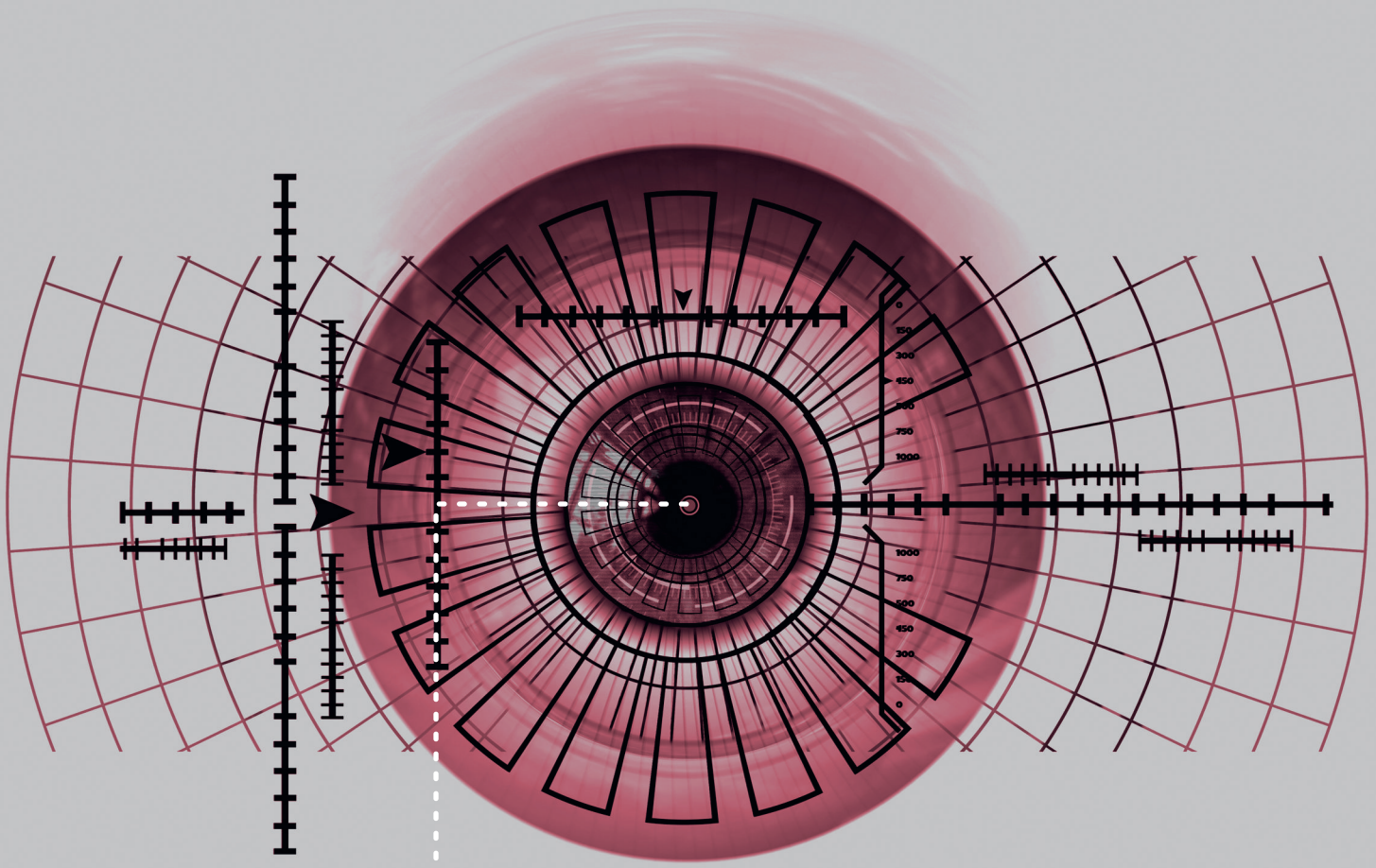


Tätigkeitsbericht 2019

KDSA Ost

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und
des Katholischen Militärbischofs

Herausgeber:

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und des Katholischen Militärbischofs

Margaretenstraße 1
39218 Schönebeck
Telefon: 03928 7287181
E-Mail: kontakt@kdsa-ost.de
www.kdsa-ost.de

„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus."

Bundesverfassungsgericht Urteil vom 15.12.1983 - 1BVR 209-83

4. Tätigkeitsbericht des Diözesandatenschutzbeauftragten

für

das Erzbistum Berlin
das Bistum Dresden-Meißen
das Bistum Erfurt
das Bistum Görlitz
das Bistum Magdeburg
den Katholischen Militärbischof

Berichtszeitraum 01.01.2019 bis 31.12.2019

Inhaltsverzeichnis

Vorwort

Jeder Ausführung zum Datenschutz ist voranzustellen, dass Datenschutz nicht Daten schützt, sondern Grundrechte, konkret Persönlichkeitsrechte, in Form des Rechts auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht aus Art. 1 und 2 Grundgesetz (GG) abgeleitet hat.

