abs. 4 Nr. 4 DSG-EKD mittels Datenschutz-Folgenabschätzungen.

§ 43 Abs. 1 DSG-EKD „Sicherstellen“

Diese Kernaufgabe der Datenschutzaufsicht, wie sie im durchgeführten Audit wahrgenommen wurde, schließt neben den notwendigen Hinweisen zur Verbesserung oder der Herstellung eines datenschutzkonformen Zustandes insbesondere die Ausübung der Befugnisse gem. § 44 Abs. 1 – 3 DSG-EKD ein, beginnend mit der schriftlichen Ankündigung des Datenschutz-Systemaudits:

- Verlangen der Unterstützung sowie der Auskunft und die Einsichtnahme in alle oder ausgewählte Unterlagen und Akten mit personenbezogenen Daten und der Informationsbereitstellung über gespeicherte Daten mit personenbezogenen Daten und über eingesetzte Programme zur Datenverarbeitung,
- Zutritt zu allen Diensträumen und zu allen Verarbeitungsanlagen /-geräten,
- Beanstandung einer Verarbeitung, sobald die Aufsichtsbehörde Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei einer Verarbeitung feststellt,
- Aufforderung zur Stellungnahme.

„Sicherstellen“ im Sinne des Gesetzes schließt Anordnungen durch Verwaltungsakt ein, um

- eine Verarbeitung in Einklang mit dem Gesetz zu bringen,
- eine Verarbeitung vorübergehend oder dauerhaft zu beschränken oder zu unterlassen,
- die Übermittlung in Länder ohne ausreichendes Datenschutzniveau angemessen abzusichern oder zu unterlassen,
- personenbezogene Daten zu berichtigen, zu sperren oder zu löschen,
- die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen.

§ 43 Abs. 2 DSG-EKD „Sensibilisieren, Informieren und Beraten“

Während des Audits wurden die Mitglieder der Leitung als auch Mitarbeiter der auditierten Stelle sensibilisiert, informiert und beraten.

Mit der gesetzlichen Regelung in § 43 DSG-EKD hat

der kirchliche Gesetzgeber die Aufgaben kirchlicher Aufsichtsbehörden deutlich ausgeweitet im Vergleich zu den gesetzlichen Aufgaben der staatlichen Aufsichtsbehörden gemäß DS-GVO. Unter strenger Abwägung könnte dadurch die Gefahr von Interessenkonflikten bis hin zu einer Gefährdung der Unabhängigkeit der kirchlichen Aufsichtsbehörden entstehen.

Die Sensibilisierung, Information und Beratung der kirchlichen Öffentlichkeit, der verantwortlichen Stellen und der kirchlichen Auftragsverarbeiter stellt auch unsere Aufsichtsbehörde ganz praktisch vor nicht geringer werdende Herausforderungen.

§ 43 Abs. 2 DSG-EKD „Unterrichten von Betroffenen“

Während des Audits wurden insbesondere Mitarbeiter als Betroffene über ihre Rechte und über eigene Möglichkeiten, den Datenschutz am Arbeitsplatz zu unterstützen und sicherzustellen, unterrichtet.

§ 43 Abs. 3 DSG-EKD „Schulen und Fortbilden örtlich Beauftragter“

Der örtlich Beauftragte für den Datenschutz war auf Seiten der verantwortlichen kirchlichen Stelle Teil bzw. Mitglied des sogenannten Audit-Teams.

Es ergab sich als ein praxisnaher Nebeneffekt, dass der örtlich Beauftragte im Zuge des nicht von ihm selbst verantworteten Audits in vielfältiger Weise seine Fähigkeiten im eigenen Zuständigkeitsbereich prüfen und erweitern konnte.

§ 43 Abs. 4 DSG-EKD „Prüfen von Verarbeitung“

Im Zuge der Interviews mit Mitarbeitern der auditierten Stelle wurden ungeregelte Verarbeitungen personenbezogener Daten in Drittländern, zu denen es keine dokumentierte Behandlung der damit verbundenen rechtlichen Anforderungen gab, erkannt und beanstandet. Entsprechende Hinweise wurden gegeben.

Die fortgesetzte Nichtbehandlung kann als Folge die Anordnung zur vorübergehenden oder dauerhaften Unterlassung der Verarbeitungen nach sich ziehen.

Das erste Datenschutz-Systemaudit hat während der Durchführung und in den Ergebnissen frühere Einschätzungen des Datenschutzbeauftragten für Kirche und Diakonie bestätigt, dass „noch viel zu tun ist“, um Datenschutz in den kirchlichen Stellen systematisiert zu verankern, damit er als Teil des kirchlichen Auftrags einen Beitrag leisten kann.

Fazit zur Arbeit der Aufsichtsbehörde im Berichtszeitraum

Die Aufsichtsbehörde für den Datenschutz hat in den Jahren 2020/2021 ihren gesetzlichen Auftrag im Rahmen der bereitgestellten Mittel erfüllt.

Diese Mittel sind im Wesentlichen die personellen Planstellen und hinreichende Sachmittel im Rahmen eines eigenen Haushaltstitels. Mit einer höheren personellen Ausstattung kann auch die Aufgabenerfüllung weiter verbessert werden.

Auf den nächsten Seiten des hier vorgelegten Berichts sind ausgewählte Arbeitsbereiche und Arbeitsergebnisse unserer Aufsichtsbehörde, von der themenübergreifenden Gremienarbeit bis hin zu einer Auswahl von aufsichtsrelevanten Einzelfragen im zurückliegenden Berichtszeitraum dargestellt.

Gremien, Arbeitskreise, Projekte

Konferenz der unabhängigen Aufsichtsbehörden für den Datenschutz in den Gliedkirchen der EKD

Der Datenschutzbeauftragte für Kirche und Diakonie ist eine durch Kirchengesetz der Ev.-Luth. Landeskirche Sachsens errichtete unabhängige Aufsichtsbehörde für den Datenschutz gemäß dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD).

Aufsichtsbehörden für den Datenschutz sind mit dem Ziel der einheitlichen Anwendung und Durchsetzung des kirchlichen Datenschutzrechts ohne Einschränkung ihrer Unabhängigkeit auch zur Zusammenarbeit und Abstimmung untereinander und über Bereichsgrenzen hinweg verpflichtet.

In § 43 Abs. 9 DSG-EKD heißt es dazu im Wortlaut: "*Die Beauftragten für den Datenschutz arbeiten zusammen und bilden eine Datenschutzkonferenz, auf der gemeinsame Stellungnahmen und Handreichungen zu Datenschutz- und Kohärenzfragen beschlossen werden können. Sie tauschen mit allen Aufsichtsbehörden für den Datenschutz Erfahrungen und zweckdienliche Informationen aus und geben im Bedarfsfall Stellungnahmen ab.*"

Der Datenschutzbeauftragte für Kirche und Diakonie ist Mitglied der Konferenz der Aufsichtsbehörden für den Datenschutz in den Landeskirchen und der EKD.

Weitere Mitglieder der Datenschutzkonferenz sind (Stand 31.12.2021):

- Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland, vertreten durch Herrn Oberkirchenrat Michael Jacob
- Der Datenschutzbeauftragte für die Nordkirche, vertreten durch Herrn RA Peter von Loeper
- Die Beauftragte für den Datenschutz der Evangelischen Kirche der Pfalz, vertreten durch die Landeskirchenrätin Pia Schneider

Die Anzahl unabhängiger Aufsichtsbehörden für den Datenschutz wird in den kommenden Jahren voraussichtlich weiter sinken, nachdem die Nordkirche als auch die Evangelische Kirche der Pfalz eine Übertragung der Aufgaben und Befugnisse der Datenschutzaufsicht an die Aufsichtsbehörde der EKD beschlossen haben.

Hingegen sind im Bereich der Katholischen Kirche in Deutschland insgesamt fünf unabhängige Aufsichtsbehörden für den Datenschutz etabliert.

Zusammenarbeit, Konferenz, Kohärenz sowie ökumenischer Austausch

Die Beauftragten der Aufsichtsbehörden in der EKD haben den Auftrag zur Zusammenarbeit.

Der Beauftragte für den Datenschutz in Kirche und Diakonie pflegt diese im Rahmen der Konferenz durch Abstimmung zu Themen mit Relevanz für alle Gliedkirchen und Werke in der EKD.

In der Erarbeitung gemeinsamer Stellungnahmen als auch im Rahmen der Rechtsgespräche, welche die Konferenz zusammen mit dem Kirchenamt der EKD pflegt, wird die Anforderung der Kohärenz in der einheitlichen Auslegung und Anwendung des kirchlichen Datenschutzrechts angestrebt.

Über diese innerkirchliche Zusammenarbeit hinaus pflegen die Aufsichtsbehörden in der EKD den Erfahrungsaustausch mit der Konferenz der fünf Diözesandatenschutzbeauftragten in der Katholischen Kirche in Deutschland.

Beschlüsse und Entschließungen der Datenschutzkonferenz

24.07.2020: Gemeinsame Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zum „Schrems II"-Urteil des EuGH vom 16.07.2020

Die Beauftragten für den Datenschutz in der EKD äußern sich anlässlich der Entscheidung „Schrems II" des EuGH, mit der der Beschluss 2016/1250 der EU-Kommission über die Angemessenheit des vom EU-US Privacy Shield gebotenen Schutzes für ungültig erklärt wird.

Link: https://dsbkd.de/dsk-ekd-20200724/

21.04.2021: Evangelische und katholische Datenschutzaufsichtsbehörden veröffentlichen „Kirchliches Datenschutzmodell".

Auf dem ökumenischen Datenschutztag der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche in Deutschland und der Konferenz der Beauftragten für den Datenschutz in

der EKD am 21. April 2021 wurde das Kirchliche Datenschutzmodell (KDM) verabschiedet.

Link: https://dsbkd.de/dsk-ekd-20210430/

15.10.2021 Gemeinsame Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zur Datenübermittlung in die USA

In Ergänzung zur Gemeinsamen Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zum „Schrems II"-Urteil des EuGH vom 16. Juli 2020 werden in dieser Stellungnahme die Entwicklung sowie die rechtlichen Grundlagen bei der Übermittlung personenbezogener Daten in die USA erläutert.

Link: https://dsbkd.de/dsk-ekd-20211015/

Arbeitskreis Rechtsgespräch

In Zusammenarbeit mit dem Kirchenamt der EKD, hier vertreten durch den juristischen Referenten für Datenschutz und weitere Sachgebiete findet mit den Mitgliedern der Konferenz der unabhängigen Aufsichtsbehörden für den Datenschutz ein bis zweimal im Jahr ein Fachaustausch in Form eines Rechtsgesprächs statt.

Gegenstand der Rechtsgespräche sind sowohl Aspekte und Fragen der Datenschutzgesetzgebung, als auch der Austausch zur Rechtsprechung zu datenschutzrechtlichen Fällen.

Ein Schwerpunkt der Rechtsgespräche in den Jahren 2020 und 2021 waren rechtliche Fragestellungen im Blick und Vorgriff auf die beginnende Evaluierung des EKD-Datenschutzgesetzes.

Arbeitskreis Microsoft

Im Zuge der veröffentlichten Stellungnahme zur Datenübermittlung in die USA beschloss die Konferenz eine Arbeitsgruppe einzurichten, die sich mit konkreten datenschutzrelevanten Aspekten eines Einsatzes von Microsoft Software und -technologien in Kirche und Diakonie beschäftigt.

Ziel ist es, eine Handreichung zu veröffentlichen. Die Handreichung soll und wird dabei auch die dann vorliegenden Ergebnisse der Arbeitsgruppe Microsoft-Onlinedienste der DSK unter den geltenden rechtlichen Bedingungen gemäß DSG-EKD berücksichtigen.

Gutachterausschuss der EKD

Mitarbeiter der Behörde sind als Mitglieder des Gutachterausschusses der EKD tätig. Sie sind an der Durchführung von Lieferantenaudits unter den Prämissen des Qualitätsmanagements, unter besonderer Beachtung kirchlicher und diakonischer Anforderungen, beteiligt. Wichtiger Teil des Anforderungskatalogs sind Aspekte von Datenschutz und Datensicherheit.

