An den Höheren Oberen der Ordensgemeinschaft der Alexianerbrüder

Bericht des Ordensdatenschutzbeauftragten
der
Congregatio Fratrum Cellitarum seu Alexianorum

für die Zeit vom 01.01.2020 – 01.03.2021

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 nichtkirchlichen Bereich. Hierbei wird auch auf spezifische datenschutzrechtliche Themen eingegangen, die im Zuge der Corona-Pandemie Relevanz erlangten.

I. Seelsorge-Patientendatenschutzgesetz

Am 23. November 2020 beschloss der Verband der Diözesen Deutschland das Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens. Dieses Gesetz wurde für das Bistum Münster vom Bischof erlassen und im Amtsblatt 2021, Nr. 3, Art. 51, S. 141 ff. veröffentlicht. Das Seelsorge-PatDSG gilt für alle Krankenhäuser i. S. d. §§ 107 Abs. 1, 108 Sozialgesetzbuch Fünftes Buch (SGB V) und Vorsorge- und Rehabilitationseinrichtungen i. S. d. §§ 107 Abs. 2, 111 SGB V.

Das Gesetz unterscheidet zwischen der Rechtmäßigkeit der Datenweitergabe an einen Krankenhausseelsorger bei Vorhandensein eines Konzepts zur Krankenhausseelsorge (§ 3 Seelsorge-PatDSG), der Offenlegung von Patientendaten gegenüber einer mit Seelsorgeauftrag ausgestatteten Person bei Fehlen eines Seelsorgekonzeptes (§ 4 Seelsorge-PatDSG) sowie der Offenlegung von Patientendaten gegenüber der Kirchengemeinde (§ 5 Seelsorge-PatDSG).

Verfügt eine katholische Einrichtung des Gesundheitswesens über ein verabschiedetes und ausgehängtes Seelsorgekonzept, so darf die Einrichtung dem Krankenhausseelsorger Patientendaten mitteilen. Der Patient muss im Rahmen des Behandlungsvertrages jedoch zuvor auf die konzeptionelle und tatsächliche Einbindung eines Krankenhausseelsorger hingewiesen werden.

Ist in einer Einrichtung kein Seelsorgekonzept eingeführt worden, dürfen katholische Einrichtungen des Gesundheitswesens Vor- und Nachname des Patienten, dessen Religionszugehörigkeit, Aufenthaltsort in der Einrichtung und das Datum der Aufnahme in die katholische Einrichtung des Gesundheitswesens an eine Person mit Seelsorgeauftrag der betroffenen Einrichtung zum Zweck der Seelsorge ebenfalls unter bestimmten Umständen offenlegen. Wird der Patient bei Abschluss des Behandlungsvertrages nach seiner Religionszugehörigkeit befragt, muss dieser darauf hingewiesen werden, dass es sich um eine freiwillige Angabe handelt und

dass die Angabe zum Zwecke der Seelsorge verwendet wird, d. h. der Patient muss informiert werden, dass Daten und welche Daten an eine Person mit Seelsorgeauftrag weitergegeben werden. Gemäß § 4 Seelsorge-PatDSG ist keine ausdrückliche Einwilligung des Patienten erforderlich. Hat man die Informationspflicht beachtet, so ist eine Weitergabe der hier aufgeführten personenbezogenen Daten zulässig; es sei denn der Patient hat zum Ausdruck gebracht, dass er keine Seelsorge wünscht.

Die Auflistung der zuvor genannten Patientendaten ist jedoch nicht der Kirchengemeinde gegenüber offenzulegen; es sei denn der Patient hat ausdrücklich in die Datenweitergabe eingewilligt. Der Umstand allein, dass die Religionszugehörigkeit im Behandlungsvertrag angegeben wurde, ist nicht als Einwilligung zu werten.