Bei allen Verlockungen, die Big Data, künstliche Intelligenz und die vermeintlich kostenlosen Dienste der social Media Konzerne offerieren, muss der Mensch immer im Mittelpunkt stehen. Jeder einzelne Mensch muss selbstbestimmt die Kontrolle über seine Daten behalten. Digitale Souveränität wird als Schlagwort oft genutzt, wenn es darum geht Datenschutzvorschriften im Sinne kommerzieller Unternehmen zu lockern, weil es doch dem Einzelnen überlassen bleiben müsse, wem er seine Daten gegebenenfalls im Austausch für andere Leistungen zur Verfügung stellt. Gerade hier setzt aber die Verpflichtung der Datenschützer ein, dafür zu sorgen, dass die Kontrolle und damit auch das Vertrauen in die Datenverarbeitung erhalten bleibt. Dieses Unterfangen ist deshalb so schwierig, weil es bei den Betroffenen bzw. Anwendern ein erhebliches Datenschutzparadoxon gibt. Verbraucher fordern häufig mehr oder weniger lautstark mehr Kontrolle über ihre Daten im Internet. Gleichzeitig sind sie aber vielfach nicht bereit, dafür Abstriche bei der Bequemlichkeit in Kauf zu nehmen oder für die angebotenen Dienste konkret Geld zu bezahlen, anstatt mit ihren Daten. Viele geben sich überrascht und empören sich, wenn aufgedeckt wird, an wen ihre personenbezogenen Daten von dem App- oder Seiten-Betreiber, dessen Dienste sie in Anspruch nehmen, weiterverkauft werden. Dabei ist den Verkäufern nicht unbedingt ein Vorwurf zu machen, wenn sie denn ihre Kunden über ihr Geschäftsmodell transparent informieren. Dies ist jedoch häufig nicht der Fall. So kommt es, dass uninformierte Nutzer einer Datenschutzaufsicht gegenüberstehen, die um die Risiken weiß und die Nutzung bestimmter Dienste untersagt, weil diese auch die Rechte Dritter beeinträchtigen. Immer wieder gibt es deshalb Differenzen im Hinblick auf die Anfertigung und Versendung von Fotos oder nunmehr auch im Hinblick auf die Nutzung von Facebook Fanpages.

Auch kleinere kirchliche Vereine oder Einrichtungen äußern den Wunsch nach weniger strikten Datenschutzvorschriften. Aus ihrer Sicht ist diese

Forderung vielleicht zunächst nachvollziehbar. Bei genauerer Betrachtung, insbesondere wenn man die Perspektive der betroffenen Personen einnimmt, erschließt sich nicht, warum ihre Daten in einer kleinen Einrichtung weniger schützenswert sein sollen, als bei der Verarbeitung durch kommerzielle Konzerne.

Führt man sich das Spektrum vor Augen, in dem gerade kirchliche Vereine und Einrichtungen tätig sind, erscheint die Beachtung von Persönlichkeitsrechten und damit die Einhaltung eines konsequenten Datenschutzes besonders wichtig. Vereine, die sich um Haftentlassene, psychisch Kranke und Wohnungslose kümmern oder Klienten in sozialen Notlagen oder Schwangerschaft beraten, Vereine die in jedem Fall Gesundheits- und Sozialdaten verarbeiten oder Kinder und Schüler betreuen, sollte zum Schutz ihrer Klientel eine erhöhte Sensibilität für den Datenschutz wichtig sein.

Diese Forderung betrifft aber nicht nur die Hauptamtlichen, sondern in gleicher Weise Laien. Häufig sind sie es, die sich an Aktionen gegen die Übergriffigkeit von Kirche beteiligen. Diese Aktivitäten mögen oftmals gerechtfertigt sein. Übergriffigkeit fängt aber da an, wo die Persönlichkeitsrechte des anderen nicht akzeptiert werden. Dort, wo das eigene Ego über die Rechte des Anderen gestellt wird. Wenn Fotos von Personen ungefragt auf der eigenen Homepage veröffentlicht werden, um darzustellen wie schön das Sommerfest im Altenheim oder im Kindergarten war oder um die Gemeinschaft bei den Pfadfindern zu dokumentieren, findet diese Darstellung ausschließlich im Eigeninteresse statt. Die Fotos der Abgebildeten ohne deren Zustimmung zu diesem Zweck zu verwenden ist übergriffig.

Das gleiche gilt beim Betreiben von Facebook Fanpages. Der Betrieb dieser Seiten wird als unverzichtbar bezeichnet, weil Kirche damit angeblich eine Verbindung zur jüngeren Generation aufgebaut hat und diese jetzt auch über ein modernes Medium erreichen kann. Dabei ist es primär ein eigenes Interesse, was Kirche hier verfolgt. Da mag es stören, wenn die Datenschutzaufsicht darauf hinweist, dass Facebook die bei der Nutzung anfallenden Metadaten möglicherweise zur Erstellung von Persönlichkeitsprofilen nutzt, in jedem Fall aber über die Erhebung und Nutzung dieser Daten keine rechtskonforme Auskunft erteilt. Wer im Eigeninteres-

se darüber hinwegsieht und eine Gefährdung der Nutzer billigend in Kauf nimmt, handelt übergriffig.

Kirche hat sich immer für den Schutz der Schwachen eingesetzt. Das ist gut! Konsequent wäre es, den Schutz der Schwächeren auch dann in den Vordergrund zu stellen, wenn es der eigenen Selbstdarstellung nicht nutzt.

1 Die Entwicklung des Datenschutzes

1.1 Die Entwicklung des Datenschutzes in der Bundesrepublik Deutschland

Im Jahr der Einführung von Datenschutz-Grundverordnung (DS-GVO) und Bundesdatenschutzgesetz (BDSG) 2018 gab es große Vorbehalte gegen diese gesetzlichen Regelungen. Die Wirtschaft befürchtete eine weitere Belastung mit bürokratischen Regelungen. Insbesondere kleinere Unternehmen glaubten die Vorschriften nicht umsetzen zu können und fürchteten Abmahnungen. Datenschutz bekam auf einmal eine bis dahin ungewohnte Aufmerksamkeit, was im Wesentlichen wohl auf die in den Gesetzen angedrohten, für deutsche Verhältnisse exorbitanten Strafen, zurückzuführen war.

