

Abschlussbericht 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 meinen turnusgemäßen Bericht über die Situation des Datenschutzes in der Nordkirche¹. Gleichzeitig ist dies mein Abschlussbericht an Sie.

Ich verweise in meinem Bericht auf verschiedenen Fundstellen. Die finden Sie in den Fußnoten. Der Bericht wird auf der Internetseite des Datenschutzbeauftragten der EKD daten-schutz.ekd.de veröffentlicht.

1. Datensicherheit

Zwei Beispiele zum Auftakt:

Am 15.08.2023 kommt die Nachricht, dass die Datensicherheit der Microsoftcloud im Auftrag des US-Präsidenten durch die Cyber Safety Review Board (CSRB)² untersucht wird. Hintergrund ist eine massive Datenpanne in der Microsoftcloud. Mutmaßlich chinesische Hacker haben einen Master-Key entwendet.³ Dadurch soll der Zugang zu fast allen Daten in der Microsoftcloud eröffnet gewesen sein. Microsoft selber hat bisher nicht mitgeteilt, welche Daten betroffen sind.

Schon einen Monat später am 19.09.23 geht eine neue Nachricht durch die Presse: Wieder hat es eine Datenpanne in der Microsoftcloud gegeben. 38 Terrabyte personenbezogene Daten seien im Netz offengelegt worden.⁴

Datensicherheit ist eins der großen aktuellen IT-Themen. Nach einer Untersuchung der Fa. IBM aus diesem Jahr sind die Kosten für Unternehmen für die Bewältigung von Datenpannen weltweit mittlerweile im Durchschnitt auf 4,45 Mio. US-Dollar pro Fall gestiegen⁵. Auch in unserer Landeskirche hat es schon Datenpannen z.B. durch Ransomware gegeben, deren Kosten in ähnliche Bereiche vorgestoßen sind.

¹ § 41 Datenschutzgesetz EKD (DSG-EKD)

² eine auf Datensicherheit spezialisierte Behörde

³ <https://www.heise.de/news/Microsofts-gestohlener-Master-Key-USA-stellen-Cloud-Security-auf-den-Pruefstand-9244487.html> m.w.Nachw.

⁴ <https://chatgpt-prompts.de/microsoft-ki-forscher-decken-massive-datenpanne-auf>

⁵ <https://www.it-business.de/kosten-einer-datenpanne-erreichen-hoch-a-fcb23915dd8b119edbd603a79917a74a/>

Die Angriffe werden immer ausgebuffter, so dass auch staatliche Stellen oder große Unternehmen wie z.B. Banken oder Versicherungen nicht davor gefeit sind. In der Presse hören wir wöchentlich von den großen Datenpannen.

Der EKD ist das Thema Datensicherheit lange bewusst. Sie hat schon am 29.05.2015 die IT-Sicherheitsverordnung beschlossen. Und sie hat weitere Regelungen im Datenschutzgesetz der EKD getroffen. Danach sind kirchliche Stellen gesetzlich verpflichtet,

- Datenschutzkonzepte (gem. § 5 Abs. 2 DSGVO-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 DSGVO-EKD

zu erstellen, oder besser: bereits erstellt zu haben. Ich zitiere aus meinem Bericht an Sie von vor zwei Jahren:

„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.“

Zitat Ende. Seitdem hat sich nicht viel getan. Ich kann nur davor warnen diese Schutzvorschriften weiterhin so wenig zu beachten, nicht nur der materielle Schaden einer Datenpanne kann immens sein. Wir wissen es doch alle.

2. Angemessenheitsbeschluss

Ein sog. Angemessenheitsbeschluss der EU-Kommission erlaubt den Datenverkehr in das EU-Ausland z.B. die USA. Das Safe-Harbour- und des Privacy-Shields-Abkommens waren solche Angemessenheitsbeschlüsse, bis sie vom EuGH aufgrund Klagen von Herrn Max Schrems aufgehoben wurden. Die EU-Kommission hat am 10.07.2023 einen neuen Angemessenheitsbeschluss zum Datenverkehr in die USA mit der Bezeichnung „EU-US-Data Privacy Framework“⁶ erlassen. Danach ist jetzt die Übertragung von personenbezogenen Daten in die USA grundsätzlich wieder zulässig.