Der Auftrag des Gutachterausschusses besteht darin, mittels der Audits die Leistungsfähigkeit der Lieferanten zu prüfen und Hinweise zur stetigen Verbesserung zu geben. Regelmäßig finden neben den eigentlichen Lieferantenaudits entsprechende Arbeitstreffen des Gutachterausschusses statt, im Berichtszeitraum bedingt durch die Regelungen zur Pandemiebekämpfung nur online.

Erkennbar wichtig wird diese Mitarbeit im Blick auf Entwicklungen, wie sie sich derzeit rund um das neue kirchliche Gemeindegliederprogramm "Meldewesen 5.0" abzeichnen.

Relevanz von Datenschutz und Datensicherheit für das kirchliche „Meldewesen 5.0"

Durch und in Zusammenarbeit mit Dienstleistern wird eine hoch integrierte, cloud-basierte IT-Architektur zur schrittweisen Ablösung bzw. Überführung der bisherigen Systeme und Arbeitsweisen im Bereich des kirchlichen Meldewesens geplant und entwickelt. Die Architektur wird flexibel die Verbindung zu den gliedkirchlichen IT-Systemen ermöglichen und soll über ein Service-Portal die Verwaltung von Nutzern mit Rollen und Berechtigungen bis hin zu einer durchgehenden „Einmal-Anmelden-Lösung" (Single-Sign-On) anbieten. Darüber hinaus eröffnen sich Perspektiven bis hin zu umfassenden Verwaltungsfunktionen auf den verschiedenen organisatorischen Ebenen in den Gliedkirchen.

Damit ergeben sich neue Herausforderungen zum Datenschutz und zur Datensicherheit.

Anwender aus den Landeskirchen sind an der Erarbeitung der Fachanwendungen und -prozesse beteiligt, prüfen, überwachen und helfen diese zu verbessern. IT-Spezialisten der Dienstleister in den Gliedkirchen schaffen die Funktionsfähigkeit und stellen die Sicherheit der Systemarchitektur, sowie

deren Aufbau und Betrieb sicher.

Es braucht zusätzlich die systematische Einbeziehung von Experten, um die rechtlichen Anforderungen des Datenschutzes angemessen zu berücksichtigen. Empfohlen wird die Anwendung des Kirchlichen Datenschutzmodells.

Ökumenische Projektgruppe Kirchliches Datenschutzmodell

Das von einer ökumenischen Projektgruppe erarbeitete Kirchliche Datenschutzmodell (KDM) will – basierend auf dem Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – geeignete Mechanismen anbieten, um die Anforderungen der Datenschutzgesetze in technische und organisatorische Maßnahmen zu überführen.

Mit dem KDM wird eine Methode bereitgestellt, mit der die Risiken für die Rechte und Freiheiten natürlicher Personen mit Hilfe von geeigneten technischen und organisatorischen Maßnahmen beseitigt oder reduziert werden können.

Mitglieder der Datenschutzaufsichtsbehörde arbeiten seit Beginn mit und leiten beispielsweise die Unterarbeitsgruppe Fallbeispiel KDM.

L: https://www.kirchliches-datenschutzmodell.de

Ev.-Luth. Landeskirche Sachsens

- Beratungen mit dem Dezernat V Finanzen und Vermögen, dem auch das Rechtsgebiet Datenschutz zugeordnet ist
- Beratungen und Fortbildungen mit den Datenschutzbeauftragten in den Regional-kirchenämtern

Evangelische Kirche in Mitteldeutschland (EKM)

- Beratung mit dem Referat Allgemeines Recht des Landeskirchenamtes zur geplanten Durchführungsverordnung zum DSG-EKD
- Gemeinsame Schulungsveranstaltung für Qualitätsmanagementbeauftragte in der Diakonie Mitteldeutschland zusammen mit dem Referat Allgemeines Recht
- Austausch zur Änderung und Ergänzung des EKD-Datenschutzgesetzes (DSG-EKD) zur Ermöglichung der institutionellen Aufarbeitung sexualisierter Gewalt

Evangelische Landeskirche Anhalts

- Beratungen zu Datenschutzfragen mit dem Landeskirchenrat
- Fortbildung des Datenschutzbeauftragten

Diakonie Mitteldeutschland

- Beratung / Unterstützung des Qualitätszirkels Kita im Hinblick auf das Verzeichnis der Verarbeitungstätigkeiten für Kitas der Diakonie
- Zusammenarbeit bei Vorbereitung und Durchführung von Schulungen und Beratungen
- Beratung und Austausch im Hinblick auf die Aufgaben und Ausstattung der Aufsichtsbehörde mit der kaufmännischen Vorständin und der Leitung des Bereichs Wirtschaft, Finanzen, Recht

Diakonie Sachsen

- Übergabe des letzten Praxisberichtes 2018-2020 und der Aufgaben der ehemaligen Referentin für den Datenschutz im Diakonischen Amt
- Abstimmungen und gemeinsame Beratungen zu dem bereits länger laufenden Projekt e-Kita der Landeshauptstadt Dresden
- Zusammenarbeit mit dem örtlichen Datenschutzbeauftragten der Geschäftsstelle zur Initiierung eines Erfahrungsaustauschkreises für die Mitglieder der beiden Diakonischen Werke im Zuständigkeitsbereich unserer Aufsichtsbehörde.

Schwerpunktthema Microsoft

Das Schwerpunktthema wurde gewählt, weil die Aufsichtsbehörde im Berichtszeitraum häufig Anfragen erreicht haben, die den gesetzlichen Beratungsauftrag der Behörde nutzen wollten, um eine Zulässigkeitserklärung oder Duldung des Einsatzes bestimmter Technologien oder Anwendungen mit Verweis auf Anforderungen der Digitalisierung und „moderner“ Arbeitsweisen zu erreichen. Die meisten dieser Anfragen wurden zum Einsatz von Microsoft Office gestellt.

Einsatz der Software und Dienste von Microsoft in Kirche und Diakonie

Ist Microsoft Office „von Haus aus“ schon datenschutzkonform?

Die Antwort ist nein. So manchem Fragesteller fehlt das Wissen, dass nicht eine Technologie oder eine bestimmte Anwendung aus Sicht der kirchlichen bzw. diakonischen Stelle als „datenschutzkonform“ bestätigt werden kann, auch wenn Werbeaussagen dies so darstellen. Es kommt einzig darauf an, für jede konkrete Verarbeitung von Personendaten die Konformität mit den rechtlichen Anforderungen des Datenschutzes für diese Verarbeitung zu prüfen.

Software und Dienste von Microsoft als Hilfsmittel zur Durchführung von Verarbeitungstätigkeiten sind wie alle anderen IT-Produkte auch vor der Übernahme in die produktive Nutzung immer für ihren geplanten Einsatzzweck im Blick auf die zu verarbeitenden Datenkategorien dokumentiert zu prüfen, und zwar im Rahmen eines geordneten Verfahrens zur Software- oder Dienstfreigabe.

Umfang der Prüfungen

Die geplanten Verarbeitungstätigkeiten und im Besonderen die Arten bzw. Kategorien der zu verarbeitenden Daten bestimmen die konkreten Anforderungen. (vgl. §§ 4, 13, 14 DSG-EKD)

Das Verarbeiten von persönlichen Daten mit hohem Schutzbedarf, beispielsweise während einer Sucht- oder Schuldnerberatung mittels Videokonferenz-Software einschließlich dem Austausch von Dokumenten mit Gesundheitsdaten oder Daten zu persönlichen finanziellen Verhältnissen, ist anders zu beurteilen und zu gestalten als das Verarbeiten von Personendaten mit normalem Schutzbedarf in der Geschäftspost.

Können Zertifikate eigene Prüfungen ersetzen?

Es kommt darauf an, was zertifiziert wurde. Gemäß § 35 DSG-EKD können kirchliche bzw. diakonische Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch geeignete Stellen prüfen und bewerten lassen. Dies kann auch die Nutzung von Microsoft Software und Diensten für konkret beschriebene Verarbeitungssituationen unter Berücksichtigung der datenschutzrechtlichen Anforderungen beinhalten.

Die von Microsoft angegebenen umfangreichen Zertifizierungen können nicht die eigenen internen Prüfungen oder die genannte Zertifizierung nach § 35 DSG-EKD ersetzen, die den Fokus auf die konkreten Verarbeitungsvorgänge in der jeweiligen kirchlichen Stelle legen müssen.

Interne Dokumentation zum Nachweis des datenschutzkonformen Einsatzes von Microsoft Software und Diensten (§ 5 Abs. 2 DSG-EKD)

- Ergänzung des Verarbeitungsverzeichnisses um Aspekte der verwendeten Mittel (z.B. MS-Office)

Zu dem Verzeichnis von Verarbeitungstätigkeiten gemäß § 31 DSG-EKD sollte, nicht beschränkt auf Microsoft Software und Dienste, zusätzlich dokumentiert werden, mittels welcher Anwendungen und Dienste sowie IT-Systeme die im Verzeichnis dokumentierten Verarbeitungen durchgeführt werden. Ausreichend wäre dafür auch ein Link oder Verweis zu diesen Informationen in einer umfassenden IT-Systemdokumentation.

- Dokumentierte Risikoanalysen

Interne Bereiche der kirchlichen bzw. diakonischen Stellen und die Aufsichtsbehörde sind Adressaten für die Datenschutzdokumentation. Deshalb müssen alle Informationen zu den Maßnahmen, die im Ergebnis der durchgeführten Risikoanalysen umgesetzt werden, an die relevanten Mitarbeiter und sonstigen Personen weitergegeben werden, z. B. Richtlinien, Anleitungen und Schulungen. Dabei ist durch das Datenschutzmanagment zu gewährleisten, dass diese Informationen dauerhaft, also auch bei einem Wechsel von Zuständigkeiten in der Organisation verankert bleiben sowie wiederholt geschult und gelebt werden.

Jede Microsoft Anwendung und jeder Dienst ist grundsätzlich einsetzbar

Grundsätzlich bedeutet, Ausnahmen sind möglich.

Es gehört nicht, wie manche Fragesteller irrtümlich vermuten, zu unseren gesetzlichen Aufgaben die Nutzung bestimmter Geräte, Anwendungen oder Dienste, wie denen von Microsoft, pauschal zu erlauben oder zu untersagen. Den Einsatz entscheiden zunächst allein die gesetzlichen Vertreter der kirchlichen bzw. diakonischen Stellen.

Die Aufsichtsbehörde schließt keine Software und keinen Dienst von Microsoft oder anderen Herstellern aus. Vielmehr geben wir Hinweise und verweisen zusätzlich auf Erkenntnisse und Hinweise anderer Fachleute und Aufsichtsbehörden in Deutschland und in Europa.

So hat 2021 beispielsweise der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg nach Prüfung einer speziell für den schulischen Einsatz konfigurierten Microsoft 365-Umgebung zusammen mit Microsoft im Ergebnis feststellen müssen, dass die Schulen mit hoher Wahrscheinlichkeit nicht in der Lage sind, Microsoft 365 datenschutzkonform einzusetzen.

Im Falle von Beschwerden seitens Eltern oder Schülern werden die Schulen durch die Aufsichtsbehörde aufgefordert, den Nachweis für einen datenschutzkonformen Einsatz zu erbringen. Nicht allein für Schulen wird empfohlen, auf tragfähige und rechtssichere Lösungen zu setzen.

Verantwortliche Stellen müssen rechtskonform agieren und den Verarbeitungen von Datenkategorien gemäß § 13 i. V. m. § 4 Abs. 1 Nr. 2 DSG-EKD besondere Aufmerksamkeit widmen, z. B. bei der Verarbeitung der Daten von Kindern oder der Gesundheitsdaten von Patienten und Klienten.

Jeglicher Einsatz ist bei der Planung immer aus der Perspektive Betroffener zu prüfen. Die Prüfung ist vorlagefähig zu dokumentieren.

