Unabhängige Aufsichtsbehörde
für den Datenschutz
Evangelisch-Lutherische
Kirche in Norddeutschland

Baustr. 34
17109 Demmin
Tel. +49 3998 2598478
peter.loeper@dsb.nordkirche.de
www.datenschutz-nordkirche.de

Bericht des Beauftragten für den Datenschutz der Evangelisch-Lutherischen Kirche in Norddeutschland an die Landessynode und Kirchenleitung

Hohes Präsidium, sehr verehrte Synodale!

Heute halte ich Ihnen nach § 41 Datenschutzgesetz EKD (DSG-EKD) meinen Bericht über die Situation des Datenschutzes in der Nordkirche.

Das Präsidium hat gebeten, dass ich mich kurzfasse. Datenschutz kann zugegebenermaßen ja auch ein wenig mühsam sein, oft so pingelig klein-klein. In meinem mündlichen Bericht werde ich daher nur auf die Auswirkungen des sogenannten Schrems-II-Urteils des Europäischen Gerichtshofes (EuGH) für unsere Kirche sowie die Vorlage zur Übertragung der Datenschutzaufsicht auf die EKD eingehen.

Im schriftlichen Bericht, der auf unserer Internetseite veröffentlicht wird, finden Sie dann insb. noch Ausführungen zu Corona und Datenschutz, die Evaluation des Datenschutzgesetzes EKD, Schulungen, Datenpannen und Einzelfällen natürlich ohne Namen. Besonders hervorheben möchte ich aus dem schriftlichen Bericht den Punkt Kirchliches Datenschutzmodell (KDM). Gemeinsam mit den Aufsichtsbehörden der römisch-katholischen Kirche ist es gelungen, eine Parallele zum staatlichen Standarddatenschutzmodell zu entwickeln und zu veröffentlichen. Ein sehr hilfreiches Werkzeug für die kirchlichen Praxis.

Hinweisen möchte ich darauf, dass beim Nomosverlag ein Kommentar zum evangelischen Datenschutzrecht erarbeitet wird. In bescheidenem Umfang darf ich als Bearbeiter daran mitwirken. Dieser Kommentar wird hoffentlich ebenfalls für die Praxis und die gleichmäßige Anwendung des Datenschutzrechtes hilfreich sein.

Bevor ich aber in die Themen einsteige, will ich Ihnen über eine Feststellung berichten, die mich in den letzten beiden Jahren immer wieder erstaunt hat: Kirchliche Stellen sind gesetzlich verpflichtet,

- Datenschutzkonzepte gem. § 5 Abs. 2 DSG-EKD,
- IT-Sicherheitskonzepte seit 31.12.2017 gem. § 7 IT-Sicherheitsverordnung EKD und ggf.
- Verfahrensverzeichnisse seit 30.06.2019 gem. § 55 Abs. 4 Satz 2 DSG-EKD

zu erstellen, oder besser: bereits erstellt zu haben.

Unabhängig von der kirchlichen Ebene musste ich vor allem im Bereich der verfassten Kirche in den meisten Fällen feststellen, dass davon nur wenig fertig vorhanden ist. Es werden

Daten quasi ohne Netz und doppelten Boden verarbeitet. Dabei ist häufig sogar das Bewusstsein vorhanden, dass es sowohl riskant als auch rechtswidrig ist. Selbst in Bereichen, in denen sensibelste Daten mit sehr hohem Schutzbedarf verarbeitet werden, sind erhebliche Mängel im Datenschutz festzustellen. Und auch in diesen Bereichen hat es schon Datenpannen mit entsprechend hohem Risiko gegeben. Stellen Sie sich doch bitte einmal vor, dort kommt es zu einer Datenpanne mit Außenwirkung. Was für ein Reputationsschaden für unsere Kirche ginge damit einher.

Die Anzahl der Datenpannenmeldungen nimmt immer weiter zu. Auch der Datenschutzbeauftragte EKD stellt das fest. Beispiele sind unten unter Einzelfälle zu finden. Entgegen der Hoffnung ist die Grundregel: alles was schief gehen kann, geht irgendwann schief. Wenn die Handhabung des Datenschutzes weiterhin nur als Hindernis gesehen wird, warne ich davor, dass es nicht mehr lange dauern wird, bis wir eine Datenpanne mit erheblicher Außenwirkung haben werden.