Eine vertiefte Diskussion über den neuen Beschluss hat noch nicht stattgefunden. Es gibt aber schon Datenschutzaufsichtsbehörden die darauf hinweisen, dass bei einem erneuten Klageverfahren die ernsthafte Gefahr der erneuten Aufhebung des Angemessenheitsbeschlusses besteht⁷. Dies wird damit begründet, dass es keine wesentlichen Änderungen in der Datenschutz- und Rechtsschutzpraxis der USA für EU-Bürger gebe. Eine besonders

⁶ https://ec.europa.eu/commission/presscorner/detail/de/ip_23_3721

⁷ Z.B.: https://lfd.niedersachsen.de/startseite/themen/internationaler_datenvverkehr/datenubermittlung_in_die_usa_eu_erlasst_neuen_angemessenheitsbeschluss/datenubermittlung-in-die-usa-eu-erlasst-neuen-angemessenheitsbeschluss-223847.html und <https://datenschutz.hessen.de/daten-schutz/internationaler-datentransfer/eu-us-data-privacy-framework-in-kraft-getreten>

ausführliche und sehr lesenswerte Stellungnahme findet man beim Datenschutzbeauftragten von Thüringen⁸.

Schließlich wird berichtet⁹, dass Max Schrems erneut eine Klage anstrebt. Er wird mit seinem schönen Bonmot zitiert: *„Man sagt, die Definition von Wahnsinn sei, dass man immer wieder das gleiche tut und dennoch ein anderes Ergebnis erwartet“*.

Bis es ein breiteres Meinungsbild etwa von der Konferenz der Datenschutzbehörden des Bundes und der Länder (DSK) gibt, wird wohl noch einige Zeit vergehen. Jedes nationale Gericht kann aufgrund einer Klage das Verfahren dem EuGH vorlegen. Es steht zu erwarten, dass das bis Ende diesen oder Anfang nächsten Jahres erfolgen wird. Der EuGH braucht zwar ein bis zwei Jahre für seine Entscheidungen. Er kann aber für die Dauer des Verfahrens die Anwendung des Angemessenheitsbeschlusses sofort aussetzen.

3. Zusammenarbeitsplattform/Microsoft

Auf der letzten Synode haben Sie das IT-Gesetz und damit die Zusammenarbeitsplattform beschlossen. Sie wollen dort Microsoft 365 einsetzen. Sie haben in Art. 4 des Gesetzes einen Vorbehalt eingebracht, wonach es im Wesentlichen erst in Kraft tritt, wenn die Kirchenleitung die Datenschutzkonformität festgestellt hat.

Ich warne eindringlich davor, allein aufgrund des verabschiedeten „EU-US-Data Privacy Framework“ diesen Beschluss nach Art. 4 ITG zu fassen. Es besteht die nicht unerhebliche Gefahr, dass der Angemessenheitsbeschluss erneut aufgehoben wird. Investierte Gelder könnten dann verloren sein. Die Kirchenleitung habe ich direkt nach dem Erlass des Angemessenheitsbeschlusses auf diese Gefahren hingewiesen.

Nur mit dem neuen Angemessenheitsbeschluss ist die Datenschutzkonformität von Microsoft 365 sowieso noch nicht hergestellt. Ich verweise dazu auf meine ausführliche Stellungnahme auf der letzten Synode und gegenüber der Kirchenleitung. Microsoft erhebt von den Nutzern umfangreich personenbezogene Telemetriedaten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat festgestellt, dass eine völlige Abschaltung der Übertragung der Telemetriedaten nicht möglich sei¹⁰. Und Microsoft weigert sich standhaft mitzuteilen, welche Daten wofür erhoben und wie sie verarbeitet werden. Zu diesen Telemetriedaten hat die Datenschutzkonferenz des Bundes und der Länder festgestellt¹¹, dass zurzeit eine Nutzung von Microsoft 365 trotz des neuen Angemessenheitsbeschlusses rechtswidrig sei. Auch in einem zwei Jahre dauernden gemeinsamen Projekt zwischen der DSK und Microsoft war es trotz 14 langer Videokonferenzen nicht möglich datenschutzkonforme Einstellungen für die Telemetriedatenübermittlung zu finden.

