An den Höheren Oberen der Ordensgemeinschaft der Alexianerbrüder

Bericht der Ordensdatenschutzbeauftragten

der

Congregatio Fratrum Cellitarum seu Alexianorum

für die Zeit vom 01.03.2021 – 28.02.2022

Die Datenschutzaufsicht erstellt gemäß § 44 Abs. 6 der Kirchlichen Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) jährlich einen Tätigkeitsbericht, der dem Höheren Oberen der Ordensgemeinschaft der Alexianerbrüder vorgelegt und der Öffentlichkeit zugänglich gemacht wird. Dieser Tätigkeitsbericht enthält eine Darstellung der wesentlichen Entwicklungen des Datenschutzes im kirchlichen sowie nicht-kirchlichen Bereich.

I. Überprüfung des Gesetzes über den kirchlichen Datenschutz

Sowohl die Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) sowie das Gesetz über den kirchlichen Datenschutz (KDG) sehen in § 58 Absatz 2 vor, dass binnen dreier Jahre nach Inkrafttreten eine Überprüfung der Regelung bzw. des Gesetzes vor. Diese Frist lief am 24. Mai 2021 ab. Die Deutsche Bischofskonferenz (DBK) ließ verlauten, dass mit der Evaluierung des KDG begonnen wurde. Unter anderem der Bund der Deutschen Katholischen Jugend (BDKJ), die Gesellschaft Katholischer Publizisten (GKP) sowie der Gemeinsame Ordensdatenschutzbeauftragte DOK Süd (GDSB SÜD), Jupp Joachimski, haben bereits Vorschläge unterbreitet. KDG und KDR-OG sind überwiegend wortgleich. Es ist naheliegend, dass etwaige Änderungen des KDG auch Einfluss in das KDR-OG finden werden.

Zu den vorgeschlagenen Änderungen zählt unter anderem eine Konkretisierung wann die 72-Stunden-Meldefrist bei Datenschutzverletzungen beginnt. Am 23. November 2020 hatte der Verband der Diözesen Deutschlands das Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG) beschlossen, auf dessen Grundlage die kirchliche Datenschutzaufsicht im Rahmen ihrer Zuständigkeiten nach Art. 91 Abs. 2 DSGVO handelt. Dieses Gesetz war für das Bistum Münster vom Bischof erlassen und im Amtsblatt 2021, Nr. 1, Art. 5, S. 22 ff. veröffentlicht worden. Im KDS-VwVfG sind u. a. die Anhörung von Beteiligten, Akteneinsicht durch Beteiligte, Fristen und Termine, Nichtigkeit des Verwaltungsaktes sowie die Heilung von Verfahrens- und Formfehlern geregelt. In Anbetracht der Diskussion wie die 72-Stunden-Meldefrist von Datenschutzverletzungen gemäß § 33 KDG zu bemessen ist, stellte § 7 Abs. 4 KDS-VwVfG klar, dass Sonntage, gesetzliche Feiertage oder Sonnabende bei einer nach Stunden bemessenen Frist mitgerechnet werden. Eine potentielle Überarbeitung des KDG würde hier anknüpfen und Klarstellen ab wann die Frist beginnt. In der Vergangenheit hatte es unterschiedliche Ansichten gegeben, ob die Frist bereits mit dem verletzenden Ereignis beginnt, mit dem Bekanntwerden bei der entdeckenden Person unabhängig von der Funktion oder mit dem Bekanntwerden beim Verantwortlichen bzw. dem Leiter der Einrichtung.

Die GKP schlug bspw. vor, dass im KDG in Anlehnung an Erwägungsgrund 51 der DSGVO hinzugefügt würde, dass die Verarbeitung von Lichtbildern, Audio- und Videoaufnahmen nur dann eine Verarbeitung besonderer Kategorien von personenbezogenen Daten darstelle, wenn sie mit speziellen technischen Mitteln verarbeitet würden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.