Persönlich verstehe ich diesen häufig in unserer Kirche anzutreffenden Umgang mit personenbezogenen Daten nicht. Das Datenschutzgesetz und die IT-Sicherheitsverordnung sind doch Regeln, die wir uns als Kirche selbst gegeben haben, und sie sollen die durch die Verfassung garantierten Grundrechte von uns allen schützen.

Als Grund wird dann häufig angeführt, dass es an den notwendigen personellen Ressourcen fehle. In vielen Fällen ist feststellbar, dass wirklich nicht genügend Stellenanteile zur Verfügung gestellt werden. Das geht so weit, dass schlicht eine mitarbeitende Person ausgeschaut wird, die den örtlichen Datenschutz ohne Stellenanteile „mitzumachen“ hat.

Aber oft ist es auch mangelnde Planung. Wenn Datenschutz bei einem Projekt oder einer neuen Aufgabe oder neuen Programmen von vornherein mitgedacht würde, ist das kaum Mehraufwand. Vielmehr führt das zu klaren Prozessen und Verantwortlichkeiten. Tatsächlich ist wirksamer Datenschutz nur möglich, wenn diese Verwaltungs- oder Geschäftsprozesse mit der notwendigen Pingeligkeit durchstrukturiert sind und klar ist, wer welche Entscheidungen zu treffen hat. Nach meinen Erfahrungen fehlt es daran nicht selten. So war bei durchgeführten Prüfungen oft schon unklar, wer eigentlich die verantwortliche Stelle ist.

Neben meiner ausdrücklichen Warnung vor dem nicht unerheblichen Risiko für unsere Kirche will ich heute daran appellieren, den Datenschutz ernster zu nehmen, ihn als elementaren Schutz der Grundrechte und sogar als Chance für die Prozessoptimierung zu verstehen.

1. Schrems-II-Urteil und seine Folgen

Kurz will ich auf die Folgen des sogenannten Schrems-II-Urteils des EuGH vom 16.07.2020 eingehen. Ausführlich wird dieses Thema behandelt z.B. in einer gemeinsamen Stellungnahme der Datenschutzbeauftragten in der EKD, die auf unserer Internetseite zu finden ist, und in mehreren Verlautbarungen der Datenschutzkonferenz des Bundes und der Länder, zu finden unter www.datenschutzkonferenz-online.de, mit Verweisen auf den Europäischen Datenschutzausschuss.

US-amerikanische IT-Dienstleister sind führend in vielen Bereichen, sowohl bei Software als auch bei IT-Infrastruktur z.B. Microsoft, Google, Facebook, Amazon. Diese Unternehmen

haben in manchen Bereichen fast so etwas wie eine Monopolstellung. Auch kirchliche Einrichtungen wollen vielfach diese Produkte einsetzen.

Bei der Nutzung dieser Produkte werden personenbezogene Daten in die USA übermittelt. Bisher geschah das in der Regel auf der Grundlage des sog. Privacy-Shields-Abkommens zwischen den USA und der EU.

Der EuGH hat das untersagt, insb. weil die Zugriffsrechte der US-amerikanischen Sicherheitsbehörden zu weitgehend seien und EU-Bürger keinen hinreichenden Rechtsschutz in den USA haben.

Eine Übermittlung personenbezogener Daten in die USA sei aber grundsätzlich noch aufgrund von sog. Standardvertragsklauseln zulässig. Die werden von der EU verabschiedet. Dann aber haben die für die Datenübermittlung Verantwortlichen eine ergänzende Prüfung durchzuführen, ob die Rechtslage oder die Praxis in dem jeweiligen Drittland dem Schutzniveau in der EU entspricht. Ist das nicht der Fall, sind weitere Schutzmaßnahmen zu treffen.[1]

Was bedeutet das für Übertragungen von personenbezogenen Daten in die USA? In seinem Urteil hat der EuGH ja selber das Datenschutzniveau in den USA im Detail geprüft und eben für unzureichend befunden. Im Fall von Datenübermittlungen in die USA sind daher regelmäßig ergänzende Maßnahmen erforderlich, die einen Zugriff der US-Behörden auf die verarbeiteten Daten verhindern[2]. Das gilt wegen des CLOUD-Act (Clarifying Lawful Overseas Useof Data Act vom 20.03.2018) auch für die Datenübermittlung an in Europa ansässige Tochterunternehmen von US-amerikanischen Unternehmen z.B. in Irland. Verhindert werden kann der Zugriff insbesondere durch die sichere Verschlüsselung der Daten, bevor sie in die Cloud gelangen. Dafür gibt es Verfahren am Markt. Wie ein Transfer von personenbezogenen Daten in die USA bei der Nutzung von Facebook-Fanpages verhindert werden kann, ist bisher nicht ersichtlich.