II. Verwaltungsverfahrensgesetz

Der Verband der Diözesen Deutschlands beschloss am 23. November 2020 ebenfalls das Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG), auf dessen Grundlage die kirchliche Datenschutzaufsicht im Rahmen ihrer Zuständigkeiten nach Art. 91 Abs. 2 DSGVO handelt. Dieses Gesetz wurde für das Bistum Münster vom Bischof erlassen und im Amtsblatt 2021, Nr. 1, Art. 5, S. 22 ff. veröffentlicht. Das KDS-VwVfG regelt die nach außen gerichtete Tätigkeit der Datenschutzaufsicht in Bezug auf ihre Aufgaben, welche sich aus Kapitel 6 (Datenschutzaufsicht) und Kapitel 7 (Beschwerde, gerichtlicher Rechtsbehelf, Haftung und Sanktionen) des KDG ergeben. Das KDS-VwVfG regelt u.a. die Anhörung von Beteiligten, Akteneinsicht durch Beteiligte, Fristen und Termine, Nichtigkeit des Verwaltungsaktes sowie die Heilung von Verfahrens- und Formfehlern.

Beispielsweise darf die kirchliche Datenschutzaufsicht gemäß § 4 Abs 3 KDS-VwVfG „die Entgegennahme von Erklärungen oder Anträgen, die in ihren Zuständigkeitsbereich fallen, nicht deshalb verweigern, weil sie die Erklärung oder den Antrag in der Sache für unzulässig oder unbegründet hält“.

Denkt man an die Diskussion zurück, wie die 72-Stunden-Meldefrist von Datenschutzverletzungen gemäß § 33 KDG zu bemessen ist, so stellt § 7 Abs. 4 KDS-VwVfG nun klar, dass Sonntage, gesetzliche Feiertage oder Sonnabende in eine nach Stunden bemessene Frist mitgerechnet werden.

III. Anmeldelisten in der Kirche

Im Zuge der Corona-Pandemie wurden in Kirchen Anmeldungen zu kirchlichen Veranstaltungen zur Religionsausübung wie Beerdigungen und Gottesdiensten eingeholt und hierbei die Kontaktdaten der Teilnehmer erfasst. Dies ist in Nordrhein-Westfalen auf Basis der Verordnung zum Schutz vor Neuinfizierungen mit dem Coronavirus SARS-CoV-2 (CoronaSchVO) gemäß § 6 Abs. 1 lit. a KDG i. V. m. § 1 Abs. 3 CoronaSchVO zulässig. Die Aufbewahrungsdauer für diese personenbezogenen Daten beträgt vier Wochen. Nach Ablauf dieser Frist sind die erfassten Daten zu löschen bzw. die Listen zu vernichten.

IV. Wärmebildkameras / Temperatur-Messungen

Im Mai 2020 verlautete es in den Nachrichten, man ziehe in Italien Temperaturmessungen mittels Thermoscanner bei Teilnehmern an Beerdigungsmessen vor dem Eintritt in die Kirche in Betracht. In Deutschland sah man es im Rahmen der Verhinderung von Corona-Erkrankungen, so dass verschiedene Unternehmen dazu übergingen, Wärmebildkameras am Eingang von Werkstoren anzubringen, um eine eventuell erhöhte Körpertemperatur bei Bediensteten oder Besuchern festzustellen. Mit der Wärmebildkamera am Eingangsgebäude oder am Werkstor erfolgte eine automatisierte Temperaturmessung bei allen Personen, die das Gelände oder Gebäude betreten. Selbst wenn bei der automatisierten Messung noch keine weiteren Daten wie der Name oder sonstige Kontaktdaten der betroffenen Person erhoben werden und auch keine Daten gespeichert werden, ist der Einsatz von Wärmebildkameras oder anders gestalteten Temperaturmessungen nicht unproblematisch. Ein Rückschluss auf eine konkrete natürliche Person ergibt sich schon dadurch, dass die betroffene Person vom Security-Dienst angesprochen und am Betreten des Gebäudes gehindert wird, sofern es das Messergebnis hergibt. Gerade zu Stoßzeiten erfährt so eine größere Anzahl weiterer Personen, wem der Zutritt gewährt und wem der Zutritt verwehrt wurde.

Die persönliche Körpertemperatur ist ein Gesundheitsdatum und somit ein Datum aus der Kategorie besonderer personenbezogener Daten. Für die Verarbeitung besonderer personenbezogener Daten durch katholische Einrichtungen bedarf es einer Rechtsgrundlage gemäß § 11 KDG. Im Gegensatz zu § 6 Abs. 1 lit. g KDG stellt die Wahrung berechtigter Interessen keine Legitimation für die Verarbeitung besonderer personenbezogener Daten dar.