Die Datenschutzbehörden sind dieser Stimmung mit Besonnenheit entgegengetreten. Es wurden zahlreiche Beratungen durchgeführt und umfangreiches Informationsmaterial veröffentlicht. Von der Möglichkeit Strafen zu verhängen wurde zunächst restriktiv Gebrauch gemacht.

Dieses Vorgehen bestimmte zunächst auch das Jahr 2019.

In der zweiten Jahreshälfte gab es jedoch dann erste Meldungen über zum Teil empfindlich hohe Geldbußen gegen Verantwortliche. Dabei handelte es sich aber durchweg um große Unternehmen. Die zunächst vorgetragene Befürchtung, die Kleinen würden hängen, die Großen lässt man laufen, wurde somit nicht bestätigt.

Gegen Ende des Jahres fand die erste Änderung des BDSG statt. Aufgrund von Anregungen aus der Wirtschaft, namentlich kleinerer Betriebe, wurde das Quorum des § 38 Abs. 1 BDSG für die Verpflichtung einen betrieblichen

Datenschutzbeauftragten zu benennen heraufgesetzt. Nunmehr müssen Verantwortliche einen betrieblichen Datenschutzbeauftragten erst benennen, wenn in der Regel mindestens 20 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, vorher galt diese Verpflichtung ab zehn Mitarbeitern. Der Sinn dieser Regelung ist durchaus zweifelhaft, da sich der Verantwortliche nunmehr allein um die Einhaltung des Datenschutzes kümmern muss. Der Verzicht auf einen kompetenten Berater kann sich dabei als zusätzliche Belastung erweisen und das Bußgeldrisiko erhöhen.

Außerdem wurde § 26 BDSG geändert. Eine Einwilligung im Beschäftigungskontext kann nunmehr „schriftlich" oder „elektronisch" erfolgen. Zuvor war dafür die Schriftform gem. § 126 BGB erforderlich. Diese Änderung dürfte eine Klarheit im Rechtverkehr herbeiführen, da vielen Betroffenen zuvor nicht verständlich gewesen sein dürfte, dass eine E-Mail der Schriftform nicht entspricht, sondern nur als Textform[1] gilt.

1.2 Datenschutz in der katholischen Kirche

Das Vorgehen der fünf Datenschutzaufsichten in der katholischen Kirche hat sich von dem der Landesbeauftragten nicht wesentlich unterschieden. Auch hier wurden im letzten Jahr weiterhin Informationsveranstaltungen und Beratungen mit Betroffenen und Verantwortlichen abgehalten.

Ein Austausch mit den Landesdatenschutzaufsichten fand ebenso statt, wie mit den Datenschutzaufsichten der evangelischen Kirche.

Anfang März wurde die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) von den Bischöfen in Kraft gesetzt, die die bis dahin übergangsweise fortgeltende KDO-DVO ersetzt hat. Diese Verordnung ergänzt die gesetzlichen Regelungen um praxisnahe Ausführungen. Auch die Verordnung nimmt ebenso wie bereits das Gesetz bisher bestehende Regelungen auf und passt die Festlegungen der alten Verordnung an die neue Gesetzeslage an.

Eine Veränderung des Rahmengesetzes hat im Gegensatz zum staatlichen Bereich nicht stattgefunden. Tatsächlich haben sich bislang die vor-

1 BT-Drs.17/12637 S.44

handenen Regelungen in der Praxis grundsätzlich bewährt. Soweit sich in einzelnen Bereichen ein Änderungsbedarf aus der Praxis ergeben hat, sind solche in dem durch § 58 Abs. 2 KDG geforderten Evaluationsprozess bis zum Mai 2021 zu klären. Jede Änderung muss sich dabei an der europäischen Verordnung orientieren, damit der Einklang mit diesen Regelungen und damit die Grundlage für einen eigenen kirchlichen Datenschutz nicht in Frage gestellt wird. Deshalb steht bereits jetzt fest, dass es im Rahmen dieses Prozesses nicht zu einer grundsätzlichen Diskussion über die Grundlagen des Datenschutzes kommen muss. Es liegt vielmehr ein gutes, praktikables und dem europäischen Standard entsprechendes Gesetz vor.

Ein Schwerpunkt der Arbeit unserer Aufsicht lag darin, einen engen Kontakt zum einen zu den datenschutzrechtlichen Verantwortlichen zum anderen zu den betrieblichen Datenschutzbeauftragten und zu Multiplikatoren zu erhalten.

Die von uns errichteten Arbeitskreise mit den betrieblichen Datenschutzbeauftragten der unterschiedlichen Einrichtungen bzw. Einrichtungsarten haben sich weiter etabliert. Diese finden mehrmals jährlich bei guter Beteiligung statt

Einen weiteren wichtigen Kreis von Multiplikatoren stellen die Mitglieder der Mitarbeitervertretungen dar. In allen Bistümern wurden Veranstaltungen für die Interessenvertretungen angeboten. Dieser Personenkreis sollte besonders für den Datenschutz sensibilisiert werden, da durch die Mitarbeitervertretungsordnung den Interessenvertretungen die Verpflichtung auferlegt wird, für die Einhaltung von Recht und Billigkeit in den Einrichtungen einzutreten. Diese Verpflichtung fordert auch auf die Einhaltung der Vorschriften zum Datenschutz zu achten.