⁸ [https://www.tfdi.de/fileadmin/tfdi/presse/Pressemitteilungen_2023/230714_PM_MS365 .pdf](https://www.tfdi.de/fileadmin/tfdi/presse/Pressemitteilungen_2023/230714_PM_MS365.pdf)

⁹ <https://www.heise.de/news/Kritik-an-Wahnsinn-EU-Kommission-gibt-Datentransfer-in-die-USA-wieder-frei-9212124.html>

¹⁰ <https://www.bsi.bund.de/dok/14859574>

¹¹ <https://datenschutz.ekd.de/2022/11/29/der-einsatz-von-microsoft-365-ist-weiterhin-nicht-datenschutzkonform-moeglich/>

Microsoft sagt einfach nicht, was es mit den Daten macht, das ist doch komisch. Wir müssen aber einem Betroffenen oder einem Mitarbeitenden bei einem Auskunftverlangen konkret sagen, was mit seinen erhobenen Daten geschieht.

Natürlich nicht zufällig habe ich am Anfang als Beispiele für Datenpannen zwei Vorfälle in der Microsoftcloud angeführt. Ich will Ihnen damit nur zeigen, dass es um die Datensicherheit bei Microsoft auch nicht so besonders bestellt ist. Auch die kochen nur mit Wasser.

Eine Gruppe staatlicher Datenschutzbehörden hat die Microsoftverträge geprüft und am 22.09.2023 eine 21-seitige Handreichung mit „Praxis-Tipps für Verträge mit Microsoft“ herausgegeben¹². Ich empfehle dringend die Lektüre und Beachtung vor Abschluss von Verträgen mit Microsoft.

Jeder Betroffene kann nach § 46 DSGVO Beschwerde gegen die Verarbeitung seiner Daten einlegen. Bei der Zusammenarbeitsplattform wäre das jedes Gemeindeglied und jeder Mitarbeitende deren Daten auf der Plattform verarbeitet werden. Aufgrund einer solchen Beschwerde muss die zuständige Datenschutzaufsicht spätestens tätig werden¹³. Das könnte letztlich die Untersagung der Verarbeitung auf der Zusammenarbeitsplattform zur Folge haben. Dieses unternehmerische und wirtschaftliche Risiko trägt die verantwortliche Stelle.

Ein – mein letztes Wort zur Zusammenarbeitsplattform: Sie ist ja grundsätzlich ein gutes Projekt, aber warum ausgerechnet mit Microsoft. Damit holen wir uns unabsehbare Probleme ins Haus. Wann und ob Microsoft ohne Einwilligung datenschutzkonform betrieben werden kann, weis kein Mensch. Es kann noch lange dauern. Die Zusammenarbeitsplattform soll doch losgehen. Es gibt Alternativen zu Microsoft. Andere Landeskirchen gehen diese alternative Wege, auch wenn sie ein wenig steiniger erscheinen. Vielleicht kann man da noch mal schauen. Zeit dafür ist ja bis Microsoft seine Intransparenz - vielleicht - aufhebt.

4. Übertragung der Datenschutzaufsicht der Nordkirche an die EKD

Bereits seit dem 01. Januar 2022 führt der Datenschutzbeauftragte der EKD die Datenschutzaufsicht über die Diakonie der Nordkirche, ab morgen auch über die verfasste Kirche. Es gibt schon seit geraumer Zeit eine enge Zusammenarbeit. Wir haben uns z.B. gegenseitig zu Vertretern bestellt und treten gemeinsamen im Internet auf. In Rechtsfragen haben wir uns eng abgestimmt. Auch zu Microsoft und Facebook gibt es eine gemeinsam erarbeitete Rechtsauffassung. Sie wurde auf der letzten gemeinsamen Dienstberatung wieder bestätigt. Sie werden keine Überraschungen erleben.

Die Datenschutzaufsicht über die gesamte Nordkirche wird ab morgen von einer gut bestellten und sehr kompetenten Behörde geführt werden. Sie ist etwas weiter weg, Sie

¹² <https://fd.niedersachsen.de/startseite/infothek/presseinformationen/einsatz-von-microsoft-365-praxis-tipps-fur-vertraege-mit-microsoft-225722.html>

¹³ VG Wiesbaden, Urteil vom 24. September 2021 – 6 K 442/21.WI – Leitsatz zu 1 und Rn.33ff, juris; Sydow, EU-DSGVO 2017, Art. 77 Rn.25; Herrlein in: Sydow, Kirchliches Datenschutzrecht 2020, § 48 Rn.8

werden z.B. den Beauftragten hier auf der Synode nur in Ausnahmefällen erleben, aber Sie werden eine hervorragende Expertise bekommen.