1. In Betracht ziehen kann man, ob sich eine Rechtsgrundlage aus dem Arbeitsschutz ergibt. Die Corona-Arbeitsschutzverordnung hat die Minimierung einer Infektion mit dem Coronavirus bei der Arbeit sowie den Schutz der Sicherheit und Gesundheit der Beschäftigten zum Ziel. Als Schutzmaßnahmen sind darin u. a. aufgeführt: Einhalten des Mindestabstands, Lüftungsmaßnahmen, geeignete Abtrennungen zwischen den anwesenden Personen, Tragepflicht von Mund-Nase-Schutz oder Atemschutzmasken für alle anwesenden Personen und sonstige im Hygienekonzept ausgewiesenen Maßnahmen. Temperaturmessungen sind darin nicht explizit aufgeführt. Allerdings hat der Arbeitgeber gemäß § 2 Corona-ArbSchV i. V. m. §§ 5 und 6 ArbSchG eine Gefährdungsbeurteilung u. a. aufgrund der Gegebenheiten des Arbeitsplatzes, der Art der Tätigkeit und der Zahl der Beschäftigten vorzunehmen und zu ermitteln, welche zusätzlichen Maßnahmen gegebenenfalls zum Infektionsschutz bei der Arbeit erforderlich sind. Da eine erhöhte Körpertemperatur aber auch andere Ursachen haben kann und nicht bei jeder infizierten Person eine erhöhte Körpertemperatur feststellbar ist, ist die Erhebung der Körpertemperatur bereits kein geeignetes, und im Vergleich zu obigen genannten Maßnahmen, auch nicht sichereres Mittel zur Eindämmung der Pandemie.
2. Dies sollte man auch bedenken, falls man sich im Rahmen des Arbeitsschutzes zwecks Einführung von Temperaturmessungen am Eingang zum Gelände bzw. Gebäude zu einer Dienstvereinbarung nach der Mitarbeitervertretungsordnung entschließt.

3. Sofern sich eine Einrichtung auf die Einwilligung der Betroffenen stützen möchte, muss die Freiwilligkeit der Einwilligung in die Durchführung der Temperaturmessung und damit einhergehende Datenerhebung gewährleistet werden. Andernfalls ist eine Einwilligung unwirksam. Wie bekannt ist es im Arbeitgeber-Mitarbeiterverhältnis komplexer, die Freiwilligkeit einer Einwilligungserklärung von Mitarbeitern zu gewährleisten. Eine mögliche Lösung wäre beispielsweise, den Zutritt in das Gebäude über zwei Eingänge zu ermöglichen. An einem der beiden Zutrittswege findet eine Temperaturmessung statt während dies an dem anderen Zutrittsweg nicht erfolgt. Dies würde zumindest die Freiwilligkeit der Einwilligung stützen. Ob die Einführung des Systems dann jedoch von allen Arbeitnehmern genutzt wird, ist ebenso fraglich wie dessen Geeignetheit. In Anbetracht dessen, dass es im Regelfall sicherere, mildere Mittel gibt, welche in der Corona-Arbeitsschutzverordnung genannt sind, sind diese stattdessen heranzuziehen.

V. Videokonferenzsysteme

Durch die Coronavirus-Pandemie und die damit verbundenen Abstandsregeln greifen viele auf Videokonferenzsysteme zurück. Hierzu wurde oftmals aufgrund der Kurzfristigkeit des Bedarfs sehr schnell agiert und nicht zwingend alle Gepflogenheiten eines ordnungsgemäßen Auswahlverfahrens im Hinblick auf Datenschutz und Informationssicherheit eingehalten.