Weiterhin wurden von unserer Aufsicht Veranstaltungen für Erzieherinnen und Erzieher der Kindergärten in den Bistümern durchgeführt. Dabei ging es insbesondere darum, nicht nur die Leiter/innen der Einrichtungen anzusprechen, sondern vor allem auch die Erzieher/innen, die in direktem Kontakt mit den Betroffenen, also den Kindern und deren Eltern, stehen.

Im Berichtsjahr hat die Zahl der gemeldeten Datenschutzvorfälle stetig zugenommen. Dabei erfolgt ein großer Teil der Meldungen von den betrieb-

lichen Datenschutzbeauftragten oder den Verantwortlichen über die zentral eingerichtete Meldeplattform. Darüber hinaus mehrt sich aber auch die Anzahl der Beschwerden von Betroffenen stetig. Im letzten Quartal des Berichtsjahres wurden einige Bußgeldverfahren eingeleitet. Solche Verfahren werden durch das KDG im Gegensatz zur vorherigen Gesetzeslage ermöglicht.

2 Gemeldete Datenschutzvorfälle

2.1 Wann ist eine Datenschutzverletzung zu melden?

Seit der Einführung des KDGs am 24.05.2018 sind alle Einrichtungen, die dem KDG unterliegen, verpflichtet Datenschutzverletzungen an die Datenschutzaufsicht zu melden.

Die einzelnen Regelungen dazu finden sich in den §§ 33 und 34 KDG wieder. Im Regelfall hat die Mitteilung durch den Verantwortlichen innerhalb von 72 h an die Behörde zu erfolgen, eine verzögerte Meldung ist zu begründen.

Die DS-GVO sieht vor, dass sämtliche Datenschutzverletzungen zu melden sind, „es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt." § 33 Abs. 1 KDG lautet dagegen: „Der Verantwortliche meldet der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt."

Die beiden Regelungen sind nur scheinbar identisch. Nach dem europäischen Recht ist für den Fall, dass eine Rechtsverletzung noch nicht absehbar ist, jedenfalls eine Meldung zu erstatten. Nach der Regelung des KDG kann in diesem Fall eine Meldung unterbleiben. Um hier die Gleichwertigkeit der kirchlichen Regelung nicht infrage zu stellen, muss auf jeden Fall eine Dokumentation im Sinne des § 33 Abs. 4 KDG erfolgen, auch wenn der Verantwortliche der Auffassung ist, dass Risiken für geschützte Rechte in Wirklichkeit gar nicht bestehen.

2.2 Online-Meldung einer Datenschutzverletzung

Für die Meldung einer Datenschutzverletzung werden im § 33 Abs. 3 KDG Mindestanforderungen formuliert, welche bei der Nutzung des Online-Formulars auf den Webseiten der Datenschutzaufsichten abgefragt werden. Durch das Ausfüllen des Online-Formulars erhält die Datenschutzaufsicht alle notwendigen Informationen, die für eine erste Beurteilung der Datenschutzverletzung erforderlich sind.

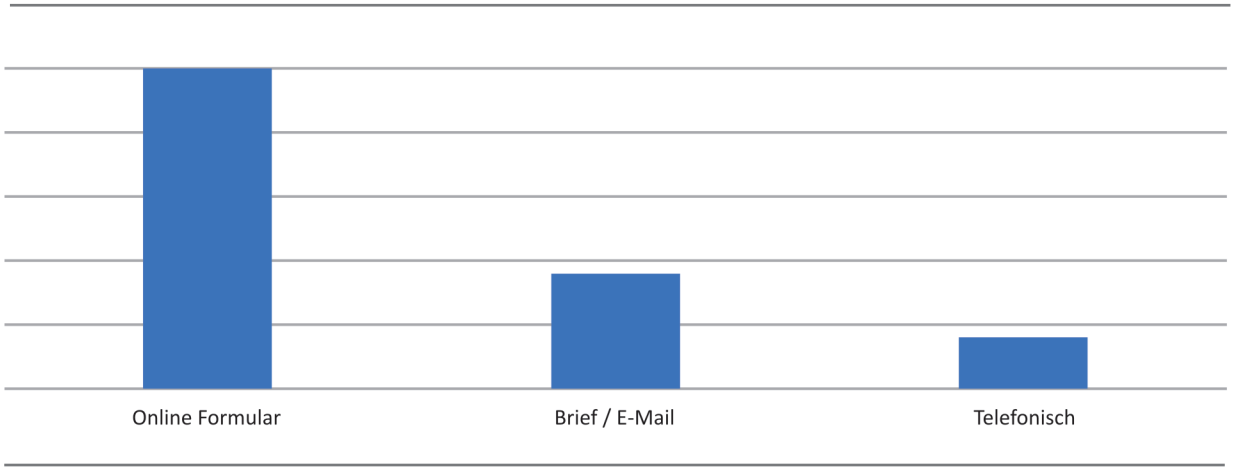
Dennoch besteht die Möglichkeit der Datenschutzaufsicht auch einen Datenschutzvorfall in anderer Form wie z.B. als E-Mail, per Brief oder Telefonat zu melden. Diese Vorfälle oder vermehrt auch Beschwerden werden in der Praxis meist von den direkt Betroffenen oder auch von Mitarbeitern der Einrichtungen der Datenschutzaufsicht zugetragen. Für die Nutzung der anderen Kommunikationswege neben der Möglichkeit Datenschutzverletzungen oder Beschwerden über das Online-Formular zu melden, gibt es unterschiedliche Gründe.