Als Betroffene sind insbesondere alle Mitarbeiter der kirchlichen und diakonischen Stellen zu berücksichtigen, deren Daten zur Durchführung des Dienstverhältnisses verarbeitet werden. Möglichkeiten und Grenzen der Verarbeitung ihrer Daten stehen unter den Regelungen des § 49 DSG-EKD. Die Mitarbeitervertretung ist in jedem Fall einzubeziehen und anzuhören und, soweit vom Gesetzgeber vorgesehen, um die erforderliche Zustimmung zu ersuchen, wenn die Möglichkeit der Überwachung der Arbeitsweise und -leistung nicht sicher auszuschließen ist.

Allgemeine Hinweise

Der Einsatz von Microsoft Software ist nicht alternativlos. Alternativen sollen mindestens als Teil des IT-Notfallmanagements und einer „Exit-Strategie“ in die Prüfungen für eine souveräne IT-Landschaft einbezogen werden. Die Erfahrungen der jüngsten Geschichte zeigen, dass politische Entscheidungen die Verfügbarkeit von Ressourcen beeinträchtigen können. Das kann auch für IT-Ressourcen aus der „Wolke“ Wirklichkeit werden.

Auszuwählende Software und Dienste müssen geeignet sein, die Ziele des Datenschutzes und der Datensicherheit zu erfüllen. Kriterien für die Auswahl geeigneter Schutzmaßnahmen liefert das Kirchliche Datenschutzmodell (KDM).

Für alle Verarbeitungen sind Risikoanalysen und ggf. Datenschutz-Folgenabschätzungen gemäß § 34 DSG-EKD durchzuführen und zu dokumentieren.

Auswahl von Microsoft Software und Diensten nach Erforderlichkeit und Beherrschbarkeit

Die Erforderlichkeit ergibt sich aus der gewählten Form der zulässigen Verarbeitung.

Die Beherrschbarkeit ist das Resultat aus den hinreichend vorhandenen personellen Ressourcen.

Wann der Einsatz von M365 unmöglich ist

Insbesondere zwei interne Prüfergebnisse müssen zu der Konsequenz führen, dass der Einsatz komplexer Software und Dienste wie M365 nur eingeschränkt oder nicht möglich ist:

1. Fehlende personelle und finanzielle Ressourcen für die anfängliche und dann fortwährend gepflegte und dokumentierte Planung, Implementierung, Administration und Schulung
2. Fehlende Kapazitäten für die Erfüllung der Rechenschaftspflicht für den rechtskonformen Einsatz gemäß den Datenschutzanforderungen und den Anforderungen des (kirchlichen) Arbeits- und Mitbestimmungsrechts

Hinweise zu Microsoft Windows

Der Einsatz des Betriebssystems „Windows“ steht unter folgenden Mindestanforderungen:

- einsetzbar als Windows 10 oder 11 bis zum Ende des Supports mit Sicherheits-Updates,
- berücksichtigen der BSI-Empfehlungen zu Systemintegrität, Protokollierung, Härtung und Sicherheit (in Win 11 entsprechend anwenden),
- grundsätzlich Einsatz der Enterprise-Versionen in allen kirchlichen bzw. diakonischen Stellen (Education im Bereich Bildung) mit Bitlocker-Verschlüsselung aller Geräte und Telemetrie-Level „Security“ oder vergleichbar (Ausnahme für kleine Einrichtungen: Pro-Version mit Bitlocker-Verschlüsselung aller Geräte und manuelle Telemetrie-Einschränkung),
- Windows 365 (Cloud-PC) Einsatz nur mit Sicherstellung o. g. Anforderungen; Sinngemäß Gleiches gilt für Cloud-PCs anderer Hersteller.

Hinweise zu Microsoft Office ohne Cloud

Microsoft Office sollte als on-Premise Version eingesetzt werden, wenn keine Erforderlichkeit oder administrative Beherrschbarkeit für cloud-typische Funktionalitäten besteht und Sicherheitsanforderungen durch den Einsatz von Zusatzsoftware erfüllt werden. Beispiel: Die betriebsinterne Zusammenarbeit an Dokumenten kann on-Premise, also ohne Cloud innerhalb der lokalen Netzwerkumgebung ermöglicht werden.

Gestuft ist u. a. folgendes möglich:

- Office 2019/2021 lokal mit nur on-Premise Diensten. Wichtig: Cloud-Dienste für die automatisierte Sprachübersetzung von E-Mail und Dokumenten oder für das Erhalten von Design-Vorschlägen sind deaktiviert, weil diese Dienste die Dokumentinhalte „lesen“ können müssen, um zu funktionieren. Das gilt insbesondere für Datenverarbeitungen durch Berufsgeheimnisträger.
- Office 2019/2021 einsetzbar wie oben und mit Windows Server on-Premise für das lokale Active Directory sowie für die Datenablage und weitere Server-Anwendungen, wie Exchange oder SharePoint (beide on-Premise)
- Office 2019/2021 mit nicht-Microsoft Diensten wie z.B. einem alternativem Mail-Server oder Groupware-Lösung wie Open Xchange o. a.

Hinweise zu Microsoft Office mit Cloud

Das Thema „Drittlandübertragung“ ist relevant. Sicherzustellen ist, dass Personendaten in allen Verarbeitungszuständen nicht unbefugt von Dritten zur Kenntnis genommen werden können. Zu den Standardvertragsklauseln der EU-Kommission sind ggf. Zusatzmaßnahmen umzusetzen.

Die Datenspeicherorte als auch die Verarbeitungen „in transit“ in Deutschland oder Europa sind allein kein hinreichendes Kriterium für den Datenschutz. Solange die Bedingungen des § 10 DSG-EKD nicht erfüllt werden können und die Gesetzeslage im Drittland einen aus europäischer oder deutscher Sicht unzulässigen Zugriff prinzipiell ermöglicht, kann Microsoft Office in Verbindung mit den Microsoft Cloud-Diensten nur verwendet werden, wenn wirksame Zusatzmaßnahmen die potenziell möglichen Zugriffe verhindern, z. B. durch geeignete Verschlüsselungsmethoden.

Das Gesagte gilt für

- Office 2019/2021 mit Microsoft Cloud-Diensten (Exchange Online als Mail-Server, OneDrive for Business, Teams, SharePoint Online u. a. m.)
- Microsoft 365 in allen Versionen

Zusammenfassung

Das Angebot der Hersteller ist international. So erstellt und vermarktet Microsoft seine Produkte in einem weltweiten Kontext. Dementsprechend stellt die Fülle an Möglichkeiten zum produktiven Einsatz große Herausforderungen an die Verantwortlichen, diese Möglichkeiten auf das zulässige Maß einzuschränken und vor allem nur im erforderlichen Umfang einzusetzen.

Microsoft hat mit seinen Technologien und Produkten einen Verbreitungsgrad erreicht, der in vielen kirchlichen und diakonischen Stellen zu dem Fehlschluss führen kann, dass es für die Erfüllung des kirchlichen/diakonischen Auftrages und der damit verbundenen Aufgaben und Tätigkeiten keine oder kaum vergleichbare Alternativen gäbe.

Kirchliche bzw. diakonische Stelle sollen nur solche Hilfmittel einsetzen, womit zielführend, sicher und rechtskonform gearbeitet werden kann.

Schwerpunktthema Alexa, Siri & Co.

Gegenstand ist der Einsatz digitaler Assistenten mit Spracherkennung durch oder bei zu pflegenden Menschen im privaten häuslichen Umfeld oder in den Einrichtungen von Kirche und Diakonie.

Die Entscheidung, dieses Schwerpunktthema auszuwählen, ist der zunehmenden Relevanz des Themas geschuldet. Bereits 2020 wurden erste Anfragen aus dem Bereich des Diakonischen Werkes Sachsens an die Aufsichtsbehörde gerichtet. In der Folge bis heute kamen und kommen weitere Anfragen auch aus dem Bereich der Diakonie Mitteldeutschland hinzu.

Aus diesem Grund stellen wir die Einschätzung des Datenschutzbeauftragten für Kirche und Diakonie als Schwerpunktthema hier noch einmal für alle interessierten bzw. betroffenen Stellen dar.

Sprachassistenten im (Pflege-)Alltag

Vorzüge moderner Technik

Sprachassistenten wie Alexa, Siri & Co. stellen für immer mehr Menschen eine selbstverständliche Unterstützung im Alltag dar. Die Erleichterung der Bedienung von Geräten bis hin zur Ermöglichung der Gerätenutzung bei eigener eingeschränkter Mobilität sind nur die wichtigsten Motive zum Einsatz dieser nicht mehr neuen Technik.

Insbesondere für pflegebedürftige Menschen können solche Möglichkeiten erhebliche Erleichterungen im Alltag bewirken und den Grad der Eigenständigkeit verbessern helfen.

Umfangreiche Datenverarbeitung

Da bei Sprachassistenten die Sprache als Eingangssignal dient, müssen die integrierten Mikrofone ständig aufnahmebereit sein. Daten aus dem Umfeld des Nutzers enthalten Informationen, um anhand der Stimme (Ton) oder auch von Gesichtsmerkmalen (Video) Personen zu identifizieren und aus geäußerten Worten Aktionen auszulösen, wie z. B. das Bedienen von Haustechnik oder Geräten. Damit kann das Persönlichkeitsrecht dritter Personen beeinträchtigt werden, die sich in Räumen aufhalten, in denen mittels solcher Technik persönliche Daten, wie das gesprochene Wort oder Bilder verarbeitet werden.

Im Folgenden verwendete Begriffe

Wenn im Folgenden von zu Pflegenden die Rede ist, sind damit sowohl Heimbewohner, Pflege- bzw. Hilfebedürftige, welche in einer stationären Einrichtung oder durch eine Sozialstation gepflegt werden, als auch Angehörige gemeint.

Ist von Pflegeeinrichtung die Rede, sind sowohl stationäre Pflegeeinrichtungen (Pflegeheime) als auch ambulante Pflegeeinrichtungen (Pflegedienste bzw. Sozialstationen) gemeint.

Der Begriff Mitarbeiter wird sowohl für Beschäftigte i. S. v. § 4 Nr. 20 DSG-EKD als auch für andere Personen (z. B. Ehrenamtliche, Praktikanten, sonstige Betreuende), die an der Leistungserbringung beteiligt sind, verwendet.

Funktionen digitaler Sprachassistenten kennen und verstehen

Sprachassistenten gibt es bekanntlich von Google (Google Assistent), Amazon (Alexa), Apple (Siri), Samsung (Bixby), Telekom (Hallo Magenta) oder Huawei (HiVoice) u. a. m.

Der Verbreitungsgrad solcher Dienste wird technisch maßgeblich mit beeinflusst von enthaltenen offenen Schnittstellen für Drittanbieter und deren Dienste. So hat Amazon den Dienst Alexa per Entwicklerschnittstelle offengelegt.

Viele Firmen haben bzw. können Hard- und Software entwickeln, die Alexa als Cloud-Dienst nutzen. Die Funktionen können sich dann signifikant unterscheiden. Angeboten werden z. B. Anwendungen des Hausnotrufs für Senioren auf Basis des Alexa-Dienstes.

Als digitaler Sprachassistent wird ein System bezeichnet, dessen Hard- und Software es ermöglicht, mittels Sprachbefehl Anweisungen auszuführen, z. B. Informationen abzufragen, Dialoge zu führen und Assistenzdienste zu erbringen. Die aufgenommene Sprache der Nutzer muss vom System erkannt und verstanden werden. Deshalb wird in der Regel eine Internetverbindung zu einem Cloud-Dienst aufgebaut, an den die auszuwertenden Daten (Sprache) gesendet werden, wenn die Verarbeitung nicht ausschließlich lokal auf dem Gerät erfolgt.

Nachdem Spracherkennungsalgorithmen die Daten analysiert haben, wird die erkannte Anweisung zur

Ausführung an eine Anwendung weitergeleitet (z. B. das Ergebnis einer Internetsuche vorgelesen) oder eine andere Anwendung gestartet (z. B. die Lieblingsmusik abgespielt). Fortgeschrittene Assistenten können bei Unklarheiten Rückfragen an den Nutzer stellen oder um Bestätigungen bitten.