Es gibt einige Regeln zu beachten, um Videokonferenzen datenschutzkonform durchzuführen. Wir geben einen kurzen Überblick, worauf Sie und Ihr Unternehmen achten sollten:

» *Auswahl des richtigen Anbieters:* Bei Cloud-basierten Anwendungen sollte nach Möglichkeit darauf geachtet werden, dass der Cloud-Server und die vorgenommene Datenverarbeitung in der EU bzw. im EWR stattfindet. Gehen Sie den sichersten Weg: Wenn ein Dienst aus den USA und ein gleichwertiger Dienst aus der EU zur Auswahl stehen, wählen Sie lieber den Dienst aus der EU. Daneben sollte bei der Anbieterauswahl auf die Datenschutzfreundlichkeit bei den Einstellungen (u. a. Verschlüsselung, Profiling, Protokolle und Aufzeichnungen) geachtet werden.

» *Abschluss eines Auftragsverarbeitungsvertrags:* Mit Auftragsverarbeitern müssen Sie Auftragsverarbeitungsverträge entsprechend den gesetzlichen Anforderungen abschließen. Die meisten Anbieter bieten derartige Vereinbarungen an. Dieser sollte dann durch den Datenschutzbeauftragten geprüft werden.

» *Informationspflichten:* Weil solche Videokonferenzen/Webinare eine Datenverarbeitung darstellen, müssen die Informationen vor Beginn der Veranstaltung zur Einsicht bereitgehalten werden. Die Bestätigung dieser Informationen im Rahmen des Anmeldeverfahrens bietet sich an.

» *Interne Regeln:* Zu empfehlen ist für die Mitarbeiter die Erstellung eines Merkblatts/Leitfadens, wie sie sich bei Videokonferenzen zu verhalten haben und was zu beachten ist. Es sollte darauf geachtet werden, dass über das Webinar bzw. über die Videokonferenz keine zusätzlichen personenbezogenen Daten ausgetauscht werden, wenn diese aufgezeichnet

wird. Müssen trotzdem personenbezogene Daten ausgetauscht werden, so sollte dies separat durchgeführt werden (z. B. per Mail).

» *Aufzeichnungen nur mit Einwilligung:* Sollen die Webinare aufgezeichnet werden, um sie später auch anderen Interessenten bereitzustellen, so ist dies einwilligungspflichtig. Auf Mitschnitte von externen Teilnehmern sollte man daher verzichten. Eine Einwilligung seitens des Referenten als Mitarbeiter des Webinar-Anbieters sollte schriftlich eingeholt werden, wobei die typischen Problemstellungen der Einwilligung im Arbeitsverhältnis bleiben.

Oben genannte Risiken insbesondere im Hinblick auf den Drittlandtransfer können durch den Einsatz einer selbst-gehosteten Instanz ausgeschlossen werden.

VI. EuGH-Urteil zum Privacy Shield

Gemäß den gesetzlichen Vorgaben müssen Verantwortliche und Auftragsverarbeiter auch bei Datentransfers in Drittländer ein angemessenes Datenschutzniveau gewährleisten. Drittländer sind alle Länder außerhalb der EU/EWR. Hierbei ist zwischen sicheren und unsicheren Drittländern zu unterscheiden. Sichere Drittländer sind solche, denen die Europäische Kommission per Angemessenheitsbeschluss[1] ein angemessenes Datenschutzniveau bestätigt hat. Dort gewährleisten die nationalen Gesetze einen Schutz von personenbezogenen Daten, welcher mit dem des EU-Rechts vergleichbar ist. In diese Länder ist die Datenübermittlung daher ausdrücklich gestattet. Bislang zählten hierzu auch die USA, wenn der Empfänger dem Privacy Shield angehört. Dies änderte sich mit dem EuGH-Urteil Schrems II vom 16. Juli 2020.

Die Kernpunkte des Urteils sind:

1. Das Privacy Shield, auf welches Datentransfers zwischen Unternehmen aus EU-Mitgliedstaaten und den USA bislang u. U. gestützt werden konnten, wurde für ungültig erklärt. Datentransfers[2] von Verantwortlichen aus der EU/EWR in die USA auf Basis des Privacy Shield sind nicht mehr möglich.
2. Standardvertragsklauseln können weiterhin abgeschlossen werden. Dies gilt jedoch auch nur noch dann, wenn Verantwortlicher und Auftragsverarbeiter gewährleisten können, dass die Klauseln des Vertrages eingehalten werden können. Ob die Parteien die Vertragsklauseln einhalten können, ist abhängig von den jeweiligen nationalen Gesetzen in den Drittländern.
3. Den Aufsichtsbehörden kommt die Befugnis bzw. Pflicht zu, Datentransfers zu prüfen und ggf. zu untersagen, wenn ein sicheres Datenschutzniveau nicht durch entsprechende Garantien gewährleistet werden kann.