Des Weiteren wird eine Erweiterung des Begriffes „Beschäftigte" um ehrenamtlich tätige Personen befürwortet. Gemäß § 31 Absatz 5 KDG müssen kirchliche Stellen ein Verzeichnis von Verarbeitungstätigkeiten erstellen, wenn diese 250 oder mehr Beschäftigte haben. Im kirchlichen Bereich arbeitet jedoch eine vergleichsweise hohe Anzahl ehrenamtlich tätiger Personen, welche ebenfalls – auch mit hochsensiblen - personenbezogenen Daten in Kontakt kommen und diese für die Erfüllung ihrer ehrenamtlichen Aufgaben verarbeiten.

Zudem wird Anpassungsbedarf bei § 8 KDG hinsichtlich des Einwilligungserfordernisses gesehen. Derzeit bedarf die Einwilligung der Schriftform soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Diese Formulierung sorgt jedoch für Rechtsunsicherheit, da unklar ist wie eng die Formulierung „besondere Umstände" zu verstehen ist. Bezeichnet dieser Ausdruck generell bestimmte Arten von Ausnahmetatbeständen oder enge Ausnahmesituationen. Hier wird eine Anpassung an Artikel 7 Absatz 1 DSGVO favorisiert, gemäß dem eine Einwilligung des Betroffenen in die Verarbeitung ihrer personenbezogenen Daten lediglich nachweisbar sein muss.

Die GKP moniert auch, dass gemäß § 51 Absatz 6 KDG gegen kirchliche Stellen im Sinne des § 3 Absatz 1 KDG (u. a. Diözesen, Kirchenstiftungen, Kirchengemeindeverbände), keine Geldbußen verhängt werden können soweit diese kirchlichen Stellen im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind und nicht als Unternehmen am Wettbewerb teilnehmen.

Außerdem wurde vorgeschlagen ins KDG eine § 53 DSG-EKD vergleichbare Regelung aufzunehmen, welche die Übertragung und Aufnahme von Gottesdiensten oder kirchlichen Veranstaltungen ausdrücklich datenschutzrechtlich für zulässig erklärt soweit die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden. Hierbei sind aber auch Bereiche, die von der Aufzeichnung ausgenommen sind, als solche ausgewiesen werden.

II. Entscheidungen der kirchlichen Datenschutzgerichte

1. Offener E-Mailverteiler (Az.: IDSG 04/2019)

Das Interdiözesane Datenschutzgericht stellte am 29. November 2021 fest, dass durch die Verwendung eines offenen E-Mailverteilers dem Zusatz „To: Wunschgrosseltern Projekt" im Adressfeld gefolgt von allen E-Mailanschriften der Interessenten sowie mit der Anrede „Liebe Familien, liebe Wunschgroßeltern" im E-Mailtext nicht nur die E-Mailadressen unbefugt weitergegeben wurden, sondern die Datenschutzverletzung auch personenbezogene Daten aus dem Privat- und Familienleben der Antragstellerin betrifft.

2. *Prüfung der Vollständigkeit von Gottesdienstbesucherlisten (Az.: IDSG 27/2020)*

Das ISDG erklärte mit Beschluss vom 01.03.2021, dass leitende Pfarrer Einsicht in Gottesdienstbesucherlisten nehmen dürften, um die Vollständigkeit der Liste zu überprüfen und dadurch die Einhaltung des Coronaschutzkonzeptes gemäß § 6 Abs. 1 Buchstaben a und d KDG in Verbindung mit der Coronaschutzverordnung NRW zu gewährleisten.

3. *Zurechnung von Geldbußen (Az.: IDSG 14/2020)*

Am 19.04.2021 hatte das Interdiözesane Datenschutzgericht einen Bußgeldbescheid einer Datenschutzaufsicht zu überprüfen. Bei der Antragstellerin war eine Rechnung für eine Selbstzahlerin versehentlich an den falschen Adressaten versendet worden. Die zuständige Datenschutzaufsicht hatte gegen das Krankenhaus ein Bußgeld i. H. v. 2.000 € verhängt. Die Datenschutzaufsicht hatte bemängelt, dass im Verfahrensverzeichnis bei der Prozessbeschreibung keine Endkontrolle vor dem Versand vorgesehen sei und eine Nachschau auch nicht stattgefunden habe. Daher läge ein Organisationsverschulden vor. Die Antragstellerin machte geltend, dass im kirchlichen Datenschutzrecht eine Zurechnungsnorm fehle, wonach dem Verantwortlichen das Verhalten seiner Mitarbeiter zugerechnet werde. Zurechnungsregelungen entsprechend Art. 83 DSGVO und § 30 Abs. 1 OWiG enthalte § 51 KDG nicht.