Sprachassistenten reagieren bisher in der Regel auf sprachliche Anweisung (beginnend mit einem Aktivierungswort). Dann wird eine Aufzeichnung der Frage bzw. Anweisung über eine bestehende Internetverbindung an den Dienst (z. B. Alexa) geleitet, damit das System zur Spracherkennung und zum Verständnis der natürlichen Sprache die gewünschte Aktivität starten kann. Solche Dienste werden in eigenen oder beauftragten Rechenzentren auf entsprechend leistungsfähiger IT-Infrastruktur verarbeitet.

Dass die Form der Verarbeitung und die Orte der Verarbeitung, zum Beispiel in einem Drittland, besonderen Anforderungen an einen datenschutzkonformen Betrieb unterliegen können, wird als bekannt vorausgesetzt. Es wird auf die einschlägigen Veröffentlichungen der Aufsichtsbehörden verwiesen.

Kann ein Aktivierungswort nicht erkannt werden, wird die Verarbeitung der Daten gestoppt. Aktiviert werden können Sprachassistenten auch durch (Fehl-)Interpretation von Worten oder auch durch Satzteile (bei Alexa z. B. „Alles klar“ statt „Alexa“) oder durch Einschalten.

Sprachassistenten bieten nicht selten selbst oder durch Verknüpfungen zu anderen Apps den Zugriff auf weitere Kommunikationsdienste an, wie z. B. die Möglichkeit, Nachrichten zu senden und zu empfangen, zu telefonieren u. s. w. Hierfür müssen Nutzer in der Regel vor Verwendung ihr Einverständnis erklären, eine entsprechende Nutzungsrichtlinie einzuhalten.

Mit diesem Einverständnis übernimmt der Nutzer auch die Verantwortung, das für ihn oder sie maßgebliche (Datenschutz-)Recht einzuhalten.

Die Hersteller und Dienstanbieter halten sich selbst mit den Vertragsbedingungen frei. Eine Verletzung von Datenschutzrechten haben danach allein die Nutzenden zu vertreten.

Sofern der Sprachassistent ein Aktivierungswort oder ein anderes zur Aktivierung vorgesehenes Signal (z. B. Bewegung) erkennt und Daten mit den Diensten austauscht, signalisiert dies in der Regel ein visuelles oder akustisches Signal. Für einige Geräte besteht die Möglichkeit, solche erkennbaren Betriebsanzeigen in den Einstellungen abzuschalten.

Verfügt ein Sprachassistent über keinen Ein-/Ausschalter, muss erst die Stromzufuhr unterbrochen werden, um das Gerät und damit alle Sensoren wie Mikrofone und Kameras zu deaktivieren. Dies kann jedoch durch fest verbaute Akkus unmöglich werden.

Das Löschen der Audio-/Videoaufnahmen obliegt den Inhabern bzw. Nutzern. Je nach System ist einstellbar, dass Aufzeichnungen nach einer bestimmten Zeit oder automatisch gelöscht oder gar nicht erst gespeichert werden.

Arbeitsschutzrechtliche Einordnung

Fürsorgepflicht des Dienst- bzw. Arbeitgebers auch bei psychischen Belastungen

Aus § 618 BGB ergibt sich die Fürsorgepflicht des Dienst- bzw. Arbeitsgebers (im Weiteren Arbeitgeber) für seine Mitarbeiter.

Zu den Grundsätzen gemäß ArbSchG gehört es, die Arbeit so zu gestalten, dass eine Gefährdung für das Leben sowie die physische und psychische Gesundheit möglichst vermieden und die verbleibende Gefährdung gering gehalten wird (§ 4 Nr. 1 ArbSchG).

Der Arbeitgeber hat durch eine Gefährdungsanalyse zu ermitteln, welche Maßnahmen des Arbeitsschutzes erforderlich sind (§ 5 Abs. 1 ArbSchG).

Gemäß § 5 Abs. 3 Nr. 6 ArbSchG kann sich eine Gefährdung für Mitarbeiter durch psychische Belastungen ergeben.

Ein eingeschalteter digitaler Sprachassistent ermöglicht eine Raumüberwachung durch die Verarbeitung von Sprache und Bild.

Der damit einhergehende Überwachungsdruck, dem das Pflegepersonal bei der Erbringung der Pflegeleistung in dem überwachten Raum ausgesetzt ist, kann zu psychischen Belastungen führen, weil das eigene Verhalten (permanent)

anderen (dem Anbieter des digitalen Sprachassistenten und dem Nutzer) präsentiert wird. Das führt dazu, Eigenheiten und eigene Gewohnheiten abzulegen – bei der Pflege z. B. nicht mehr frei mit dem Pflegebedürftigen zu kommunizieren. Der oder die überwachte Person verliert die Freiheit und das Recht selbstbestimmten Entscheidens und Handelns im Rahmen der Aufgabenerfüllung bei der Arbeit.

Der Arbeitgeber muss den erzeugten Überwachungsdruck und die Auswirkungen auf die psychische Gesundheit der Beschäftigten in die Gefährdungsanalyse einbeziehen. Die DGUV1 (Grundsätze der Prävention) definiert die entsprechenden Pflichten des Arbeitgebers.

Es muss sichergestellt werden, dass während der Pflege nicht heimlich bzw. unbefugt Daten von Mitarbeitern der Pflegeeinrichtung durch einen digitalen Sprachassistenten des zu Pflegenden erhoben und verarbeitet werden (Aufklärung, Klausel im Heim-/Pflegevertrag).

Datenschutzrechtliche Einordnung

Die Mikrofone des Sprachassistenten nehmen jedes Geräusch im Raum auf. Es wird nicht unterschieden zwischen befugten Nutzern (zu Pflegender) und anderen Personen (Mitarbeiter, Besucher, Mitbewohner).

Wegfall des sog. Haushaltsprivilegs

Sofern mittels eines Sprachassistenten auch Daten von Mitarbeitern, Besuchern oder eines Mitbewohners erhoben und verarbeitet werden, liegt nicht mehr nur eine Verarbeitung personenbezogener Daten zur Ausübung ausschließlich, persönlicher oder familiärer Tätigkeiten (Haushaltsprivileg, vgl. Art. 2 Abs. 2 lit. c DS-GVO) vor.

Damit muss dann durch den Nutzer (die zu Pflegenden oder deren rechtliche Betreuung) das Datenschutzrecht gemäß der Datenschutz-Grundverordnung (DS-GVO) beachtet werden.

Möglichkeit von Sanktionen und Geldbußen

Aufsichtsbehördliche Befugnisse bis hin zu Sanktionen und Geldbußen sind gegen Nutzer von digitalen Assistenten oder deren rechtliche Betreuung denkbar, wenn Verletzungen des Persönlichkeitsrechts Betroffener eintreten.

Bereits Überwachungs- und Verhaltensdruck kann für den Eingriff in Persönlichkeitsrechte ausreichen.

Ton- und Videoaufnahmen greifen in das Recht auf informationelle Selbstbestimmung ein, da Betroffene keine Kontrolle mehr haben, was im Weiteren mit ihren personenbezogenen Daten passiert. Grenzen der Nutzung von Technik durch zu Pflegende und/oder Angehörige bestehen da, wo ein unverhältnismäßiger Eingriff in Persönlichkeitsrechte der Mitarbeiter der Pflegeeinrichtung oder anderer Personen erfolgt.

Digitale Sprachassistenten funktionieren über Sprache. Die Stimme gehört – ebenso wie ein Gesichtsfoto – als biometrisches Datum (Art. 4 Nr. 14 DS-GVO) zu den besonderen Kategorien personenbezogener Daten nach (Art. 9 Abs. 1 DS-GVO) und sind besonders schützenswert.

Auf Grund von Art. 9 Abs. 2 DS-GVO erfordert die Erhebung von Daten Nicht-Angehöriger, die den Raum betreten, wenn ein digitaler Sprachassistent aktiviert ist, eine ausdrückliche Einwilligung des bzw. der Eintretenden für einen oder mehrere festgelegte Zwecke. Die Einwilligung muss die Anforderungen nach Art. 7 DS-GVO i. V. m. Art. 4 Nr. 11 erfüllen. Eine solche Einwilligung dürfte in der Praxis kaum rechtskonform realisierbar sein.

Auch nicht in Frage kommt eine Einwilligung der Mitarbeiter gegenüber dem Arbeitgeber (Pflegeeinrichtung), da auf Grund des Abhängigkeitsverhältnisses Zweifel an der Freiwilligkeit der Einwilligung bestehen (vgl. § 49 Abs. 3 DSG-EKD).

Die Einwilligung als Rechtsgrundlage für die Verarbeitung scheidet also aus.

Darüber hinaus ist die Datenverarbeitung durch Sprachassistenten nicht erforderlich zur Begründung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch für Zwecke der Personalplanung und des Personaleinsatzes (§ 49 Abs. 1 DSG-EKD).

Datenschutzpflichten des Nutzers eines digitalen Sprachassistenten

Daten von Mitarbeitern der Pflegeeinrichtung

dürfen nicht durch einen digitalen Sprachassistenten des zu Pflegenden erhoben, an den Dienstanbieter übermittelt und verarbeitet werden. Damit muss vom Nutzer des Sprachassistenten verlangt werden, dass der Sprachassistent während der Pflege und Betreuung ausgeschaltet ist.

Die folgenden Erläuterungen werden gemacht, um die rechtlichen Anforderungen aufzuzeigen.

In der Praxis dürfte deren Umsetzung durch die zu Pflegenden, ihre Angehörigen oder auch durch die rechtlichen Betreuer kaum durchführbar sein, was eindeutig für das Abschalten aller Sprachassistenten während der Anwesenheit der Mitarbeiter in den Räumlichkeiten der zu Pflegenden spricht.

Sofern der digitale Sprachassistent während der Pflege und Betreuung nicht ausgeschaltet ist, gilt: Werden durch einen digitalen Sprachassistenten personenbezogene Daten von Mitarbeitern der Pflegeeinrichtung erhoben, sind die zu Pflegenden bzw. deren rechtliche Betreuer gegenüber den Mitarbeitern zur Information gemäß Art. 13 DS-GVO verpflichtet (Offenlegung der Verarbeitung). Dazu gehört u. a.: Wo die Daten verarbeitet werden, die Speicherdauer der Daten, der Hinweis auf das Recht auf Widerspruch gegen die Verarbeitung der eigenen Daten sowie auf Beschwerde bei der zuständigen Datenschutzaufsicht.

Die Informationen müssen vom Nutzer des Sprachassistenten gegenüber Mitarbeitern so dargestellt werden, dass diese sie ohne übermäßigen Aufwand verstehen (Art. 12 Abs. 1 DS-GVO).

Der für die Datenverarbeitung Verantwortliche (zu Pflegender bzw. rechtlicher Betreuer) muss auf Anforderung von Mitarbeitern deren Recht auf Auskunft (Art. 15 DS-GVO) erfüllen.

Mitarbeiter der Pflegeeinrichtung werden ihre Anfragen und Beschwerden möglicherweise zuerst an die kirchliche Datenschutzaufsicht richten. Auch wenn diese Möglichkeit besteht und der Datenschutzbeauftragte für Kirche und Diakonie die Betroffenen in ihren Anliegen unterstützen wird, werden solche Anfragen und Beschwerden letztlich von der zuständigen Datenschutzaufsicht beim Landesdatenschutzbeauftragten bearbeitet.

Rechte betroffener Mitarbeiter

Wie bereits weiter oben erwähnt, muss die Einrichtung vom Nutzer des Sprachassistenten verlangen, dass der Sprachassistent während der Pflege und Betreuung ausgeschaltet ist.

Ignorieren die zu Pflegenden oder in ihrem Namen handelnde Angehörige bzw. die rechtliche Betreuung das Auskunftsverlangen gemäß Heim-/Pflegevertrag, ist ein mögliches (kostenfreies) Werkzeug die Wahrnehmung ihrer Datenschutzrechte durch Betroffene, also durch die Mitarbeiter selbst. Mit Hilfe des Datenschutzrechts können Mitarbeiter

- ihre Rechte wahrnehmen (Art. 15 ff. DS-GVO),
- ggf. Widerspruch gegen die Verarbeitung ihrer Daten einlegen (Art. 21 DS-GVO)
- und sich bei der Aufsichtsbehörde beschweren (Art. 77 DS-GVO).