Zum einen haben diese betroffenen Personen meistens keine Kenntnis darüber, dass es ein Online-Formular bei der zuständigen Aufsichtsbehörde gibt. Daneben haben die Betroffenen häufig auch keine Kenntnis darüber, dass es für die kirchlichen und caritativen Einrichtungen eine eigenständige zuständige kirchliche Datenschutzaufsichtsbehörde gibt. Das liegt sowohl an der Unwissenheit der Betroffenen, für die die Regelungen im Datenschutz immer noch recht neu sind als auch daran, dass Betroffene nicht um das Bestehen von kirchlichen Datenschutzaufsichten wissen oder das Datenschutzerklärungen der Einrichtungen den Hinweis auf das Beschwerderecht bei der zuständigen Aufsichtsbehörde nicht enthalten. So wissen beispielsweise Patienten, die sich in kirchlichen Krankenhäusern behandeln lassen, meistens nicht, dass für diese Einrichtungen nicht die Landesdatenschutzaufsichten, sondern die kirchlichen Datenschutzaufsichten zuständig sind.

Weiterhin wird das Online-Formular nicht verwendet, weil Betroffene am Arbeitsplatz keine Möglichkeit besitzen dieses zu nutzen, da ihnen kein PC-Arbeitsplatz zur Verfügung steht.

Häufig wollen sich die betroffenen Personen erstmal nur telefonisch über einen Sachverhalt beschweren, ohne zu wissen, dass es sich bei ihrem Anliegen um eine Datenschutzverletzung nach dem KDG handelt.

Die Verteilung der unterschiedlichen Kommunikationswege, die seit Inkrafttreten des KDG genutzt wurden, um Datenschutzvorfälle zu melden, lässt sich vereinfacht auch durch dieses Diagramm darstellen:



Es lässt sich ferner feststellen, dass 2018 die Meldungen ausschließlich über das Online-Formular der Datenschutzaufsicht zugetragen wurden. Hingegen nahm im zweiten Jahr nach der Einführung des KDG bzw. der DS-GVO die Anzahl der Beschwerden von Betroffenen deutlich zu. Eine steigende Sensibilität der Bevölkerung gegenüber dem Datenschutz sowie auch die gestiegene Kenntnis über das allgemeine Recht zur Beschwerde sind die vermutlichen Gründe dafür.

2.3 Datenschutzvorfälle nach Einrichtungsart

Bei der Bearbeitung der seit dem 24. Mai 2018 gemeldeten und zugetragenen Datenschutzvorfälle konnte beobachtet werden, dass sich in einigen Einrichtungen häufiger Datenschutzvorfälle zutragen bzw. gemeldet werden als in anderen Einrichtungen.

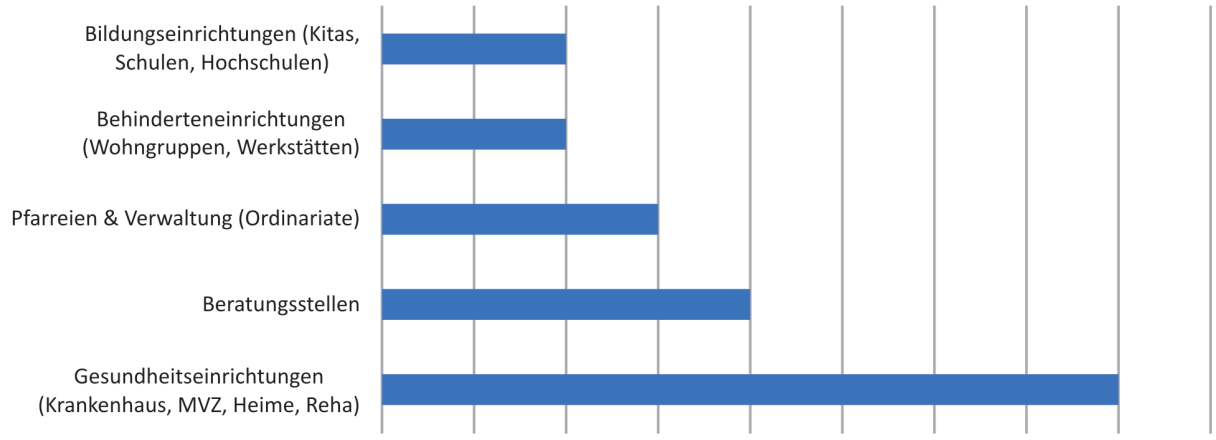
So war das Auftreten von Datenschutzverletzungen in Einrichtungen des Gesundheitswesens größer als in den Pfarreien oder Verwaltungen. Rückschlüsse, dass in den Einrichtungen des Gesundheitswesens nachlässig mit

personenbezogen Daten umgegangen wird, lassen sich daraus aber nicht ziehen.