Das IDSG beschloss, dass die Verstöße der Antragstellerin als der Verantwortlichen im Sinn der §§ 51 Abs. 1, 4 Ziffer 9. KDG zuzurechnen seien. „Juristische Personen haften in Bezug auf Geldbußen als Verantwortliche gemäß dem Funktionsträgerprinzip für schuldhafte Datenschutzverstöße aller ihrer Mitarbeiter unabhängig davon, ob die Mitarbeiter eine Organstellung oder eine andere Führungsposition (§ 30 Abs. 1 OWiG) innehaben." Das IDSG erkennt, dass es umstritten ist, ob im Datenschutzrecht nach der DSGVO das Funktionsträgerprinzip gilt, schließt sich aber der Rechtsprechung des Landgerichts Bonn (LG Bonn, Urteil vom 11. November 2020) an. Die Anwendung des Funktionsträgerprinzips sei u. a. durch den Grundsatz der Effektivität und Einheitlichkeit des Datenschutzes geboten. Das Landgericht Berlin hingegen hatte sich in seinem Beschluss vom 18.02.2021 (Az.: 526 OWi LG, 212 Js-OWi 1/2 gegen das Funktionsträgerprinzip ausgesprochen und die Auffassung vertreten, dass nur natürliche Personen eine Ordnungswidrigkeit vorwerfbar begehen könnten. Das Berliner Gericht erachtete es als erforderlich, dass einem konkret benannten Organ einer juristischen Person die Begehung einer Ordnungswidrigkeit nachgewiesen wird bevor diese dem Verantwortlichen zugerechnet wird und stellte in seinem Beschluss ausführlich dar, warum es dem Rechtsträgerprinzip folgt. Das Landgericht Berlin führt schlagkräftige Argumente aus, aber die Anwendung des Rechtsträgerprinzips führt zu einem deutlichen höheren Aufwand bei den Datenschutzaufsichtsbehörden. Zudem besteht das Risiko gerade in Unternehmen mit komplexeren Strukturen, dass keinem spezifischen Repräsentanten ein Verschulden konkret nachgewiesen werden kann, obschon feststeht, dass ein Datenschutzverstoß vorliegt. Die Streitfrage geht in die nächste Runde. Das Urteil des Landgerichts Bonn ist zwar rechtskräftig geworden, aber gegen den Beschluss des Landgerichts Berlin wurde von der Staatsanwaltschaft Berlin Beschwerde eingelegt. Die Sache gelangte somit zum Kammergericht Berlin, welches dem Gerichtshof der Europäischen Union die Frage zur Klärung vorlegte, ob in Bußgeldverfahren nach Artikel 83

Absatz 4 bis 6 DSGVO das Funktionsträgerprinzip oder das Rechtsträgerprinzips Anwendung findet. Es bleibt spannend im Datenschutz.

III. Aktuelle Themen in 2021

1. Nudging im Rahmen von Cookie Bannern auf Websites

Cookies sind Bestandteil einer Vielzahl von Internetseiten und im Alltag von Website-Besuchern längst angekommen. Sie können unterschiedlichsten Zwecken dienen: Sicherung von Login-Daten, um beim erneuten Besuch einer Seite die Zugangsdaten nicht erneut eingeben zu müssen, aber auch um das Surfverhalten von Nutzern zu analysieren, um ihnen individuell auf sie zugeschnittene Angebote zu unterbreiten.

Der Europäische Gerichtshof hat im Jahr 2019 klargestellt, dass der Einsatz von Cookies, die nicht für den technischen Betrieb der Seite erforderlich sind, nur mit ausdrücklicher Einwilligung des Nutzers erfolgen darf. Ebenso macht die Europäische Datenschutzgrundverordnung strenge Vorgaben zur Einholung des Einverständnisses des Nutzers. Der Frage beim erstmaligen Besuch einer Webseite, ob man mit dem Einsatz von Cookies einverstanden ist, begegnet man tagtäglich.