Andere rechtliche Möglichkeiten eröffnen

- § 201 StGB (Verletzung der Vertraulichkeit des [nicht öffentlich gesprochenen] Wortes),
- § 22 Kunsturhebergesetz (KunsturhG); ggf. § 201a StGB (Recht am eigenen Bild) – im Falle von Videoaufnahmen.

Ausgehend von seiner Fürsorgepflicht sollte der Arbeitgeber Mitarbeiter bei der Durchsetzung von Datenschutzrechten oder beim Einlegen anderer Rechtsmittel unterstützen.

Fazit

Der Arbeitgeber muss auf Grund seiner Fürsorgepflicht im Rahmen der Gefährdungsanalyse mögliche psychische Belastungen durch einen Überwachungsdruck, dem seine Mitarbeiter durch einen aktivierten digitalen Assistenten im Bewohnerzimmer ausgesetzt sind, berücksichtigen und erforderliche Schutzmaßnahmen vorsehen.

Geprüft werden sollte, in welchem Umfang der Nutzung privater Technik vertraglich Grenzen gesetzt werden können.

Die zu dokumentierende Information und Aufklärung in Aufnahmegesprächen als auch in Klauseln im Heim- bzw. Pflegevertrag, dass

- Ton-, Bild und Filmaufnahmen einschließlich Videoüberwachung von Personal (der Einrichtung) ohne eine informierte Einwilligung nicht zulässig sind,
- das heimliche Erstellen von Ton-, Bild- und Filmaufnahmen eine Straftat darstellt und damit neben zivilrechtlichen auch strafrechtliche Folgen auslösen kann,
- zivilrechtlich ein Verstoß u. a. Ansprüche auf Schadensersatz sowie die Kündigung des Vertrages zur Folge haben kann,

bedürfen in der Praxis auch der aktiven Durchsetzung der aufgezeigten Konsequenzen.

Das Mitschneiden von Sprach-, Bild- und Videodaten sowie das unbefugte Speichern und Verarbeiten solcher Aufnahmen kann strafbar sein.

Mitarbeiter diakonischer Einrichtungen haben das Recht auf den Schutz ihrer Persönlichkeitsrechte und die entsprechende Unterstützung durch ihre Arbeit- und Dienstgeber.

Ausübung der aufsichtsrechtlichen Befugnisse gemäß DSG-EKD

Kontrollen

Die Aufsichtsbehörde für den Datenschutz hat auf gesetzlicher Grundlage umfangreiche Befugnisse, um die einheitlichen Anwendung und Durchsetzung des kirchlichen Datenschutzrechts zu überwachen, indem sie beispielsweise auf Verlangen einen jederzeitigen und ungehinderten Zugang zu Räumen und einen Zugriff auf Anlagen bekommen muss, in bzw. mit denen personenbeziehbare Daten verarbeitet werden.

In der Regel werden anlassbezogen, z. B. im Zuge der Bearbeitung von Datenschutzverletzungen Dokumente und Verfahrensabläufe geprüft, um die tatsächlichen Ursachen und Begleitumstände einer Datenschutzverletzung zu erkennen.

Anlasslose Kontrollen als ein besonders starkes Instrument wurden und werden stichprobenweise durchgeführt.

Beanstandungen

Der Datenschutzbeauftragte für Kirche und Diakonie hat im Berichtszeitraum in den meisten Fällen durch Beschwerden Betroffener oder Meldungen von Datenschutzverletzungen gemäß § 44 Abs. 2 Satz 1 DSG-EKD Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten festgestellt und dies gegenüber der verantwortlichen Stelle oder gegenüber dem Auftragsverarbeiter formell beanstandet.

Sofern die Verletzung der kirchengesetzlichen Datenschutzbestimmungen nicht offensichtlich war, wie zum Beispiel im Falle der Ablage oder Speicherung von behördlichen Führungszeugnissen in Personalakten ohne nachweisbare Einwilligung der Betroffenen, ermittelte die Aufsichtsbehörde durch Ausübung ihrer Befugnisse nach § 44 Abs. 1 DSG-EKD den gesamten Sachverhalt.

Regelmäßig wird davon Gebrauch gemacht, Hinweise zu geben, wenn beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen kirchliches Datenschutzrecht verstoßen.

Anordnungen

Im Berichtszeitraum nicht ausgeübt wurde die Befugnis, gemäß § 44 Abs. 3 DSG-EKD mittels förmlichen Verwaltungsaktes anzuordnen,

- Verarbeitungsvorgänge auf bestimmte Weise und in einem bestimmten Zeitraum mit dem DSG-EKD in Einklang zu bringen;
- Verarbeitungsvorgänge vorübergehend oder dauerhaft zu beschränken oder zu unterlassen;
- die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation auszusetzen;
- personenbezogene Daten zu berichtigen, zu sperren oder zu löschen;
- die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen.

In den bearbeiteten Vorgängen genügten konkrete Hinweise der Aufsichtsbehörde und diese wurden von den kirchlichen Stellen entsprechend umgesetzt.

Bußgelder

Die Aufsichtsbehörden können gemäß § 45 DSG-EKD gegen verantwortliche Stellen, soweit sie als Unternehmen im Sinne des § 4 Nr. 19 DSG-EKD am Wettbewerb teilnehmen, Geldbußen verhängen oder für den Wiederholungsfall androhen, wenn eine verantwortliche Stelle oder ein kirchlicher Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen des DSG-EKD verstößt. Dabei stellen die Aufsichtsbehörden sicher, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

Im Berichtszeitraum wurden zwei begonnene Bußgeldverfahren wieder eingestellt, nachdem die betreffenden diakonischen Träger zeitnah angemessene Maßnahmen umgesetzt hatten.

Ausgewählte Themen bei Beratung und Aufsicht im Berichtszeitraum

Herausforderung COVID-19

Der Berichtszeitraum war dominiert durch die seit Anfang 2020 deutschland- und weltweit bestehende Pandemielage im Zusammenhang mit Covid-19 und die sich daraus ergebenden Herausforderungen.

Von Beginn an war der Datenschutzbeauftragte für Kirche und Diakonie als Aufsichtsbehörde in seinem Zuständigkeitsbereich involviert und Adressat für zahlreiche Anfragen, Kritiken und Beschwerden. In den meisten Fällen waren diese ausgelöst durch teils unvorhersehbare, teilweise sehr kurzfristig vom Gesetzgeber beschlossene Maßnahmen. Die nachfolgend dargestellten Sachverhalte sind ausgewählte Vorgänge, die nicht chronologisch geordnet sind.

Abfrage Impfbereitschaft und Dokumentation von Impfnachweisen

In den zur Thematik eingereichten Anfragen ging es häufig um die Möglichkeit, die Impfbereitschaft zur Vorbereitung innerbetrieblicher Impfkampagnen abzufragen und um die Dokumentation von Impfnachweisen. Insbesondere wurde angefragt, ob Impfnachweise zu Dokumentationszwecken kopiert und aufbewahrt werden dürfen.

Der Datenschutzbeauftragte für Kirche und Diakonie wies wiederholt darauf hin, dass derartige Dokumente nach Ablauf zu definierender Fristen oder nach Wegfall einer nur befristet geltenden Rechtsgrundlage datenschutzgerecht physisch gelöscht werden müssen. Das bedeutet ganz konkret, dass Impfnachweise eingesehen werden und als Aktennotiz mit Datum der Einsichtnahme und der Gültigkeit der entsprechenden Nachweise hinterlegt werden konnten, solange dafür die rechtliche Grundlage gegeben war.

Besucherlisten bei kirchlichen Veranstaltungen

Im Bereich der verfassten Kirche gab es mehrfach Anfragen, wie mit den Besucherlisten von kirchlichen Veranstaltungen insbesondere Gottesdiensten umgegangen werden muss. Die Aufsichtsbehörde hat dazu angemerkt, dass derartige Besucherlisten nicht für mehrere Veranstaltungen hinterlegt werden dürfen. Besser ist die Anfertigung der von der Landeskirche bereitgestellten Einzelnachweise, die nach einem definierten Zeitraum von spätestens vier Wochen datenschutzgerecht zu entsorgen sind. Bei den Anwesenheitslisten oder auch Besucherlisten musste sichergestellt werden, dass diese nicht in fremde Hände geraten bzw. dass durch Besucher keine unbefugte Einsicht in diese Listen vorgenommen werden konnte.

Meldungen über den Impfstatus

Anfragen hatten die Meldung des Impfstatus von Kita-Personal an staatliche Behörden zum Inhalt. Derartige Übermittlungen sind nur aufgrund gesetzlicher Bestimmungen möglich. Wenn die jeweils geltende Corona-Schutz-Verordnung des Bundeslandes eine solche Übermittlung vorschreibt, ist sie nicht nur möglich, sondern muss zwingend erfolgen. Besonders zu achten war dann auf den zulässigen und erforderlichen Umfang der Datenübermittlung.

Verteilung von sogenannten Impflisten

Andere Anfragen hatten die Verteilung von Impflisten per E-Mail zum Gegenstand. Die Aufsichtsbehörde hat darauf hingewiesen, dass E-Mail ohne weitere Maßnahmen ein unsicheres Übertragungsmedium darstellen kann und dass derartige Listen auch bei gebotener Eilbedürftigkeit nur verschlüsselt und über sichere oder alternative Übertragungswege übermittelt werden dürfen.

Die Auswahl geeigneter Schutzmaßnahmen muss sich dabei immer an der Schutzbedürftigkeit der von der Verarbeitung betroffenen Kategorien von Daten orientieren.

Aufgrund der in den ersten Wochen von Februar bis April 2020 allseits bestehenden Unsicherheiten und des Ziels, eine größere Ausbreitung von Infektionen, insbesondere in sozialen Einrichtungen so schnell und effektiv wie möglich zu unterbinden, wurde mitunter fahrlässig den Fragen des Datenschutzes nicht die rechtlich gebotene Aufmerksamkeit zuteil.

In einem Fall kam es so zur Verbreitung dieser Listen an einen Personenkreis, der nicht zur Einsicht in diese Listen berechtigt gewesen war. Dies wurde durch die Aufsichtsbehörde mit entsprechenden Hinweisen beanstandet.

Zulässigkeit der Erfassung von Impfstatus

In mehreren Anfragen wurde die Zulässigkeit der Erfassung des Impfstatus in Frage gestellt. Diesen Anfragen konnte mit Verweis auf das Infektionsschutzgesetz abgeholfen werden, das solche Erhebungen des Impfstatus ausdrücklich vorsah. Als Konsequenz musste beispielsweise auch bei Veranstaltungen in Schulen in freier Trägerschaft der Impfstatus der Mitarbeiter und sonstiger Teilnehmer erhoben werden.

Beschwerde wegen Preisgabe des Impfstatus durch eine Diakonie Sozialstation

Das sensible und über die letzten beiden Jahre kontrovers diskutierte Thema der Impfung gegen Covid-19 war insbesondere im Hinblick auf zulässige Verarbeitungen der Informationen zum Impfstatus ein häufiger Anfrage- oder Beschwerdegrund.

Die Information über eine Bereitschaft oder Nichtbereitschaft zur Impfung findet einen grundsätzlichen Schutz im Recht auf informationelle Selbstbestimmung, falls nicht eine Rechtsgrundlage dieses Recht zulässig einschränkt.

Außer auf Grundlage der besonderen, zeitlich befristeten gesetzlichen Regelungen für den Zutritt zum Arbeitsplatz und die damit verbundene Verarbeitung des Impf-, Genesenen- (Sero-) und Teststatus in Bezug auf Covid-19 muss niemand Auskunft über seinen Impfstatus geben. Dies ist jederzeit zu respektieren.