Gerade die Gesundheitseinrichtungen legen einen besonders großen Wert auf den Schutz personenbezogener Daten, da vorwiegend i.S.d. § 4 Nr. 2 KDG besondere Kategorien personenbezogener Daten (Gesundheitsdaten) verarbeitet werden. Ein zentraler Grund für das höhere Auftreten von Datenschutzverletzungen im Gesundheitswesen ist das sehr hohe Arbeitsaufkommen im Kontext mit einer viel höheren Anzahl von Betroffenen (Mitarbeiter, Patienten). Weiterhin ist es die Hauptaufgabe dieser Einrichtungen Patienten zu behandeln und somit Gesundheitsdaten ständig zu erfassen, zu speichern, abzurufen, zu verändern, zu übermitteln oder zu löschen. Eigentlich hat fast jeder Prozess des Aufenthalts eines Patienten im Krankenhaus zur Folge, dass personenbezogene Daten oder besondere Kategorien personenbezogener Daten in irgendeiner Form nach § 4 Nr. 4 KDG verarbeitet werden.

Somit ist die höhere Fallzahl in den Einrichtungen des Gesundheitswesens hauptsächlich der Tatsache geschuldet, dass dort vielmehr personenbezogene Daten verarbeitet werden und diese Einrichtungen einen deutlich höheren Betroffenenkreis haben als die anderen Einrichtungen. Auch sind die betrieblichen Datenschutzbeauftragten in diesen Einrichtungen erheblich sensibler.

Die Abbildung zeigt die Verteilung der gemeldeten Vorfälle nach Einrichtungsart.



Auch in Beratungsstellen treten vermehrt Datenschutzverletzungen auf, da auch hier analog den Einrichtungen aus dem Gesundheitswesen vorwiegend mit personenbezogenen Daten der Klienten gearbeitet wird.

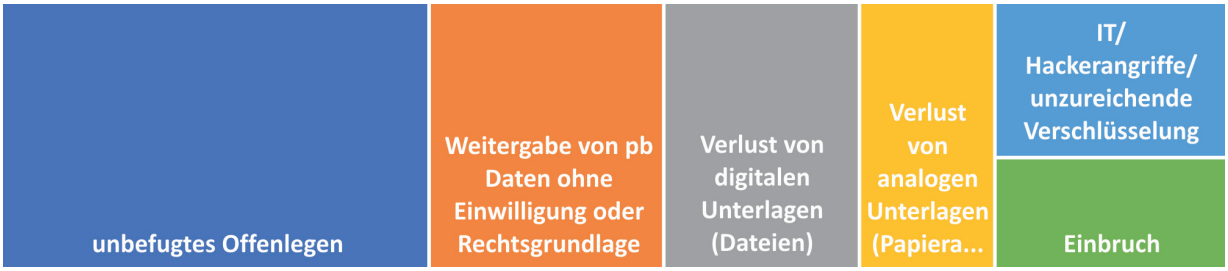
In den Pfarreien stehen dagegen die Verkündigung des Glaubens und die Seelsorge im Mittelpunkt. In Ordinariaten und anderen kirchlichen Administrationen wird sich hauptsächlich mit der Verwaltung der kirchlichen Strukturen und Territorien beschäftigt. Daher werden nicht ausschließlich und allein personenbezogene Daten verarbeitet, was dahingehend auch das Auftreten von Datenschutzvorfällen mindert.

Bildungseinrichtungen wie Kindertagesstätten oder Schulen haben in erster Linie einen Betreuungs- und Bildungsauftrag, so dass das pädagogische und fachliche Arbeiten hier der Schwerpunkt der Mitarbeiter ist. Trotzdem tragen diese Einrichtungen eine besonders große Verantwortung in dem Umgang mit personenbezogenen Daten ihrer Betroffenen, da es sich bei diesen hauptsächlich um Minderjährige handelt, die es besonders zu schützen gilt.

2.4 Charakteristik der Datenschutzvorfälle

Die der Kirchlichen Datenschutzaufsicht gemeldeten Vorfälle sind sehr unterschiedlicher Natur und ereignen sich auf sehr unterschiedliche Art und Weise. So kann es beispielsweise bei einem Einbruch auch immer zum Verlust von personenbezogenen Daten kommen, weil Fotoapparate oder Gehaltsunterlagen gestohlen wurden.

Besonders Datenschutzvorfälle im IT-Bereich sind schwierig aufzuschlüsseln, da diese zum einen nicht sofort entdeckt werden oder nicht absehbar ist, welche Daten wohin abgeflossen sind. Dennoch können die Datenschutzvorfälle, je nach dem was passiert ist, wie folgt eingeteilt werden:



Einteilung der Datenschutzvorfälle

- unbefugtes Offenlegen
- Weitergabe von pb Daten ohne Einwilligung oder Rechtsgrundlage
- Verlust von digitalen Unterlagen (Dateien)
- Verlust von analogen Unterlagen (Papierakten)
- IT / Hackerangriffe / unzureichende Verschlüsselung
- Einbruch

Die häufigsten Datenschutzvorfälle sind dadurch entstanden, dass Daten unbefugt offengelegt wurden. Dies passiert beispielsweise indem ein Arztbrief einen falschen Empfänger erreicht oder Gehaltsunterlagen mehrerer Mitarbeiter ungeschützt auf dem Schreibtisch eines Sachbearbeiters lagen. Die Vielzahl der Vorfälle zeigt auf, dass bei dem Umgang mit personenbezogenen Daten bzw. besonderen personenbezogenen Daten oft nicht die nötige Gewissenhaftigkeit an den Tag gelegt wird. Oft ist den Mitarbeitern auch nicht bewusst, welche Folgen bei Unaufmerksamkeit oder Ablenkung entstehen können. Hier ist es wichtig eindeutige Prozesse und Kontrollen zu etablieren, die kleine aber häufige Fehlerquellen ausschließen lassen.