Die Gestaltung dieser Abfrage, des so genannten Cookie-Banners, wirft allerdings viele Fragen auf und ist immer Anlass für rechtliche Diskussionen. Grundsätzlich gilt: Der User muss die freie Wahl haben, ob er mit dem Einsatz von Cookies einverstanden ist. Auf der anderen Seite haben Betreiber von Webseiten oftmals ein hohes Interesse am Einsatz von Cookies, um die Webseite besonders komfortabel zu gestalten und zu analysieren, welche Themen besonders ansprechend für die Websitebesucher waren.

Inzwischen ist in diesem Zusammenhang des Öfteren von „Nudging" die Rede. „Nudging" heißt frei übersetzt „jemanden in eine bestimmte Richtung zu bewegen" oder ihn anzustupsen. Auch Cookie-Banner können so gestaltet werden, dass Besucher von Webseiten mehr oder weniger offensichtlich dazu verleitet werden, dem Einsatz von Cookies zuzustimmen. Beispielsweise geschieht dies, in dem die Zustimmung zum Gebrauch von Cookies farblich attraktiver gestaltet wird, der Button größer ist oder die Ablehnung erst durch eine umständliche Auswahl von Einzelthemen bestätigt werden muss. Nudging sollte durch eine neutrale Gestaltung vermieden werden.

2. Telekommunikation-Teledienste-Datenschutz-Gesetz (TTDSG)

Am 20.05.2021 beschloss die deutsche Bundesregierung das „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien", kurz das TTDSG. Das Gesetz trat im Großen und Ganzen am 01.12.2021 in Kraft, während einzelne Bestimmungen bereits am Tag nach der Beschlussfassung in Kraft traten, welche jedoch keine nennenswerten Auswirkungen hatten.

Hintergrund zu diesem Gesetzesbeschluss war zum einen die Umsetzung der ePrivacy-Richtlinie der Europäischen Union, nachdem eine mangelnde Umsetzung festgestellt wurde. Hierzu

ergingen Urteile des EuGHs[1] und des BGH[2] in relevanten Fällen. Des Weiteren war es Ziel der Bundesregierung, die datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) in einem Regelwerk zu vereinen und übersichtlicher zu gestalten und gleichzeitig eine Anpassung der Regelungen durchzuführen.

Das Gesetz wird als Zwischenschritt zwischen der Umsetzung der ePrivacy-Richtlinie und der ePrivacy-Verordnung der Europäischen Union gesehen, weshalb gesetzliche Klarstellungen erfolgten und vereinzelt Neuerungen eingeführt wurden, jedoch umfassende Änderungen ausblieben. Nichts desto trotz enthält das Gesetz Regelungen, die nicht außer Acht gelassen werden sollten. Kirchliche Einrichtungen fallen ebenfalls in den Anwendungsbereich des TTDSG, sofern sie Anbieter von Telemedien und Telekommunikation sind. Im Folgenden werden ein paar wesentlichen Änderungen dargestellt.

a) Neuerungen bezüglich der Bestimmungen des TKG

Die datenschutzrechtlichen Regelungen aus dem Telekommunikationsgesetz (§§ 88 ff TKG) wurden in den Teil II des TTDSG, der die §§ 3 bis 18 beinhaltet, überführt. Im Wesentlichen wurden keine neuen materiellen Regelungen eingeführt.

Der Anwendungsbereich der Bestimmungen des TKG wurde durch das Telekommunikationsmodernisierungsgesetz ausgedehnt und umfasst nun auch sogenannte „Over-the-Top-Dienste" wie beispielsweise WhatsApp, diverse E-Mail- und weitere Nachrichtenübertragungsdienste, welche die Kommunikation über das Internet bereitstellen. Anbieter solcher Dienste unterstehen nun auch den strengeren Regelungen des TTDSG in den betroffenen Bereichen.

Das Fernmeldegeheimnis – vormals geregelt in § 88 TKG – findet ebenfalls Eingang in das TTDSG und zwar in § 3 TTDSG.

