Unabhängige Aufsichtsbehörde
für den Datenschutz
Evangelisch-Lutherische
Kirche in Norddeutschland

Büro der Landessynode

TOP 2.2

12. Tagung der II. Landessynode 11/2021

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 kurz fasse. 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[1] 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[2]. 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[3],
- IT-Sicherheitskonzepte seit **2017**[4] und ggf.
- Verfahrensverzeichnisse seit **2019**[5]

zu erstellen, oder besser: bereits erstellt zu haben.

[1] (EuGH)
[2] (KDM)
[3] gem. § 5 Abs. 2 DSG-EKD
[4] 31.12.2017 gem. § 7 IT-Sicherheitsverordnung EKD
[5] 30.06.2019 gem. § 55 Abs. 4 Satz 2 DSG-EKD

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 sensibleste 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[6] 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 von 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-Urteil des EuGH vom 16.07.2020 eingehen. Ausführlich wird dieses Thema behandelt z.B. in einer gemeinsamen Stellungname der

[6] 1. Leitungsordner, 2. Einbruch 4. Etage

Datenschutzbeauftragten in der EKD[7] und in mehreren Verlautbarungen der Datenschutzkonferenz des Bundes und der Länder[8] 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-Abkommen 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.[9]

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[10][11]. 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 zur Zeit 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.

Die Andacht heute hat diese Sorgen aufgenommen und eingeordnet. Dafür bin ich dankbar.

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

[7], die Sie auf unserer Internetseite finden,
[8], zu finden unter www.datenschutzkonferenz-online.de
[9] DSK Pressemitteilung vom 21.06.2021 S. 1, www.datenschutzkonferenz-online.de
[10] DSK Pressemitteilung vom 21.06.2021 S. 2, www.datenschutzkonferenz-online.de
[11] Das gilt wegen des CLOUD-Act (Clarifying Lawful Overseas Useof Data Act vom 20.03.2018) auch für die Datenübermittlung an in Europa ansässigen Tochterunternehmen von US-amerikanischen Unternehmen z.B. in Irland.

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 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 der Datenschutzaufsichten der EKD und der Nordkirche. Ich bin zu seinem Vertreter 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 Übertragungsverträgen 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 zu seinem Vertreter bestellt[12]. Damit ist meine Abwesenheitsvertretung sichergestellt. Die Vertragsparteien gestalten einen gemeinsamen Internetauftritt.[13] 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 Datenschutzbeauftragter EKD erledigt wird.[14]

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

Vielen Dank für Ihre Aufmerksamkeit!

[12] § 42 Abs. 4 DSG-EKD

[13] Dafür werden bisherige Inhalte der Datenschutz-Internetseite Nordkirche in die Internetseite des Datenschutzbeauftragten EKD eingebunden.

[14] 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 Datenschutzbeauftragter Nordkirche an den regelmäßigen internen Besprechungen des Datenschutzbeauftragter EKD teilnehmen. Abgeschlossene Sachakten des Datenschutzbeauftragter Nordkirche verbleiben am Ort der Entstehung. Laufende Sachakten zum Zeitpunkt der Übertragung der Datenschutzaufsicht auf den Datenschutzbeauftragter EKD werden an diesen übergeben.