Im konkreten Fall wurde durch ein Programm, auf das sämtliche Mitarbeiter Zugriff haben, zum Gebet für eine ungeimpfte Person aus dem Kollegium aufgerufen, welche an Corona erkrankt war. Im Kollegenkreis war sehr schnell bekannt, um welche Person es sich handelt, auch wenn kein Name genannt wurde. Insofern waren die Informationen und Daten hinreichend „personenbeziehbar“. Es wurde der Impfstatus in der Nachricht preisgegeben und somit das Grundrecht auf informationelle Selbstbestimmung verletzt.

Der verantwortlichen Stelle wurde eine formelle Beanstandung ausgesprochen und ein Bußgeld für den Wiederholungsfall angedroht.

Veröffentlichungen der Aufsichtsbehörde mit thematischem Bezug auf Covid-19

- 17.03.2020 Die Aufsichtsbehörde für den Datenschutz gibt Hinweise zu Datenschutz und Corona
- 25.05.2020 Hinweise zur Verarbeitung von Daten zum Schutz vor ansteckenden Krankheiten
- 30.03.2021 Stellungnahme zur Verfolgung von Kontakten mit digitalen Lösungen
- 25.11.2021 Die 3G-Regelung für den Zutritt zum Arbeitsplatz und die damit verbundene Verarbeitung des Impf-, Genesenen- (Sero-) und Teststatus in Bezug auf Covid-19

Datenschutz in Kindertagesstätten

Fragen nach dem Einsatz sogenannter Kita-Apps zeigen hohen Beratungsbedarf

Im Berichtszeitraum wurde die Möglichkeit des Einsatzes konkret benannter Kita-Apps zur Unterstützung der Kita-Verwaltung als auch der Kommunikation mit den Eltern angefragt.

Im Rahmen der Möglichkeiten wurden vereinzelt Dokumente begutachtet und Hinweise gegeben.

Ganz praktisch zeigt sich in vielen Anfragen und Vorgängen ein Mangel an Ressourcen und Expertisen kirchlicher Einrichtungen, wie z. B. in Kitas bei der Bewältigung der umfangreichen technischen und rechtlichen Anforderungen. Kitas in kirchlicher bzw. diakonischer Trägerschaft benötigen insbesondere im Hinblick auf die IT verstärkte Unterstützung auch personeller Art durch ihre Träger und Landesverbände.

Es wird empfohlen, auf Ebene der Träger und Verbände gemeinsam Lösungen zu erarbeiten und im Ergebnis den Trägern und Kitas praxistaugliche Lösungen auf der Grundlage weitgehend einheitlicher Verarbeitungstätigkeiten anzubieten.

Trägerschaft kirchlicher Kita und Fragen nach dem anwendbaren Datenschutzrecht

Als Aufsichtsbehörde sowohl für den Bereich der verfassten Kirche als auch im Bereich der Diakonischen Werke ist es immer wieder

Gegenstand von Beratungen, wie sich die unterschiedlich ausgeprägte Trägerschaft für Kindertagesstätten praktisch auswirkt auf anzuwendendes kirchliches Datenschutzrecht.

Zum einen treten Kirchgemeinden als Träger von Kindertagesstätten auf, andererseits ist die Diakonie mit ihren rechtlich selbstständigen Trägern Betreiberin vieler Kitas. Das anzuwendende Recht ist eindeutig geregelt. Datenschutzrechtlich müssen alle Kitas das DSG-EKD anwenden.

In Beantwortung von Anfragen anderer, sich dem christlichen Menschenbild und der christlichen Botschaft verpflichtet ansehenden Trägern weisen wir regelmäßig darauf hin, dass entweder die satzungsmäßige Mitgliedschaft in einem Diakonischen Werk oder ein offizieller Zuordnungsbeschluss der jeweiligen evangelischen Landeskirche einen Träger mit allen Konsequenzen rechtlich zu einem „kirchlichen“ Träger macht. Als Folge ist dann kirchliches Recht auch im Datenschutz anzuwenden.

Die Aufsichtsbehörde muss auch vier Jahre nach Inkrafttreten des neuen EKD-Datenschutzgesetzes Einrichtungen häufig darauf hinweisen, dass die DS-GVO im kirchlichen Bereich nicht anwendbar ist.

Möglich jedoch ist, dass kirchliche bzw. diakonische Stellen spezialgesetzliche Regelungen anzuwenden haben. Ist das der Fall, dann gehen diese Regelungen gemäß § 2 Abs. 6 DSG-EKD dem kirchlichen Datenschutzrecht vor.

Offener Aushang von Kontaktdaten

Mit Recht beschweren sich Betroffene über offene Aushänge in Kitas, bei denen neben Namen von Kindern und Eltern auch Anschriften, Telefonnummern und Wohnadressen für alle zugänglich gemacht werden. Während Daten der Mitarbeiter einer Kita gemäß § 49 DSG-EKD im erforderlichen Umfang innerhalb der Einrichtung auch öffentlich bekannt gegeben werden dürfen, gilt dies für die Daten der Kinder und Personensorgeberechtigten, z. B. die Eltern, nicht.

Einbruch in eine Kita, Kamera mit Kinderbildern entwendet

Einige der Datenpannen, welche gemeldet wurden, entstehen durch Einbrüche. Es werden dabei häufig Datenträger oder technische Geräte mit sensiblen Daten auf den Festplatten entwendet. Wenn es sich bei der verantwortlichen Stelle bspw. um eine Kita handelt, sind meist auch die Daten der betreuten Kinder betroffen.

Mitarbeiter kirchlicher Stellen müssen wiederholt zum Datenschutz sensibilisiert werden. Auch müssen die Datenträger und Endgeräte, wie zum Beispiel Laptops, Mobiltelefone und insbesondere digitale Fotoapparate durch Umsetzung effektiver Maßnahmen aus einem möglichst schriftlichen Schutzkonzept gesichert sein, so dass ein Diebstahl und eine Datenpanne durch Umsetzung wirksamer Maßnahmen unterbunden werden.

Eine nach dem Stand der Technik vorgenommene Verschlüsselung der Datenträger würde im Fall des Verlustes der Datenträger durch Diebstahl im Ergebnis keine Datenschutzverletzung bedeuten. Da dies auf Datenträgern in Kameras in der Regel nicht möglich ist, muss das erwähnte Schutzkonzept die sichere Handhabung genau vorschreiben.

Die Anfertigung / der Druck von Fotos durch die Kita bei Fotodienstleistern ist in der Regel nicht datenschutzkonform möglich

Bei der Nutzung von Dienstleistern für das Anfertigen von Papierabzügen von Digitalfotos ist eine Vereinbarung zur Auftragsverarbeitung gemäß § 30 DSG-EKD gesetzlich vorgeschrieben. Fotografen bieten solche Vereinbarungen an.

Eine schriftliche Anfrage ergab, dass die bekannten Dienstleister, die mit aufgestellten Automaten, z.B. in Drogerien, Fotodienstleistungen offerieren, diese Fotoarbeiten nur für Privatpersonen anbieten. Gewerbliche Kunden, wie eine Kita oder ein Kita-Träger rechtlich definiert sind, sind wegen der Unmöglichkeit, einen Auftragsverarbeitungsvertrag mit dem Dienstleister abzuschließen, praktisch nicht in der Lage, die Leistungen solcher Anbieter datenschutzkonform zu nutzen.

Aus diesem Grund bleibt nur die Inanspruchnahme eines Fotografen oder Foto-Dienstleisters mit einer Vereinbarung zur Auftragsverarbeitung (AVV) gemäß § 30 DSG-EKD oder das Ausdrucken von Fotos auf eigener Technik.

Pflicht zur Transparenz und Information schon bei der Datenerhebung

Kitas haben mit der Herausforderung zu tun, dass

sie regelkonform Erklärungen zum Datenschutz in den Einrichtungen vorhalten und abgeben müssen.

Im Datenschutzgesetz ist dies allgemein in den §§ 17 und 18 DSG-EKD (Informationspflichten bei unmittelbarer bzw. mittelbarer Datenerhebung) i. V. m. § 16 DSG-EKD (Transparente Information, Kommunikation) geregelt.

Anders als im staatlichen Bereich legt § 17 Abs. 1 DSG-EKD fest, dass den betroffenen Personen die Informationen zur Datenverarbeitung erst auf Verlangen vorgelegt werden müssen.

Da jedoch das Verlangen bereits im Zeitpunkt der Datenerhebung geäußert werden kann, haben wir in Beratungsgesprächen immer wieder darauf hingewiesen, dass die Informationspflichten sowohl nach § 17 DSG-EKD als auch nach § 18 DSG-EKD bereits vorbereitet sein sollten. Verlangen betroffene Personen diese Informationen, so sind sie umgehend zur Verfügung zu stellen.

Wir haben wiederholt empfohlen, ähnlich wie bei staatlichen Kindertagesstätten diesen Pflichten dadurch nachzukommen, dass die Informationen öffentlich ausgehängt oder als Dokument vorgehalten werden. Eine Übergabe dieser Informationen muss nicht mit Unterschrift der betroffenen Person bestätigt werden.

Veröffentlichungen der Aufsichtsbehörde mit thematischem Bezug auf Informationspflichten

- 21.07.2020 Handreichung Umsetzung der Informationspflichten nach § 17 und 18 DSG-EKD

Nutzung von Cloud-Diensten durch Kita's zur Kommunikation mit Eltern und zur Verteilung von Kinderfotos an die Eltern mittels Cloud

Einige Anfragen hatten die geplante Nutzung von Cloud-Diensten zum Inhalt, beispielsweise zur Verteilung von Daten der Kinder bzw. der Eltern einschließlich dem Teilen von Fotos.

Wir haben in Beantwortung dieser Anfragen darauf hingewiesen, dass mittels Cloud-Diensten jegliche Daten einschließlich Bilder von Kindern und Informationen über Kinder und deren Sorgeberechtigte nur dann bereitgestellt oder geteilt werden können, wenn diese Cloud-Dienste sich im Geltungsbereich der DS-GVO befinden und technisch-organisatorische Maßnahmen zu deren Schutz getroffen werden, wenn ein unbefugter Zugriff (z. B. durch Behörden) aus unsicheren Drittstaaten auf solche Daten nicht sicher ausgeschlossen werden kann. Konkret betroffen von diesen Vorgaben sind Dienste fast aller außereuropäischen Anbieter wie Amazon, Google, Dropbox, Microsoft.

Wir haben darauf hingewiesen, dass auch bei der Speicherung und Teilung von Daten immer darauf geachtet werden muss, um welche Kategorien von Daten es geht. Bilder von Kindern, auf denen auch andere Kinder abgebildet werden, können nicht ohne Weiteres an alle Eltern verteilt werden. Dies bedarf immer der Einwilligung auch der anderen Sorgeberechtigten der Kinder.

Inventarisierte Aufbewahrung von Fotos in einer Kita

Ausweislich der bearbeiteten Vorgänge gestaltet sich die Aufbewahrung von Fotos auf Datenträgern, die sich in Kameras der jeweiligen Kita befinden immer wieder als problematisch. Diesbezüglich wurden uns Datenpannen übermittelt, wo es teilweise um den Diebstahl von Kameras mit Bildern von Kindern bzw. von Festen der Kita ging. In einer Datenpanne wurde uns mitgeteilt, dass ein Datenträger mit Bildern von Kindern im Automaten einer Drogerie-Filiale zurückgelassen wurde. Dieser Datenträger wurde dann durch die Polizei der Kita zurückgegeben.

Wir haben in Beratungsgesprächen ausdrücklich darauf hingewiesen, dass Datenträger mit Fotos von Kindern mit größter Sorgfalt zu behandeln sind. Diese Datenträger sollten nach Anfertigung der Fotografien aus dem jeweiligen Aufnahmegerät entfernt und sicher verschlossen werden.

Datenträger von im Eigentum der Kita befindlichen Geräten gehören zum Inventar der jeweiligen Kita und müssen dementsprechend verwaltet werden. Auch die Verwaltung der Bilder selbst sollte organisiert werden. Bilder müssen leicht auffindbar sein, z. B. für den Fall, dass einer Aufforderung zur Löschung nachgekommen werden muss.