Eine echte Neuerung – die aber nur für Diensteanbieter von Telekommunikationsdiensten Relevanz besitzt – ist die Einführung eines „digitalen Erben" im § 4 TTDSG. Anfragen von Erben oder anderen befugten Personen eines Erblassers steht das Fernmeldegeheimnis nicht entgegen, weshalb davon betroffene Daten an solche Personen herauszugeben sind – soweit der Nutzer mit dem Diensteanbieter keine entgegenstehende vertragliche Abmachung getroffen hat.

b) Neuerungen bezüglich der Bestimmungen des TMG

Die Bestimmungen des Telemediengesetzes (TMG) wurden ebenso in das TTDSG überführt und sind in den §§ 19 bis 26 abgebildet. Die Regelungen zu den technischen und organisatorischen Maßnahmen für Telemedien wurden bei der Neugestaltung übersichtlicher geregelt, während der Inhalt gleichblieb. Dies betrifft auch die Regelungen zu Bestands- und Nutzungsdaten sowie den zugehörigen Auskunftsverfahren, die sich nun in den §§ 21 bis 24 TTDSG wiederfinden.

Im Bereich der Bestimmungen des TMG befinden sich zudem „echte Neuerungen", wie sie in der Einleitung zur Umsetzung der ePrivacy-Richtlinie beschrieben wurden. Betroffen von den

[1] Siehe EuGH, Urteil vom 01.10.2019 – AZ: C-673/17 (Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e. V. gegen Planet49 GmbH).

[2] Siehe BGH, Urteil vom 28.05.2020 – AZ: I ZR 7/16.

Regelungen sind vordergründig Cookies und ähnliche Tracking-Methoden, die entweder auf Daten auf Endgeräten von Nutzern zugreifen oder Daten auf die Endgeräte von Nutzern speichern. Nachfolgend werden die echten Neuerungen dargestellt.

c) Schutz der Privatsphäre von Endeinrichtungen (§ 25 TTDSG)

Durch die Neuformulierung des vormaligen § 15 Abs. 3 TMG wurde eine Anpassung der Regelung an die ePrivacy-Richtlinie vorgenommen. Wichtig ist in diesem Zusammenhang die technologieneutrale Formulierung, welche letztlich nicht nur Cookies betrifft, sondern generell alle „Endeinrichtungen" von Nutzern vor Zugriffen auf vorhandene Daten oder vom Abspeichern von Daten darauf schützen soll. Die Bestimmung hat somit auch Auswirkungen auf Funktionen oder Geräte im Bereich des IoT (Internet of Things) oder anderen Smart-Home-Anwendungen.

Der Wortlaut der Bestimmung orientiert sich dabei eng an den Formulierungen der ePrivacy-Richtlinie und enthält ein explizites Einwilligungserfordernis.

Die Besonderheit zu anderen datenschutzrechtlichen Regelungen ist, dass diese Bestimmung sowohl personenbezogene als auch nicht-personenbezogene Daten schützt!

Die geforderte Einwilligung hat nach dem TTDSG den Vorgaben der DSGVO zu entsprechen, weshalb eine Einwilligung nur rechtswirksam ist, wenn diese freiwillig, informiert und aktiv abgegeben wird.

Nur zwei Ausnahmen vom Einwilligungserfordernis sind enthalten, wonach keine Einwilligung notwendig sein soll. Ausnahmen liegen vor, wenn

» der alleinige Zweck der Speicherung/des Zugriffs von/auf Informationen auf Endeinrichtungen der Nutzer die Durchführung einer Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist;

» die Speicherung/der Zugriff von/auf Informationen auf der Endeinrichtung unbedingt erforderlich für die Zurverfügungstellung eines vom Nutzer ausdrücklich gewünschten Telemediendienst ist.

Bitte beachten Sie, dass eine zweistufige Prüfung zu erfolgen hat, wenn bei einer Datenerhebung auch personenbezogene Daten betroffen sind. Richtet sich die Einwilligung nach dem TTDSG vorerst nur darauf, ob ein Zugriff auf das Endgerät eines Nutzers rechtmäßig ist, so benötigen nachfolgende Datenverarbeitungen stets auch einer Rechtsgrundlage nach der KDR-OG.