Am 08.09. hat die Kirchenleitung die Datenschutzdurchführungsverordnung auf Initiative des Datenschutzreferenten, Herrn Dr. Triebel, an die neue Situation angepasst.

Der Übergang morgen sollte nahtlos klappen.

5. Schulungen

Die Nachfrage nach Schulungen nimmt im gesamten Bereich der EKD signifikant ab. Gab es vor zwei Jahren noch lange Wartelisten müssen jetzt Schulungsangebote mangels Teilnehmern abgesagt werden. Und das, obwohl flächendeckend Datenschutzkonzepte und Verfahrensverzeichnisse fehlen und die Gefährdung durch komplexere Systeme und gefährlicherer Angriffe steigt - eine paradoxe Situation. Liegt es daran, dass wir nach dem rheinischen Grundsatz „Et hät noch immä jut jejang“ leben oder sind wir von der komplexen Materie überfordert. Ich empfehle, dem kirchenleitend auf den Grund zu gehen.

6. Kommentar Nomosverlag

Jetzt kommt der Werbeblock: Beim Nomosverlag erscheint im November – endlich - ein Kommentar zum evangelischen Datenschutzrecht. Dieser Kommentar wird für die gleichmäßige Anwendung des Datenschutzrechtes in der ganzen EKD hilfreich sein. Er ist praxisnah aufgebaut und nicht nur an Juristen gerichtet. Ich kann nur empfehlen ihn rege auf allen Ebenen unserer Kirche zu nutzen. Er kann bereits im Onlineshop des Nomosverlages bestellt werden¹⁴.



7. Datenschutz als Chance

Datenschutz ist sehr, sehr simpel. Daten die zur Erfüllung meiner kirchlichen Aufgaben erforderlich sind, darf ich verarbeiten, andere nicht. Und ich muss die mir anvertrauten Daten beschützen. Ganz einfach!

Datenschutz ist mühselig. Wir erleben das so. Datenschutz ist mühselig, weil ich meine Prozesse genau anschauen und unter dem Gesichtspunkt der Erforderlichkeit ordnen muss. Das ist überhaupt nicht einfach. Die Fragen z.B., wer soll informiert sein und wer hat was zu entscheiden, sind eindeutig zu beantworten. Das bedeutet oft, dass althergebrachte Strukturen deutlich zu hinterfragen sind.

¹⁴ <https://www.nomos-shop.de/nomos/titel/ekd-datenschutzgesetz-id-99144/>

Datenschutz ist eine Chance, die oft nicht gesehen wird, eine Chance zu schlankere Strukturen zu kommen. Strukturen die sich schlicht an der Erforderlichkeit orientieren. Aus meiner Sicht steckt da in der Verwaltung nicht weniger kirchlicher Stellen ein erhebliches Einsparpotential.

Soweit mein turnusgemäßer Bericht nach § 41 DSGVO-EKD.

8. Abschlussbericht

Zum Abschluss ein persönliches Wort.

Wenn ich auf meine gut zehn Jahre als Datenschutzbeauftragter der Nordkirche zurück schaue muss Ihnen gestehen, dass ich manchmal etwas frustriert war; frustriert, weil es mir durch Beratung und Unterstützung so oft nicht gelungen ist, datenschutzkonforme Zustände herzustellen.

Wir als Kirche haben uns Regeln für den Datenschutz gesetzt, wir uns selber. Und so oft habe ich erlebt, dass sie nicht eingehalten wurden. Manches mal aus Unkenntnis, da konnte ich beraten, zumeist aber im Bewusstsein der Regelwidrigkeit, um nicht zu sagen Rechtswidrigkeit. Ich habe mich dann immer gefragt, was es mit uns als Kirche macht, wenn wir gegen unsere eigenen selbst gesetzten Regeln verstoßen.