Unverschlüsselter USB-Speicherstick durch Praktikanten einer Kita verloren

Die Daten von Kindern gehören zu den besonders schützenswerten Daten. Zum Arbeitsalltag einer Kita gehört es, durch Portfolios die Entwicklung der

Kinder zu dokumentieren. Hierbei spielen auch die Bilder der Kinder eine Rolle. Der richtige Umgang in der Verarbeitung der Bilder ist dabei obligatorisch.

In einem unserer Aufsichtsbehörde gemeldeten Fall wurde bekannt, dass die Portfolio-Kinderbilder auf einem USB-Stick gespeichert waren, welcher unverschlüsselt war und auch noch weitere betriebliche Dateien enthielt. Dieser Stick ist außerhalb der Kita auf dem Heimweg vom Drogeriemarkt, bei dem die Kinderbilder entwickelt werden sollten, verloren gegangen. Er wurde durch einen Bürger, welcher ihn gefunden hat, mit dem Verdacht auf Kinderpornografie bei der zuständigen Polizeibehörde abgegeben. Diese leitete ein Ermittlungsverfahren ein. Da die Bilder aber lediglich den Kita-Alltag abbildeten und durch weitere Dateien die entsprechende Einrichtung gefunden werden konnte, wurde der Stick wieder an die Kita gegeben und das Verfahren eingestellt.

An dieser Stelle ist noch einmal darauf hinzuweisen, dass Drogeriemärkte nach unserem letzten Kenntnisstand keine Verarbeitungen im Auftrag für Kunden anbieten, die keine Verbraucher sind.

Als Sicherheitsproblem tritt hinzu, dass an den dort im Einsatz befindlichen Apparaten verschlüsselte USB-Speichersticks nicht erkannt und gelesen werden können.

Es wird empfohlen, stets Berufsfotografen zu beauftragen und diese vertraglich zu binden.

Höhere Kosten für die Bildentwicklung dürfen zu keinem Zeitpunkt als Grund für eine nicht datenschutzkonforme Verarbeitung von Fotos angeführt werden.

Daten unter dem Berufsgeheimnis

Die strafbewährte Schweigepflicht nach § 203 StGB gilt ausschließlich für Personen, nicht für Träger und Einrichtungen.

Im bei der Aufsichtsbehörde bearbeiteten Fall waren Mitarbeiter, die der Schweigepflicht unterliegen, aufgefordert worden, ihre Gesprächs- und Arbeitsdokumentationen innerhalb der Einrichtung allen Kollegen, einschließlich der Geschäftsführung offen zugänglich zu machen. Die Leitung begründete ihr Vorgehen mit dem Erfordernis einer besseren Arbeitsorganisation und behauptete in diesem Zusammenhang, „dass Vorgesetzte und Kollegen nicht als Dritte anzusehen seien, weil der freie Träger nach außen dem Datenschutz und der Schweigepflicht unterläge und so der Verschwiegenheitspflicht nach § 203 StGB Rechnung getragen sei.“

Die Aufsichtsbehörde hat Hinweise gegeben, die jedem Geschäftsführer bekannt sein müssen und beachtet werden sollten.

Mitarbeiter, die einer in § 203 Abs. 1 StGB genannten Berufsgruppe angehören, haben grundsätzlich auch innerhalb der Organisation eine strafrechtliche sanktionierte Schweigepflicht. Schweigepflichtig im Sinne des § 203 StGB ist immer der Geheimnisträger persönlich, nicht die Organisation, in der er arbeitet.

Geheimnisträger haften persönlich für alle unzulässigen Offenbarungen anvertrauter Geheimnisse. Das müssen sich auch alle Personen bewusst machen, die als Mitwirkende für Berufsgeheimnisträger tätig werden und dazu vorher auf die Verschwiegenheit nach § 203 StGB verpflichtet werden.

Die strafrechtliche Schweigepflicht kann nicht durch Weisung von Vorgesetzten aufgehoben oder abgeschwächt werden, weil sich das Direktionsrecht eines Arbeitgebers bzw. Dienstgebers nicht über strafrechtliche Vorschriften hinwegsetzen kann.

Leitungsbefugnisse (Weisung, Anordnung, Aufsicht) sind keine Eingriffsbefugnisse in die berufliche Schweigepflicht (§ 203 StGB).

Anvertraute Informationen dürfen weitergegeben werden, wenn eine Einwilligung des Betroffenen vorliegt oder es gesetzlich geboten ist (vgl. z.B. § 4 Kinderschutz-Kooperations-Gesetz).

Die Verschwiegenheit wird nicht berührt, wenn die Leitung allgemeine Informationen zur Tätigkeit der sozialpädagogischen Fachkraft (z.B. Anzahl und Dauer von Beratungsgesprächen) anfordert, ohne dass ein Personenbezug hergestellt werden kann.

Aufforderungen oder Arbeitsanweisungen Vorgesetzter, die den Geheimnisträger anstiften (§ 26 StGB) oder nötigen (§ 240 StGB), Geheimnisse zum Beispiel durch Offenlegung (allgemein oder

beschränktes Zugänglichmachen) von papierhaften oder elektronischen Mitschriften und Arbeitsdokumenten zu offenbaren, stellen selbst ein unzulässiges, strafbewährtes Handeln dar.

Durch die Änderung des § 203 StGB (im Nov 2017) wurde die Schweigepflicht für Berufsgeheimnisträger auf „sonstige Mitwirkende“ des Geheimnisträgers ausgedehnt.

Allerdings verpflichtet der Gesetzgeber die Berufsgeheimnisträger (nicht die Organisation!) dazu, die „sonstigen Mitwirkenden“ auf § 203 StGB zu verpflichten. Tut er dies nicht, haftet der Berufsgeheimnisträger für Verletzungen der Schweigepflicht der einbezogenen „sonstigen mitwirkenden Personen“.

Damit ist klar, dass sonstige Mitwirkende nicht einfach pauschal alle Kollegen oder die Leitung der Einrichtung sind.

„Sonstige Mitwirkende“ müssen jedoch nur verpflichtet werden, wenn sie nicht solche Fachkollegen sind, die bereits selbst der Schweigepflicht nach § 203 StGB unterliegen (vgl. § 203 Abs. 4 Satz 2 Nr. 1 StGB).

Berufsgeheimnisträger sind immer persönlich verantwortlich und müssen deshalb auch ihre Vertretung im Krankheitsfall, während des Urlaubs und anderer Abwesenheitsgründe selbstständig regeln und dazu im Regelfall auch eine wirksame Einwilligung der von ihnen betreuten Menschen einholen. Die Träger und Einrichtungen, in denen Berufsgeheimnisträger angestellt sind, können und sollen unterstützend die geeigneten Arbeitsbedingungen schaffen und auch die Möglichkeit der Vertretung durch geeignetes Fachpersonal sicherstellen.

IT-Systeme und Dienste, Übermittlung personenbezogener Daten in die USA, US-Hersteller im Fokus

Datenschutz - Folgenabschätzungen müssen primär die Verarbeitungen im Fokus haben

Zahlreiche Anfragen thematisierten im Berichtszeitraum die Auswahl ganzer IT-Systeme oder auch einzelner Anwendungen. Die Aufsichtsbehörde wurde in diesem Zusammenhang von kirchlichen bzw. diakonischen Stellen häufiger angefragt, ob sie die Durchführung der nach § 34 DSG-EKD erforderlichen Datenschutz-Folgenabschätzung übernehmen könne. Dies waren offenkundig Missverständnisse der anfragenden Stellen und musste selbstverständlich verneint werden, weil dies eine originäre Aufgabe der verantwortlichen Stelle selbst ist mit Beratung und Unterstützung durch den eigenen betrieblichen Datenschutzbeauftragten.

Hinzuweisen war in den meisten Fällen darauf, dass Datenschutz-Folgenabschätzungen nicht aufgrund der Einführung neuer IT-System durchzuführen sind, sondern sich die Pflicht dazu allein dann ergibt, wenn für eine konkret geplante Verarbeitung personenbezogener Daten von einem voraussichtlich bzw. wahrscheinlich hohen Risiko für die Rechte und Freiheiten der von dieser Verarbeitung betroffenen Personen ausgegangen werden muss (§ 34 DSG-EKD).

Nur für den Fall, dass im Ergebnis einer Datenschutz-Folgenabschätzung das festgestellte hohe Risiko der geplanten Verarbeitung nicht ausreichend durch geeignete technische und organisatorische Maßnahmen abgesenkt werden kann, müssen kirchliche und diakonische Stellen die Aufsichtsbehörde vor dem Beginn der Verarbeitung konsultieren.

Schulportallösungen

Bearbeitet wurden zahlreiche Anfragen aus Sachsen bezüglich der sogenannten Schulportallösungen im Bereich der Schulen in freier Trägerschaft. Diese Portallösungen stammen zum Teil aus dem Bereich der staatlichen Schulen bzw. aus Schulen freier Trägerschaft anderer Bundesländer. Die Portallösungen wurden durch die Aufsichtsbehörde insbesondere auf das Vorhandensein von Datenschutzerklärungen und hinreichender Einwilligungen überprüft.

Datenübermittlung in die USA: Bald wieder „problemlos“ möglich?

Nicht zuletzt wegen der Herausforderungen durch den zeitweiligen gesetzlichen Zwang zum Homeoffice wurde und ist die Aufsichtsbehörde häufig angefragt worden zum Einsatz von Anwendungen insbesondere US-amerikanischer Hersteller wie Microsoft, Google, Zoom u. a. m.

Die Umstände und Herausforderungen in den ersten Monaten der Pandemie haben in vielen Fällen zu einem ungeordneten Einsatz technischer Lösungen zur Online-Kommunikation geführt, auch unterstützt durch zeitweise kostenfreie Angebote von Herstellern und Dienstanbietern.

Mitten in diese Zeit fiel das sog. „Schrems II Urteil des EuGH“ und traf angesichts der Pandemielage auf weniger Verständnis als in „normalen“ Zeiten hätte erwartet werden können. Die rechtliche Bewertung dagegen war und ist eindeutig.

Der Europäische Gerichtshof (EuGH) hatte am 16.07.2020 den EU-US-Privacy Shield (ein Abkommen, auf dessen Grundlage der Austausch personenbezogener Daten mit den USA unter Einhaltung der geltenden gesetzlichen Grundsätze der Verarbeitung möglich war) für ungültig erklärt. Hauptgrund war der fehlende Rechtsschutz für europäische Bürger, wenn US-amerikanische Behörden auf Basis von amerikanischen Sicherheitsgesetzen auf deren Daten zugreifen.

Während dieser Tätigkeitsbericht entsteht, verhandeln die USA und die EU ein Nachfolgeabkommen zum Privacy-Shield.

Die rechtliche Grundlage für die Übermittlung personenbezogener Daten in Drittstaaten, wie z.B. in die USA, findet sich im DSG-EKD. Die Übermittlung ist nach § 10 Abs. 1 DSG-EKD grundsätzlich zulässig,

1. wenn die EU-Kommission ein angemessenes Datenschutzniveau entsprechend den Bestimmungen des Artikel 45 Absatz 2 Datenschutz-Grundverordnung festgestellt hat,

   ➔ Das ist nicht erfüllt, deshalb ist Datenverkehr in die USA auf dieser Grundlage nicht möglich.

2. wenn als geeignete Garantien Standard-Datenschutzklauseln verwendet werden, die von der EU-Kommission genehmigt worden sind.

   ➔ Das ist erfüllt, aber es sind weitere technische Schutzmaßnahmen wie eine Verschlüsselung nötig, wenn das geforderte Datenschutzniveau nicht allein auf vertraglicher Grundlage gewährleistet werden kann, z. B. wegen der Möglichkeit des unzulässigen Zugriffs durch Behörden.

Für Ausnahmefälle gibt es nach § 10 Abs. 2 DSG-EKD weitere Gründe einer zulässigen Übermittlung.

„Problemlos“ möglich, wie im Titel suggeriert, ist ein Transfer von Daten über Netze, Regionen und Ländergrenzen hinweg zu keinem Zeitpunkt.

Neben der Rechtmäßigkeit ist der Datenschutz gemäß aller im Gesetz gegebenen Anforderungen technisch und organisatorisch zu gewährleisten.