In der Summe ist auch der Verlust von Daten recht häufig aufgetreten. Nach KDG § 7 Abs. (1) lit f) müssen personenbezogene Daten auch vor unbeabsichtigten Verlust geschützt werden. Es müssen somit geeignete technische und auch organisatorische Maßnahmen getroffen werden, die verhindern, dass Daten verloren gehen.

Digitale Daten gehen verloren, indem technische Geräte wie Laptops, Handys, externe Festplatten bei einem Einbruch entwendet werden oder hilfreiche technische Begleiter wie MDA-Geräte oder Smartphones bei Klienten oder Patienten liegen bleiben. Durch geeignete Sicherheitsmechanismen kann zwar der Verlust dieser Geräte nicht verhindert werden, jedoch der Zugriff auf die Daten, die auf den Geräten gespeichert sind.

Trotz der zunehmenden Digitalisierung gehen auch analoge Daten in Form von Papierakten verloren. Dies kann verhindert werden, indem sensible

Daten in verschlossenen Schränken aufbewahrt werden und zudem in einer geeigneten Form Sicherheitskopien angefertigt werden. Das Anfertigen und Löschen von Sicherheitskopien sollten als Prozesse in einer Einrichtung etabliert sein.

3 Datenschutz allgemein

3.1 Betrieblicher Datenschutzbeauftragter (bDSB)

3.1.1 Reduzierung des Quorums für die Bestellung eines bDSB.

Durch Änderung des Bundesdatenschutzgesetzes zum 20.11.2019 wurde u. a. bestimmt, dass ein Betrieblicher Datenschutzbeauftragter nicht bereits dann zu bestellen ist, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Dieses Quorum ist heraufgesetzt worden. Ein Betrieblicher Datenschutzbeauftragter ist zu bestellen, wenn mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.[2]

Nach Bekanntwerden dieser Änderung kamen Anfragen aus verschiedenen Einrichtungen an unsere Dienststelle, ob dies nunmehr auch für den Bereich des KDG gelte. Eine Änderung des Gesetzestextes des BDSG hat keine Auswirkungen auf den Gesetzestext des KDG. Das KDG gilt nicht neben DS-GVO und BDSG, sondern an deren Stelle. Sofern das KDG gegenüber DS-GVO und BDSG abweichende Formulierungen verwendet, können daraus bestenfalls Schlüsse für die Auslegung der KDG Vorschrift gezogen werden.

Nicht in jedem Fall war klar, ob die Nachfragenden die gesamte Regelung zur Benennung eines Betrieblichen Datenschutzbeauftragten gem. § 38 KDG im Blick hatten.

So stellt § 38 Abs. 2 Nr. 1 KDG auf die Personen ab, die sich „ständig mit der Verarbeitung personenbezogener Daten beschäftigen“. Im Gegensatz

2 Bundesgesetzblatt Jahrgang 2019 Teil I Nr. 41, Seite 1634

zu der staatlichen Regelung wird hierbei nicht nur auf die „automatisierte Verarbeitung“ abgestellt. Der Anwendungsbereich des kirchlichen Gesetzes ist also deutlich weiter gefasst.

Nach der Intention des Gesetzes unterstützt der betriebliche Datenschutzbeauftragte den Verantwortlichen. Das ändert aber nichts an der fortbestehenden Verantwortung des Verantwortlichen. Die gesetzliche Neuregelung verzichtet also lediglich darauf, dem Verantwortlichen eine Unterstützung in datenschutzrechtlicher Hinsicht verpflichtend an die Seite zu stellen. Ob sich das, insbesondere für kleinere Einrichtungen, für deren Entlastung diese Regelung verabschiedet worden ist, tatsächliche als solche auswirkt, darf bestritten werden. Vielmehr ist anzunehmen, dass dem Verantwortlichen aus der Regelung eine Mehrarbeit erwächst. Schon aus diesem Grund sollte bei einer kommenden Evaluation des KDG von einer entsprechenden Änderung Abstand genommen werden.

Auch dürfte eine solche Änderung auf die dem KDG unterliegenden Einrichtungen wenig Auswirkungen haben. Kirchliche Stellen des verfassten Bereichs sind gem. § 38 Abs. 1 KDG in jedem Fall verpflichtet, einen bDSB zu benennen.

Die weiteren Einrichtungen werden häufig aufgrund der Regelungen des § 38 Abs. 2 lit. b) und c) KDG zur Benennung verpflichtet sein, da deren Kerntätigkeit in der umfangreichen Verarbeitung personenbezogener Daten besonderer Kategorie besteht.

Als „Kerntätigkeit“ lassen sich die wichtigsten Arbeitsabläufe betrachten, die zur Erreichung der Ziele des Verantwortlichen oder des Auftragsverarbeiters (Geschäfts- / Unternehmenszweck bzw. Unternehmensstrategie) erforderlich sind, also alle Maßnahmen, die den Geschäftszweck unmittelbar fördern, die wesentlich oder maßgeblich zum Gesamtwertschöpfungsprozess des Verantwortlichen beitragen.[3] Dies trifft im Besonderen auf die Beratungsangebote der Caritas und anderer Träger (Ehe-Familien- Lebensberatung, Suchtberatung, Schwangerenberatung u. v. m.) zu.