Die Erlaubnistatbestände des TTDSG können nachfolgende Verarbeitungen mitabdecken. Dies trifft insbesondere auf Einwilligungen zu.

d) Anerkannte Dienste zur Einwilligungsverwaltung (§ 26 TTDSG)

Das Gesetz ermöglicht den Einsatz von sogenannten „PIMS" (Personal Information Management Systems) zur zentralen Verwaltung von Nutzereinwilligungen bei unabhängigen Dienstleistern. Hierdurch sollen Cookie-Banner überflüssig werden, indem bei einem

Webseitenbesuch der Seitenbetreiber die Einstellungen des Nutzers bei einem „PIMS" abruft und die Seite entsprechend den Einstellungen gestaltet.

e) Strafvorschriften des TTDSG

Bei bestimmten Delikten gegen Bestimmungen aus dem TKG verbleibt die Möglichkeit, auch Freiheitsstrafen bis zu zwei Jahren zu verhängen oder alternativ Geldstrafen auszusprechen. Dies betrifft das Abhörverbot und den Missbrauch von Telekommunikationsanlagen.

Zudem nennt das TTDSG Tatbestände wie das nicht fristgerechte Löschen von Verkehrsdaten, das Unterdrücken von Rufnummern in bestimmten Situationen u.v.m. Die Ordnungswidrigkeiten können mit Bußgeldern belegt werden. Bei den Bußgeldern wurden folgende Abstufungen festgelegt: 300.000 Euro, 100.000 Euro, 50.000 Euro und 10.000 Euro, abhängig vom begangenen Verstoß.

Verstöße aus datenschutzrechtlicher Sicht, insbesondere gegen § 25 TTDSG, können nach dem TTDSG mit bis zu EUR 300.000 und zusätzlich nach den Bußgeldbestimmungen der KDR-OG geahndet werden.

3. Home Office: Risiken durch Smart-Home-Geräte

Fragestellungen rund um den Datenschutz bei Sprachassistenten wie Alexa, Siri & Co. sind keineswegs abschließend beantwortet. Es besteht ein starkes Spannungsfeld zwischen künstlicher Intelligenz und dem Datenschutz. Aber auch die Sicherheit der Daten von Unternehmen ist nicht gewährleistet. Deshalb ist eine besondere Sensibilität bei den Herausforderungen des Home-Office notwendig. So verfügt beispielsweise der Sprachassistent von Amazon „Alexa" über sieben Mikrofone, die im 360 Grad-Radius angeordnet und allzeit bereit sind. Damit Alexa sofort auf die Wünsche seines Besitzers reagieren kann, muss das Gerät dauerhaft mithören. Bei direkter Ansprache „Alexa, tue dies oder tue das" findet eine Datenübertragung an den Anbieterserver statt. Aber Pannen aus den letzten Monaten zeigen auch immer wieder, dass Gespräche oder Nebengeräusche (Bankdaten, Telefonnummern) übertragen werden, die nicht übertragen werden sollten. Dies lässt nur den Schluss zu, dass alles, was gesagt wird, in irgendeiner Form verarbeitet wird oder zumindest werden kann. Der Nutzer bleibt verunsichert mit Fragen zur Weiterverarbeitung und Speicherung der Daten zurück.

Tatsächlich befindet sich der Betroffene in einem Dschungel von Datenübermittlungen, die selbst die Datenschutz-Behörden vor erhebliche Herausforderungen stellen. Auch für Unternehmen bestehen Gefahren, wenn die Beschäftigten beispielsweise im Home-Office tätig sind. Bei vertraulichen Telefon- oder Videokonferenzen werden viele sensibilisierte Beschäftigte sicherlich Maßnahmen ergreifen, um fremde Ohren außen vor zu lassen (beispielsweise durch Schließen der Türe). Doch wird hierbei dann sicherlich häufig vergessen, dass „digitale" Ohren im gleichen Raum sind.

Unterzieht man diesen Befund einer Prüfung, lassen sich nachfolgende Punkte feststellen:

» Sprachassistenten hören immer mit.

» Alexa, Siri und Co. werden oftmals unbeabsichtigt aktiviert und senden die Daten an den Anbieterserver.

» Es wurde nachgewiesen, dass auch Daten bei nicht aktivierten oder ausgeschalteten Geräten gesendet werden.

» Welche Daten zu welchem Zweck erfasst werden, ist nicht wirklich nachvollziehbar.

» Die Daten werden ganz überwiegend außerhalb der EU verarbeitet.