Ein konkretes Beispiel will ich Ihnen erzählen: Bei einer Anmeldung bei WhatsApp muss man sein Alter mit 16 Jahre bestätigen. In wieviel Konfirmandengruppen wird WhatsApp als Gruppenchat eingesetzt. Die Kinder sind 13 oder 14 Jahre alt. Wenn sie sich bei WhatsApp angemeldet haben, haben sie also unwahr die Altersbestätigung abgegeben. Auch die pastörlische Person ist in dem Chat, billigt das also oder hat sogar dazu angeleitet. Ich frage mich wieder, was macht das mit uns, was mit den Kindern im Konfirmationsunterricht?

Vielleicht müssen wir uns wieder vergegenwärtigen, wozu es das Datenschutzrecht überhaupt gibt. Wir bewegen uns in asymmetrischen Machtstrukturen. Auf der einen Seite große Institutionen: Staat, Banken, Versicherungen, Krankenhäuser, auch Kirche, auf der anderen Seite der Einzelne. Wir sind im modernen Leben gezwungen, mit diesen übermächtigen Institutionen umzugehen. Das Recht, auch das Datenschutzrecht will diese Übermacht einhegen. Der Datenschutz steht doch dann auf der richtigen Seite!

Bisher haben wir uns im Datenschutz mit Hackerangriffen, Datenkraken wie Google oder Facebook, Telemetriedaten, amerikanischen Sicherheitsbehörden usw. rumgeschlagen. Die eigentliche Herausforderung rollt aber mit Vehemenz auf uns zu: sog. künstliche Intelligenz, maschinelles Lernen. Menschen unterhalten sich mit Robochats und fühlen sich endlich verstanden, Menschen bekommen in sog. sozialen Medien immer wieder die gleichen Inhalte bis sie sich in absurden Blasen bewegen, Menschen verlieren die Orientierung weil Facenews und Facefotos das Netz fluten, Menschen bekommen Kredit- oder Versicherungsentscheidungen innerhalb von Sekunden aufgrund von Algorithmen, die nicht auf menschlichen Entscheidungen beruhen, sondern allein auf maschinellem Lernen an personenbezogenen Daten, das kann sein: ethnische Zugehörigkeit, Geschlecht, Wohnort, Name, keiner weiß es mehr, keiner kann in die automatischen, sog. intelligenten Algorithmen hineinsehen. Ich spreche hier nicht von der fernen Zukunft, sondern das gibt es alles schon.

Selbst ein Elon Musk oder der Chef von ChatGPT, Sam Altman, warnen neben vielen anderen vor der KI als der größten Gefahr für die Menschheit.¹⁵

Meine Hoffnung, und die überwiegt die Frustration, meine Hoffnung ist es, dass wir uns gegen die Internetgiganten an die Seite der einzelnen Menschen stellen, dass wir uns um ihren Schutz bemühen und dass wir unseren freiheitlichen demokratischen Rechtsstaat verteidigen. Wir sind doch Kirche der Freiheit¹⁶ und wir wollen nahe bei den Menschen sein. In diesem Zusammenhang fängt das ganz kleinklein beim eigenen Umgang mit den anvertrauten Daten an. Wir gehen z.B. nicht so schludrig mit Fotos von Jugendlichen um, wie wir das gerade wieder einmal aus der Presse und dem Fernsehen erfahren mussten.

Auch Datenschutz kann ein Knoten im gestern in der Andacht von Pastor Ahrens angesprochenen Netzwerk der rettenden Liebe sein. Die Daten liegen uns am Herzen und wir begreifen Datenschutz nicht als lästiges Übel, sondern als Grundrechtsschutz für die uns anvertrauten Menschen. Ich will den Datenschutz nicht überhöhen. Aber wenn unsere Kirche eine feste Burg für Daten ist, wird auch das Vertrauen schaffen!

Vielen Dank für Ihre Aufmerksamkeit und auf Wiedersehen!

gehalten auf der Landessynode der Nordkirche am 30. September 2023 in Travemünde



Peter Loeper
Beauftragter für den Datenschutz
der Nordkirche

¹⁵ <https://www.zdf.de/nachrichten/panorama/ki-gefahr-menschheit-risiko-vernichtung-100.html>

¹⁶ <https://www.kirche-im-aufbruch.ekd.de/reformprozess/etappen/impulspapier.html>