[1] Aktuell gehören zu den sicheren Drittstaaten: Andorra, Argentinien, Kanada (nur kommerzielle Organisationen), Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay, Japan.

[2] Datentransfer: Übermittlung in die Drittstaaten (Staaten außerhalb der EU/EWR) oder mögliche Zugriffe aus Drittstaaten.

Folgende Aktivitäten sind zu ergreifen und jeder Schritt ist konsequent zu dokumentieren:

- Prüfung, ob Datentransfers in die USA oder andere Drittstaaten stattfinden bei
  - Gesellschaften innerhalb des Unternehmensverbunds
  - Dienstleistern (insbesondere Cloud- und SaaS-Anbieter)
  - Sub-Dienstleistern (insbesondere Cloud- und SaaS-Anbieter)
- Beurteilung der Notwendigkeit der betroffenen Verarbeitungen und der Unersetzbarkeit des Dienstleisters [inkl. Dokumentation]
  - Ist die Datenverarbeitung bzw. die Art der Datenverarbeitung zwingend erforderlich?
  - Ist im Rahmen der Datenverarbeitung ein Datentransfer in Drittstaaten erforderlich?
  - Kann der aktuell genutzte Dienstleister/Systemanbieter durch einen anderen Dienstleister innerhalb der EU/EWR ersetzt werden?
- Bei Feststellung der Erforderlichkeit und Unersetzbarkeit (Dokumentation nicht vergessen):
  - Kontaktaufnahme mit dem Dienstleister
  - Versand eines Fragebogens bezüglich Sub-Dienstleistern und Drittlandtransfers
  - Sofern der Vertragspartner eine EU-Gesellschaft ist und nur der Sub-Dienstleister in Drittstaaten sitzt: Erörterung der Möglichkeit, sich vertraglich zusichern zu lassen, dass ein Drittlandtransfer ausgeschlossen werden kann
    - Ist der Dienstleister selbst nach nachhaltiger Aufforderung nicht bereit, ist dies zu dokumentieren und die Unersetzlichkeit nochmal neu zu bewerten.
  - Erörterung der Möglichkeit, die Inhaltsdaten so zu verschlüsseln, dass eine Einsichtnahme durch den Dienstleister/Sub-Dienstleister nicht möglich ist
    - Ist dies nicht möglich, ist dies zu dokumentieren und die Unersetzlichkeit nochmal neu zu bewerten.

VII. Brexit: Anforderungen an den Datenschutz

Seit Ende Januar 2020 ist das Vereinigte Königreich, d. h. Großbritannien und Nordirland, kein EU-Mitglied mehr. Zwischen der Europäischen Union und dem Vereinigten Königreich war eine Übergangsvereinbarung bis zum 31. Dezember 2020 getroffen worden. Im aktuellen Entwurf des Brexit-Abkommens (Stand: 31.12.2020) wird eine weitere Übergangsfrist in Gang gesetzt. Im Abkommen ist eine viermonatige Übergangsfrist für Datenübermittlungen in das Vereinigte Königreich vorgesehen, die den befürchteten gravierenden Rechtsunsicherheiten vorbeugt (Article 10A Interim provision for transmission of personal data to the United Kingdom).

Demnach sollen Übermittlungen personenbezogener Daten von der EU in das Vereinigte Königreich (also Großbritannien und Nordirland) für eine Übergangsperiode nicht als Übermittlungen in ein Drittland (Art. 44 DSGVO) angesehen werden. Diese Periode beginnt mit dem Inkrafttreten des Abkommens und endet, wenn die EU-Kommission einen das Vereinigte Königreich betreffenden Angemessenheitsbeschluss getroffen hat, spätestens jedoch nach vier Monaten. Diese Frist kann um zwei Monate verlängert werden, falls keine der beteiligten

Parteien widerspricht. Die Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschlands fasste am 04. Januar 2021 einen entsprechenden Beschluss für Datenübermittlungen in das Vereinigte Königreich jedoch zunächst nur bis zum 30. April 2021 soweit und solange das Vereinigte Königreich die Voraussetzungen von Article 10A des Abkommens erfüllt.