Für ein Unternehmen mit Sitz in der EU gilt die DSGVO immer. Es muss sicherstellen, dass diese eingehalten wird. Die Nutzung von Sprachassistenten – auch wenn die Daten im Nicht-EU-Ausland verarbeitet werden – unterliegt daher ebenfalls diesen gesetzlichen Vorgaben.

Da nicht klar ist, welche Daten vom Sprachassistenten übermittelt und in welcher Form (maschinell oder menschlich) weiterverarbeitet werden, sollte beim Thema Home-Office ein vorhandener Sprachassistent kritisch auf den Prüfstand gestellt werden. Sensible Unternehmensdaten, personenbezogene oder besonders schützenswerte Daten über Kunden oder Mitarbeiter sind nur einige Stichworte, die die Relevanz des Umgangs mit den vermeintlich hilfreichen Alltagshelferlein verdeutlichen.

Im Home-Office sollten Sprachassistenten grundsätzlich ausgeschaltet sein oder bestenfalls entfernt werden. Die Gefahr, die von ihnen für den Datenschutz und die Sicherheit der Unternehmensinformationen ausgeht, ist nicht seriös abzuschätzen. Für Unternehmen bieten sich Maßnahmen zur Sensibilisierung der Belegschaft an. Von den politischen und administrativen Akteuren darf im Umgang mit den Anbietern der Sprachassistenten mehr Klarheit und Durchsetzungsfähigkeit erwartet werden.

4. Erpressung aufgrund mangelnder Informationssicherheit

Immer öfter werden Fälle bekannt, in denen durch einen Angriff große Teile der Produktion lahmgelegt werden. Hierbei wurden Daten und Systeme verschlüsselt. Um die Systeme wieder lauffähig zu machen, werden Lösegeldzahlungen in Millionenhöhe gefordert, aber nicht immer erhält man hinterher den Schlüssel zur Entschlüsselung. Oftmals kann man die Daten auch nach der Zahlung nicht wieder entschlüsseln. So hat man nicht nur Geld gezahlt, sondern muss einen noch höheren Preis für die Nicht-Verfügbarkeit des IT-Systems zahlen. Mehr und mehr sind auch Einrichtungen des Gesundheitswesens in das Visier von Cyberkriminellen gelangt.

Tatsächlich können Einrichtungen des Gesundheitssektors und kirchliche Stellen schon heute viel für die Datensicherheit tun und somit Prävention gegen Cyberkriminalität leisten. Der Aufbau eines Informationssicherheits-Managements ist ein wichtiger Baustein zu einer deutlich verbesserten IT-Sicherheit. Dieses Vorgehensmodell kann sich an den gängigen Normen zum Informationssicherheits-Managementsystem (ISO/IEC 27001 und 27002) orientieren und ist seit Jahren aufgrund seiner Praktikabilität anerkannt. Im Ergebnis entsteht ein Managementsystem, durch das sichergestellt werden kann, dass die Informationssicherheit in den Einrichtungen gelebt wird, auf die Bedürfnisse der Einrichtungen angepasst ist und alle wichtigen Aspekte erfasst werden.

Ein in letzter Zeit immer wichtiger werdender Bereich ist die Schulung und Sensibilisierung der eigenen Belegschaft für das Thema IT-Sicherheit und der richtige Umgang mit ihr. Die Erfahrung zeigt, dass Vorgaben nur eingehalten werden, wenn die Mitarbeiter die Hintergründe

verstehen. Andernfalls werden entweder bewusst Regeln umgangen, weil sie als „lästig/unsinnig“ empfunden werden, oder es wird unbewusst aus mangelndem Wissen gegen Vorgaben verstoßen.

IV. Tätigkeiten

Im Berichtszeitraum wurden keine Datenschutzverletzungen gemeldet. Zudem machten Betroffene weder von Ihren Betroffenenrechten Gebrauch noch gingen Beschwerden ein.

Schulungen zum Datenschutz wurden angeboten.

Tätigkeit	
Datenpanne	keine
Auskunftsersuchen	keine
Beschwerden	keine
Schulungen	wurden angeboten

Dr. Tamara Bukatz

Ordensdatenschutzbeauftragte