Um es deutlich zu sagen: unverschlüsselte Transfers personenbezogener Daten in die USA sind nach den Feststellungen des EuGH zurzeit rechtswidrig. Mir ist durchaus bewusst, dass das von vielen nicht gehört werden will. Ich erlebe aber ein immer breiter werdendes Bewusstsein, dass Menschen sich den Datensammlern in den USA nicht ausliefern wollen.

Auch die Politik arbeitet „schon“ an einer europäischen Verwaltungscloud, um sich zu befreien und staatliche Daten zu sicher. Und meine Hoffnung ist, dass bei Kenntnis der Rechtslage der Europäische Gerichtshof und seine Entscheidungen respektiert werden.

2. Übertragung der Datenschutzaufsicht der Nordkirche an die EKD

In meinem letzten Bericht vor zwei Jahren hatte ich darauf hingewiesen, dass die Kapazitäten in der Datenschutzaufsicht nach Einführung der EU-Datenschutzgrundverordnung und des neuen Datenschutzgesetz EKD nicht mehr ausreichen, und vorgeschlagen, die Datenschutzaufsicht über die Diakonie auf die EKD zu übertragen. Mittlerweile ist daraus die Vorlage

[1] DSK Pressemitteilung vom 21.06.2021 S. 1, www.datenschutzkonferenz-online.de

[2] DSK Pressemitteilung vom 21.06.2021 S. 2, www.datenschutzkonferenz-online.de

entstanden, die Datenschutzaufsicht in zwei Stufen insgesamt auf die EKD zu übertragen. Das wird gleich unter TOP 3.2 eingebracht und erörtert.

Ich möchte nur auf einen Aspekt hinweisen. Es gibt bereits eine sehr enge Kooperation zwischen den Datenschutzaufsichten der EKD und der Nordkirche. Ich bin zum Vertreter des Datenschutzbeauftragten EKD bestellt und bin intensiv in den Schulungsbetrieb eingebunden. Es gibt einen regelmäßigen und strukturierten Austausch. Wir teilen uns Aufgaben. So habe ich z.B. für die ganze EKD Verhandlungen mit Microsoft geführt.

In den vorgelegten Entwürfen der Übertragungsverträge zwischen Nordkirche und EKD ist die Möglichkeit aufgenommen, dass die Datenschutzbeauftragten EKD und Nordkirche eine Zusatzvereinbarung abschließen. Wir haben einen Entwurf erarbeitet.

Danach wird der Datenschutzbeauftragte EKD vom Datenschutzbeauftragten Nordkirche nach § 42 Abs. 4 DSG-EKD zu seinem Vertreter bestellt. Damit ist meine Abwesenheitsvertretung sichergestellt. Die Vertragsparteien gestalten einen gemeinsamen Internetauftritt. Dafür werden bisherige Inhalte der Datenschutz-Internetseite Nordkirche in die Internetseite des Datenschutzbeauftragten EKD eingebunden. Die Weiterbildungsangebote des Datenschutzbeauftragten EKD können bereits ab Januar 2022 von allen verantwortlichen Stellen auf dem Gebiet der Nordkirche wahrgenommen werden.

Ein besonderes Anliegen der Diakonie war es, eine einheitliche Aufsicht über die diakonischen und verfasst-kirchlichen Kindertageseinrichtungen sicher zu stellen. Dazu soll vereinbart werden, dass die Datenschutzaufsicht über alle Kindertageseinrichtungen - unabhängig von der Frage der Trägerschaft - bereits ab Januar 2022 vom Datenschutzbeauftragten EKD erledigt wird. Sofern es sich um Kindertageseinrichtungen in verfasst-kirchlicher Trägerschaft handelt, werden die Aufgaben vom Datenschutzbeauftragter EKD in Vertretung gemäß § 1 dieser Vereinbarung wahrgenommen. Ab dem 01. Januar 2022 kann der Datenschutzbeauftragte Nordkirche an den regelmäßigen internen Besprechungen des Datenschutzbeauftragten EKD teilnehmen. Abgeschlossene Sachakten des Datenschutzbeauftragten Nordkirche verbleiben am Ort der Entstehung. Laufende Sachakten zum Zeitpunkt der Übertragung der Datenschutzaufsicht auf den Datenschutzbeauftragten EKD werden an diesen übergeben.