Manche IT-Systeme und Programme sind inzwischen so komplex geworden, dass deren datenschutzkonformer Betrieb ohne hohe Aufwendungen für IT-Personal und IT-Service kaum noch eingerichtet, geschweige denn stets sichergestellt und kontrolliert werden kann. Deshalb sollten insbesondere diakonische Träger, deren Ressourcen dafür nicht ausreichen, mit anderen diakonischen Trägern kooperieren.

Veröffentlichungen der Aufsichtsbehörde mit thematischem Bezug

- 17.07.2020 Datenübermittlung in die USA auf Grundlage von EU-U.S. Privacy Shield ist datenschutzrechtlich unzulässig
- 10.06.2021 Position – C-311/18, Schrems II, Drittlandübermittlung
- 04.06.2021 EU-Kommission veröffentlicht aktualisierte Standarddatenschutzklauseln für internationale Übermittlungen
- 18.08.2021 Stand der Technik nach § 27 Abs. 1 DSGEKD
- 07.10.2021 Die Eignung von Software-Lösungen anhand der Vertragsbedingungen prüfen
- 15.10.2021 Gemeinsame Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zur Datenübermittlung in die USA

Elektronische Kommunikation und Videokonferenzsysteme im Speziellen

Nicht allein wegen der Umstände, welche die Covid-Pandemie mit sich brachte, jedoch dadurch gefördert, standen und stehen Fragen der Digitalisierung besonders im Vordergrund.

Datenschutzrechtliche Fragestellungen im Zusammenhang mit der Einführung und Nutzung von Videokonferenzsystemen und anderen Mitteln der elektronischen Kommunikation wurden zeitweise fast täglich auch an die Mitarbeiter der Datenschutzaufsichtsbehörde herangetragen.

Die Arbeitsinhalte sind im Wesentlichen mit den dazu erfolgten Veröffentlichungen identisch.

Veröffentlichungen der Aufsichtsbehörde mit thematischem Bezug

- 15.04.2020 Hinweise zum Einsatz von Videokonferenzsystemen – kompakt –
- 18.04.2020 Anforderungen an Videokonferenzsysteme
- 18.04.2020 Datenschutz-Hinweise zu elektronischen Kommunikationsverfahren in der diakonischen Beratungstätigkeit
- 17.06.2020 Hinweise zu elektronischen Kommunikationsverfahren in der Seelsorge
- 20.08.2021 Planung des datenschutzkonformen Einsatzes eines Videokonferenzsystems - 12-Punkte-Liste für die Überprüfung

Tätigkeiten zu übergreifenden Themen

Diakonische Träger bestellen externe DSB ohne nachgewiesene Fachkunde für kirchliches Datenschutzrecht

Auch vier Jahre nach Inkrafttreten des mit der DS-GVO in Einklang gebrachten kirchlichen Datenschutzrechts ist der Fakt, dass in Kirche und Diakonie die DS-GVO keine Anwendung findet, vielen Datenschutz“fachleuten“ und selbst einigen gesetzlichen Vertretern von kirchlichen Einrichtungen noch immer nicht bekannt. Solche Vorfälle werden grundsätzlich beanstandet.

Die Aufsichtsbehörde hat Meldungen solcher Bestellungen nicht akzeptiert und eine Frist gesetzt, bis zu der die Bestellung geeigneter Personen erfolgt bzw. die Fachkunde nachgewiesen wird.

Fehlerhafte Datenschutzerklärungen

Auf Webseiten und in Dokumenten kirchlicher und diakonischer Träger wird die Aufsichtsbehörde immer noch fündig. Die Suche nach den Kürzeln „DSGVO“ oder „DS-GVO“ ergibt zahlreiche Treffer.

Die Datenschutz-Grundverordnung (DS-GVO) ist genauso wie das Bundesdatenschutzgesetz (BDSG) im Raum der verfassten Kirche und der Diakonie mit ihren Mitgliedern nicht anwendbar.

Entsprechend sind Dokumente, die die genannten Kürzel enthalten, sehr wahrscheinlich fehlerhaft.

Kein Versehen, sondern Fahrlässigkeit: Die E-Mail in Cc an Eltern als offener Verteiler

Besonders häufig sind Datenschutzverstöße bei Verwendung eines offenen E-Mail-Verteilers ohne Zustimmung jedes einzelnen Empfängers.

Immer wieder erreichen uns dazu Beschwerden. Es wird gern mit der Funktion des Cc-Empfängerfeldes gearbeitet, welche jedoch jedem Empfänger zeigt, welche weiteren Personen im Verteiler sind. Die E-Mail-Adressen der Adressaten sind somit für alle anderen Adressaten ersichtlich.

Dieser Verstoß ist keine Bagatelle. Leider kann technisch nicht oder in den meisten Fällen nur unzureichend eingegriffen werden, um solche Verstöße zu unterbinden.

Entsprechend häufig und eindringlich sollten entsprechende Sensibilisierungen von Mitarbeitern stattfinden. Soweit technisch möglich, sollte das Versenden von E-Mail mit mehreren Empfängern in den An- und Cc-Feldern an Empfänger außerhalb der eigenen E-Mail-Domäne unterbunden werden.

Durch das Benutzen des Bcc-Empfängerfeldes kann zumindest das Problem des offenen Verteilers umgangen werden. Hierbei erhalten sämtliche Adressaten im Verteiler nur die Adresse des Absenders, nicht aber den Überblick über sämtliche Adressen der Mit-Adressaten.

Cyberangriff soll Serverausfall erklären: Die Behandlung führt zur Datenschutzverletzung

Ein von einem diakonischen Träger als Datenpanne gemeldeter, vermeintlicher Cyber-Angriff unter angeblicher Ausnutzung der im März 2021 von Microsoft veröffentlichten Exchange-Server Sicherheitslücken stellte sich bei näherer Betrachtung durch die Aufsichtsbehörde als fehlerhaftes administratives Handeln dar.

Die von der Geschäftsleitung zugelassene Herausgabe der Datenträger des Servers an die

Polizei ohne richterlichen Beschluss, statt an einen spezialisierten Dienstleister (mit Vertrag zur Auftragsverarbeitung und Vertraulichkeit), stellte die Datenschutzverletzung durch Preisgabe von Exchange-Serverdaten mehrerer Jahre dar.

Ein „Beifang“ könnte zu staatsanwaltlichen Ermittlungen gegen Personen führen, deren Daten nur aufgrund der freiwilligen Datenübergabe an die Polizei zugänglich wurden. Diese Personen könnten ihrerseits Schadenersatzansprüche aus dieser Datenschutzverletzung geltend machen.

Zusammenarbeit mit Auftragsverarbeitern, die dem Geltungsbereich der DS-GVO unterliegen

Einige Anfragen betrafen die Zusammenarbeit mit Auftragnehmern, die nicht unter die Geltung des DSG-EKD fallen. Die Aufsichtsbehörde hat auf § 30 Abs. 5 DSG-EKD verwiesen, nach dem Auftragnehmer, die unter den Geltungsbereich der DS-GVO fallen, sich dennoch der kirchlichen Datenschutzaufsicht unterwerfen müssen. Eine entsprechende Formulierungshilfe wurde von der Aufsichtsbehörde gegeben.

Eine Zusammenarbeit mit Dienstleistern, die nicht dem kirchlichen Recht unterliegen und die gleichzeitig die geforderte Unterwerfung unter die kirchliche Datenschutzaufsicht ablehnen, wird vom Datenschutzbeauftragten für Kirche und Diakonie in seinem Zuständigkeitsbereich als Aufsichtsbehörde nur in den Fällen geduldet, in denen es nachweislich keine alternativen Anbieter gibt.

Bei vermuteten Datenschutzverstößen des Auftragsverarbeiters wird die Aufsichtsbehörde alternativ auf der Grundlage von Art. 56 DS-GVO i. V. m. Art. 60 DS-GVO aktiv. Art. 56 DS-GVO regelt das Verhalten von Aufsichtsbehörden dahingehend, dass „jede Aufsichtsbehörde dafür zuständig [ist], sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen die Verordnung zu befassen, wenn der Gegenstand […] betroffene Personen […] erheblich beeinträchtigt.“ Da gemäß Art. 91 Abs. 2 DS-GVO spezifische (kirchliche) Aufsichtsbehörden die Bedingungen in Kapitel VI DS-GVO erfüllen müssen, ist der Zugang zum Verfahren nach Art. 56 DS-GVO auch für die kirchliche Aufsichtsbehörde eröffnet.

Information, Empfehlung, Ausblick

Festgestellt

Die Datenschutz-Grundverordnung (DS-GVO) findet keine Anwendung im Bereich von Kirche und Diakonie. Gleiches gilt für das Bundesdatenschutzgesetz (BDSG), das zu den datenschutzrelevanten Aspekten, die unter das Selbstverwaltungsrecht der Kirchen subsumiert werden, schweigt.

Ob Gesellschaften, Stiftungen oder Träger und Einrichtungen, egal welcher Rechtsform, zum „Rechtsraum der Kirche“ gehören und damit ausschließlich das DSG-EKD anwenden, entscheiden die Kirchen durch Gesetz bzw. auf der Grundlage einer Zuordnungsentscheidung. Die Satzungen der Diakonischen Werke regeln die Zuordnung ihrer Mitglieder zum kirchlichen Bereich.

Informationen für jeden Bedarf

Vielfältige Informationsangebote der kirchlichen und staatlichen Aufsichtsbehörden und weiterer Akteure unterstützen die verantwortlichen Stellen:

Der Datenschutzbeauftragte für Kirche und Diakonie der Ev.-Luth. Landeskirche Sachsens

- https://datenschutz.dsbkd.de

Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland

- https://datenschutz.ekd.de

DIE STIFTUNG DATENSCHUTZ

- https://stiftungdatenschutz.org

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Datenschutzkonferenz (DSK)

- https://www.datenschutzkonferenz-online.de

Der Europäische Datenschutzausschuss

https://edpb.europa.eu/edpb_de

Die Anwendung des geltenden Datenschutzrechts gemäß den kirchlichen Gesetzen und Verordnungen zum Datenschutz oder der Datenschutz-Grundverordnung im nicht-kirchlichen Bereich ist in der Praxis weitgehend einheitlich.

Deshalb sind die jeweiligen Veröffentlichungen grundsätzlich auch für alle kirchlichen und diakonischen Stellen anwendbar.

Datenschutz ist ein Grundrecht

Die Empfehlung dazu lautet, sich diesen Umstand immer wieder bewusst zu machen und sich für die Rechte und Freiheiten derer, die geschützt werden sollen, proaktiv einzusetzen.

Datenschutz ist als Primärrecht europarechtlich geregelt und findet in Deutschland Entsprechung in den Artikeln 1 und 2 des Grundgesetzes in Verbindung mit den maßgeblichen Entscheidungen des Bundesverfassungsgerichtes zu Fragen der Auslegung und Konkretisierung.

Mehr Mensch geht nicht, Datenschutz in Kirche und Diakonie

Kirche ist in einer der Definitionen dieses Begriffs die Summe der Getauften und Glieder am Leib Christi. „Mehr Mensch geht nicht“ könnte es stark vereinfacht heißen.

Kirche ist eine Gemeinschaft von Menschen, die für- und miteinander in der sie umgebenden Gesellschaft, gemäß dem Auftrag ihres HERRN Jesus Christus, leben und arbeiten.

Diakonie, die Sorge um und an den Nächsten ist Lebens- und Wesensäußerung der Kirche. Die Sorge um die Nächsten schließt den Respekt der Individualität und Intimität jedes Einzelnen ein.

Sich für den Datenschutz einzusetzen, ist ein Teil der Fürsorge für den Nächsten im christlichen Sinn.

Gemeinsam besser werden

Beratung und Austausch werden auch künftig die Schwerpunkte sein, die der Datenschutzbeauftragte für Kirche und Diakonie in seiner Arbeit setzt.

Datenschutzaufsicht wird zuerst als Aufgabe zur Unterstützung aufgefasst. Dass geltendes Recht respektiert und umgesetzt wird, muss fortwährend unterstützt und gegebenenfalls auch durchgesetzt werden.