Damit sind Übermittlungen in das Vereinigte Königreich vorerst weiterhin unter den bisherigen Voraussetzungen möglich. Gravierende Erschwernisse für die betroffenen Unternehmen werden so zunächst vermieden. Allerdings ist jetzt die EU-Kommission in der Pflicht, tragfähige Adäquanzentscheidungen vorzulegen, die auch die aktuelle Rechtsprechung des Europäischen Gerichtshofs berücksichtigen und von den Mitgliedstaaten genauso wie vom Europäischen Datenschutzausschuss sorgfältig zu prüfen sein werden.

Langfristig streben die Europäische Union und das Vereinigte Königreich einen Angemessenheitsbeschluss an, welcher das Niveau des Datenschutzes auch bei Drittlandtransfer in das Vereinigte Königreich gewährleisten würde. Einen derartigen Beschluss zu fassen, ist ein längerer Prozess, doch ist zu hoffen, dass dieser rechtzeitig gefasst wird. Die Europäische Kommission hat am 19. Februar 2021 das Verfahren zur Annahme von Angemessenheitsbeschlüssen bezüglich des Vereinigten Königreichs eingeleitet. Die Einholung einer Stellungnahme des Europäischen Datenschutzausschusses (EDSA) sowie die Zustimmung eines aus Vertretern der EU-Mitgliedstaaten bestehenden Komitologieausschusses sind noch erforderlich.

VIII. Passwortschutz

Das BSI rückte von seiner bisherigen Position ab, Passwörter regelmäßig zu ändern. In der aktuellen Ausgabe des BSI-Grundschutz-Kompendiums wurde die entsprechende Textpassage gestrichen. Passwortänderungen sind aus BSI-Sicht nur noch für folgende Fälle angeraten:

1. Ein Passwort sollte auf jeden Fall geändert werden, wenn es einen Hinweis gibt, dass es tatsächlich in die Hände von unbefugten Dritten gelangt ist.
2. Wenn festgestellt wird, dass das eigene Gerät mit einem Schadprogramm infiziert ist.
3. Wenn Cyber-Kriminelle bei Anbietern oder direkt bei Nutzerinnen und Nutzern vertrauliche personenbezogene Daten (inklusive Passwörter) abgegriffen haben.

Ob dies die einzigen Situationen sein sollen, bei denen ein Passwort-Wechsel angebracht ist, muss an dieser Stelle hinterfragt werden. Passwortänderungen, die über Jahre hinweg nur aus der Addierung der Zahl bestehen (das bestehende Passwort KleineMaus15% wird auf KleineMaus16% abgeändert), suggerieren eine Scheinsicherheit. Angreifer können solche Passwörter oftmals schnell erraten und knacken.

Gerade bei kritischen und hochsensiblen Systemen sollte weiterhin ein regelmäßiger, echter Passwortwechsel vorgenommen werden. Bedenken Sie hierbei bitte auch, dass ein entstehender Schaden deutlich größere Probleme hervorrufen kann als die Mühen, sich alle 90 oder 180 Tage ein neues Passwort zu merken.

Ein wichtiger Aspekt ist das Social Engineering: Zum einen könnten umstehende Personen einen immer mal wieder beim Eintippen eines Passworts beobachten und so mit der Zeit das entsprechende Passwort erraten, ohne dass der Betroffene selbst es merkt. Zum anderen kann durch den stetigen Passwortwechsel ein Dritter, der die Zugangsdaten entwendet hat, wieder aus einem Benutzerkonto ausgesperrt werden.

So ist ein Abrücken vom Passwort-Wechselzwang vor allem unter dem Gesichtspunkt der Informationssicherheit nicht zu empfehlen, da davon ausgegangen werden muss, dass die Offenlegung eines Passwortes häufig unbemerkt bleibt. Jedoch kann eine Ausdehnung des Gültigkeitszeitraums in unkritischen Bereichen eines Unternehmens in Betracht gezogen werden, um die Akzeptanz zu erhöhen.

IX. 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