Wir denken, dass wir mit diesem Vereinbarungsentwurf eine verantwortliche Regelung für die Übergangszeit zwischen 1. und 2. Stufe gefunden haben.

Nur Schriftlich:

3. Corona und Datenschutz

Die Corona-Pandemie und die damit zusammenhängenden Fragen haben die Beratungstätigkeit der kirchlichen Datenschutzaufsicht in vielfältiger Weise in Anspruch genommen. Folgende Fragen sollen hier beispielhaft genannt werden:

- Wie kann bei Gottesdiensten oder anderen kirchlichen Veranstaltungen die Erfassung der Kontaktdaten der Besucher bzw. Teilnehmenden zum Zwecke der Nachvollziehbarkeit der Infektionsketten datenschutzkonform gestaltet werden?
- Darf die Luca-App zur Kontaktdatenerfassung verwendet werden?
- Darf vor Veranstaltungen/Gottesdiensten die Körpertemperatur der Teilnehmenden gemessen werden?
- Darf der Impfstatus abgefragt werden? Darf er gespeichert werden?
- Welche Videokonferenzsysteme dürfen eingesetzt werden?
- Was ist beim Homeoffice aus Datenschutzsicht zu beachten?

Die Beauftragten für den Datenschutz der EKD und der Nordkirche haben frühzeitig zu wesentlichen Fragen im Zusammenhang mit Corona gemeinsam Stellung genommen:

- Gemeinsame Stellungnahme zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Corona-Pandemie vom 20.03.2020 (https://www.datenschutz-nordkirche.de/fileadmin/user_upload/baukaesten/Baukasten_Datenschutz_Nordkirche/Dokumente/20200320-Stellungnahme-Corona.pdf)
- Gemeinsame Stellungnahme zum Homeoffice im Zusammenhang mit der Corona-Pandemie vom 27.03.2020 (https://www.datenschutz-nordkirche.de/fileadmin/user_upload/baukaesten/Baukasten_Datenschutz_Nordkirche/Dokumente/Stellungnahme_Homeoffice-NoKi.pdf)

Die häufig wechselnden und in den einzelnen Bundesländern oftmals unterschiedlichen Regelungen zu Corona haben aber dazu geführt, dass viele Fragen immer wieder neu bewertet werden mussten.

4. Evaluation DSG-EKD

Nach § 54 Abs. 4 DSG-EKD ist das Datenschutzgesetz der EKD binnen fünf Jahren, also bis Ende Mai 2023, zu evaluieren. Die Evaluation wird durch die EKD, die Landeskirchen und die Aufsichtsbehörden vorbereitet. Auch die Aufsichtsbehörde der Nordkirche hat zu diesem Zweck eine umfangreiche Liste mit Änderungs- und Formulierungsvorschlägen erarbeitet und an das Kirchenamt der EKD übermittelt.

5. Schulungen

Gemeinsam mit dem Datenschutzbeauftragten der EKD werden im Rahmen der bisherigen Kooperation dreitägige Schulungen für örtliche Beauftragte für den Datenschutz auch auf dem Gebiet der Nordkirche durchgeführt. An allen Schulungen dürfen Nordkirchler teilnehmen. Die Nordkirchenaufsicht stellt Referenten.

Wegen Corona mussten die Präsenzschulungen 2020 aussetzen. Es wurde ein Onlineformat entwickelt, das seit Anfang 2021 angeboten wird. Ein Seminar wurde im September in Präsenz auf dem Gebiet der Nordkirche durchgeführt.

Es wurden zwei Online-Schulungen zum Datenschutz in Kindertagesstätten (März und April 2021) angeboten. Der regelmäßige Erfahrungsaustausch innerhalb der Nordkirche musste 2020 wegen Corona aussetzen.

6. Kirchliches Datenschutzmodell (KDM)

Auf dem ökumenischen Datenschutztag der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche und der Konferenz der Beauftragten für den Datenschutz in der Evangelischen Kirche in Deutschland am 21. April 2021 ist das Kirchliche Datenschutzmodell (KDM) verabschiedet worden.

In den letzten beiden Jahren hatte sich, auf der Grundlage eines entsprechenden Beschlusses der evangelischen und katholischen Datenschutzaufsichtsbehörden aus dem Jahr 2019, eine ökumenische Arbeitsgruppe, auch unter Beteiligung der Nordkirche, intensiv mit der Übernahme des im staatlichen Bereich eingeführten Standard-Datenschutzmodells (SDM) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder befasst.

Die ökumenische Arbeitsgruppe hat dabei das SDM auf die in der katholischen und evangelischen Kirche geltenden Datenschutzvorschriften unter Beibehaltung der Methodik der staatlichen Vorlage angepasst.

Das Kirchliche Datenschutzmodell (KDM) bietet geeignete Mechanismen, um die Anforderungen der kirchlichen Datenschutzgesetze in technische und organisatorische Maßnahmen zu überführen. Mit dem KDM haben die kirchlichen Datenschutzaufsichtsbehörden ein Werkzeug, das es ihnen ermöglicht, Prüfungen standardisiert und damit auch nachvollziehbarer durchzuführen. Gleichzeitig bietet das KDM aber auch den kirchlichen Stellen und Einrichtungen den großen Vorteil, selbst Datenschutz systematisch umzusetzen und damit für Fragen und Prüfungen der Datenschutzaufsichten gut vorbereitet zu sein.

Das KDM und weiteres Informationsmaterial sind auf der Internetseite https://kirchliches-datenschutzmodell.de zu finden.

7. Datenpannen

Die Zahl der Datenpannenmeldungen hat sich deutlich erhöht. Das liegt auch daran, dass die Verpflichtung zur Datenpannenmeldung bekannter geworden ist. Es gibt häufig Verluste von Notebooks oder Handys. Ob damit ein hohes Risiko einhergeht, hängt von der IT-Sicherheit

auf den Geräten ab. Die ist sehr unterschiedlich ausgeprägt. Das Sicherheitsniveau hängt in der Regel nicht mit dem Risiko, sondern mit der Aufmerksamkeit der Einrichtung für den Datenschutz zusammen.

Auch sehr häufig gibt es falsche Adressaten beim Versenden von E-Mails oder Faxen. Oder ein Ordner mit hochsensiblen Daten wird durch einen menschlichen Fehler in einen allgemein zugänglichen Ordner verschoben. Das hört sich belanglos an, hat aber oft gravierende Folgen, wenn etwa der Bericht über einen Heimbewohner in einen großen Verteiler gesendet wird oder Überlegungen zu Abmahnungen durch die gesamte Belegschaft eingesehen werden können. **Für mich ist die Erkenntnis daraus, dass eine elektronische Aktenverwaltung für bestimmte sehr risikobehaftete Datenverarbeitung schlicht nicht geeignet ist. Selbst wenn es keine Sicherheitslücken gäbe, sind IT-Prozesse für Fehler aufgrund menschlichen Versagens gefährdeter.** Ein Klick und die Daten sind draußen und sie können nicht mehr zurückgeholt werden.

Auch zu verzeichnen sind immer wieder Einbrüche und der Verlust von Daten. Damit wird häufig nicht gerechnet.

Hervorzuheben ist noch die große Zahl von Meldungen nach der kritischen Sicherheitslücke bei Exchange Servern (März 2021).

Nach Datenpannen stellt sich die Frage, ob und wie die Betroffenen zu informieren sind. Das sind außerordentlich schwere Entscheidungsprozesse. Oben habe ich vor dem damit einhergehenden Reputationsschaden für die Kirche gewarnt. Ich wiederhole diese Warnung hier.

7. Einzelfälle

Nachfolgend einige Fälle als Beispiele für die verschiedenartigen Tätigkeiten der Aufsichtsbehörde

- Abberufung einer örtlich Beauftragten für den Datenschutz (öDSB) ohne Rechtsgrundlage: Die Abberufung von öDSB ist nur zulässig in entsprechender Anwendung des § 626 BGB (fristlose Kündigung aus wichtigem Grund). Die kirchliche Stelle legte der öDSB gravierende Datenschutzmängel zur Last. Aber die aufgelistete Mängel waren Versäumnisse bei der Umsetzung der datenschutzrechtlichen Bestimmungen. ÖDSB wirken laut Gesetz auf die Einhaltung der Datenschutzbestimmungen hin, die Umsetzung der datenschutzrechtlichen Bestimmungen ist aber Aufgabe der Leitung der verantwortlichen Stelle, nicht der örtlich Beauftragten für den Datenschutz. Und örtlich Beauftragte für den Datenschutz können ihre Aufgaben nur erfüllen, wenn die verantwortliche Stelle sie dabei unterstützt und ihnen dafür ausreichende Ressourcen zur Verfügung stellt. Insbesondere müssen sie mit einem zur Erfüllung ihrer Aufgaben angemessenen Zeitanteil ausgestattet sein. Das war hier bei Weitem nicht der Fall. Es wurde eine Beanstandung ausgesprochen.
- Der Entwicklungsbericht eines Heimbewohners wird per Mail in einen größeren Verteiler geschickt.

- Einbruch in der 4. Etage durchs Fenster und die Entwendung eines Laptops mit höchst sensiblen Daten
- Gemeindebriefe als PDF mit Fotos und Kasualiendaten ohne Einwilligung im Internet
- Bei einem großen diakonischen Träger sendet die Telefonanlage die Faxe an andere Empfänger
- Faxversand von Gesundheitsdaten per Fax über VoIP, d.h. offen über das Internet
- In einer diakonischen Einrichtung gab es in der EDV einen Ordner, zu dem nur die Leitungskräfte Zugang hatten. Dort waren hochsensible Daten insbesondere von Mitarbeitenden gespeichert bis hin zu Überlegungen zu Abmahnungen. Durch einen menschlichen Fehler wurde dieser Ordner in einen allgemein zugänglichen Ordner verschoben mit der Folge, dass alle Mitarbeitenden Zugang hatten.
- Beschwerde einer Patientin einer kirchlichen Klinik: Während ihres Aufenthaltes war ihr erlaubt worden, im Dienstzimmer der Station ein Telefongespräch zu führen. Dabei konnte sie direkten Einblick in hoch sensible Patientendaten nehmen, unter anderem einen vorläufigen Entlassungsbericht einer Mitpatientin inkl. Grund der Aufnahme und Diagnose. Die Mitarbeitenden der Klinik wurden angewiesen, dafür Sorge zu tragen, dass beim Telefonieren keine Patienten- oder Mitarbeiterdaten einsehbar sind.
- Veröffentlichung von Fotos einer Mitarbeiterin oder von Kindern im Internet ohne Einwilligung
- Eine Mitarbeiterin in der ambulanten Pflege stellt fest, dass in den Räumlichkeiten der Klientin Kameras zur Überwachung installiert worden sind. Wir haben der Einrichtung geraten, darauf zu bestehen, dass die Kamera in der Zeit, in der die/der Mitarbeitende die Klientin versorgt, die Kamera inkl. Tonaufnahme komplett ausgeschaltet wird, und ansonsten die Versorgung abzulehnen.
- Darf eine verantwortliche Stelle mit Einwilligung der betroffenen Person sensible personenbezogene Daten auch unverschlüsselt per E-Mail versenden? Nach h.M. sind die in § 27 DSG-EKD genannten Anforderungen nicht abdingbar.
- Anschreiben durch die Kirchengemeinde von Personen, die aus der Kirche ausgetreten sind: Grundsätzlich müssen personenbezogene Daten gelöscht werden, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind. Das bedeutet aber nicht, dass man die Daten der Ausgetretenen sofort nach Austritt löschen müsste. Es kann durchaus als kirchliche Aufgabe angesehen werden, ein Kirchenmitglied, das ausgetreten ist, nicht „sang- und klanglos“ ziehen zu lassen, vielleicht sogar zu versuchen, es dazu zu bewegen, seine Entscheidung noch einmal zu überdenken oder zumindest die Gründe für seinen Austritt in Erfahrung zu bringen, um daraus Schlüsse für die kirchliche Arbeit zu ziehen. Rechtsgrundlage dafür wäre § 6 Nr. 3 DSG-EKD. Allerdings muss dies zeitlich in engem Zusammenhang mit dem Austritt geschehen. Eine schriftliche Nachfrage innerhalb von 4-6 Wochen nach Kenntnisnahme des Austritts wäre vertretbar.

Auf der Synode wurde nach meinem mündlichen Bericht gefragt, ob die Situation des Datenschutzes in der Nordkirche im Großen und Ganzen in Ordnung sei. Ich konnte das nicht

bestätigen, sondern muss auf die Gefahren des oftmals nicht ausreichenden Datenschutzes und IT-Sicherheitsschutzes für die Betroffenen und unsere Kirche hinweisen.

November 2021

Peter Loeper
Beauftragter für den Datenschutz
der Nordkirche