3 LfDI BW - 34. Tätigkeitsbericht 2018 S. 26

3.1.2 Können juristische Personen bDSB sein?

Diese umstrittene Frage ist auch im kirchlichen Datenschutzrecht virulent. Eine einheitliche Stellungnahme dazu liegt weder von der Datenschutzkonferenz (DSK) der Länder und des Bundes, noch von der Konferenz der katholischen Datenschutzaufsichten vor.

Die Kritiker, die die Beauftragung einer juristischen Person als bDSB ablehnen beziehen sich primär auf den Gesetzestext, nachdem aus dieser Sicht nur natürliche Personen die personenbezogenen Anforderungen des Art. 37 Abs. 5 erfüllen könnten.[4] Auch § 36 Abs. 6 KDG spricht insoweit von „erforderlicher Fachkunde und Zuverlässigkeit", somit also von Attributen, die nur einer natürlichen Person zugerechnet werden können. Weiterhin wird auf die englische Sprachfassung der DS-GVO hingewiesen, die mit Verwendung der Bezeichnungen „his or her" sowie „he or she" nur natürliche Personen anspricht.[5]

Andererseits findet sich in der DS-GVO aber auch an keiner Stelle eine Regelung, die ausdrücklich juristische Personen von der Bestellung ausnimmt. Die Tatsache, dass in Art. 37 nicht zwischen natürlicher und juristischer Person unterschieden wird, obwohl der Verordnung eine entsprechende Differenzierung bekannt ist, spricht für die Zulassung beider Möglichkeiten.[6]

Offensichtlich um diese Problematik zu umgehen, hat sich in der Praxis unserer Dienststelle eine Umgehung verbreitet. Anstatt die juristische Person, regelmäßig eine GmbH, als bDSB zu benennen, wird der Geschäftsführer der juristischen Person benannt. Da bestimmte Namen immer wieder auftauchen und die Verantwortlichen, die diese Person angeblich benannt haben räumlich weit auseinanderliegen, drängt sich die Frage auf, ob der benannte bDSB seinen Aufgaben noch umgehend nachkommen kann, wie es § 37 Abs. 7 KDG verlangt. Aus diesem Grunde wird eine solche Praxis von unserer Dienststelle abgelehnt.

Die Art.-29-Datenschutzgruppe geht davon aus, dass auch Organisationen als externe Datenschutzbeauftragte benannt werden können, dass in diesem Fall aber alle Mitarbeiter dieser Organisation, die Aufgaben des Da-

4 LfDI BW 34 TB 2018, S. 27; Drewes in Simitis Art. 37 Rn.49
5 ULD Saarland 27. TB Pkt 9.1.3.
6 Helfrich in Sydow DS-GVO Art. 37 Rn. 118

tenschutzbeauftragten übernehmen, die gesetzlichen Anforderungen an den Datenschutzbeauftragten erfüllen müssen. Für die Qualifikation kann dagegen auf die Gesamtheit des Teams abgestellt werden.

In diesem Fall ist aus hier vertretener Sicht das Aufführen aller Mitarbeiter/innen der juristischen Person, die mit der Ausübung des Amtes als Betrieblicher Datenschutzbeauftragter beauftragt sind, erforderlich.

3.2 Informationspflicht per Aushang oder Bestätigung durch Unterschrift

Vieles was im KDG (bzw. der DS-GVO) geregelt ist, ist nicht neu, sondern fand sich bereits -und häufig auch schon sehr lange- in der Vorgängerregelung, der KDO (im Bundesdatenschutzgesetz, BDSG). Wirklich neu sind aber die Informations- und Auskunftsrechte in den §§ 14 ff. KDG.

Mehrere Einrichtungen fragten bei uns an, ob sie sich die Erfüllung der Informationspflicht von Klienten durch Unterschrift bestätigen lassen müssen.

Eine Unterschrift der betroffenen Person als Bestätigung dafür, dass sie die Information bekommen bzw. zur Kenntnis genommen hat, ist im Gesetz nicht vorgesehen. Der betroffenen Person muss die Information nach § 15 KDG mitgeteilt werden, eine Annahmepflicht besteht für die betroffene Person aber nicht.

Bei persönlicher Anwesenheit kann die Informationspflicht erfüllt werden, indem aktiv auf einen Aushang oder einen ausliegenden Flyer mit einer Zusammenfassung der Basisinformationen hingewiesen wird. Für die weitergehenden Informationen kann dann auf eine Webseite verwiesen werden.

Verlangt der Verantwortliche von der betroffenen Person eine Unterschrift zur Bestätigung der Kenntnisnahme bringt er sich selber in eine unsichere Situation, wenn die Unterschrift vom Betroffenen verweigert wird. Gerade im Sozial- Gesundheits- und Pflegebereich stellt sich dann die Frage, ob diese Weigerung eine Ablehnung der Behandlung rechtfertigt. Da eine gesetzliche Regelung fehlt, ist das nicht der Fall. Damit ist die Unterzeichnung nicht erforderlich.

Ausreichend und erforderlich ist es in jedem Fall die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache zu übermitteln.

3.3 Haftung für Datenschutzverstöße

Wie vielerorts bereits betont, ist die Aufmerksamkeit für den Datenschutz in den letzten zwei Jahren wohl weniger durch die Einsicht in die Notwendigkeit des Persönlichkeitsschutzes gestiegen, als vielmehr den nunmehr in den Datenschutzgesetzen festgeschriebenen Geldbußen geschuldet. Die Bußgeldandrohung im KDG ist deutlich geringer als in der DS-GVO. Dennoch ist sie erstmals in einem kirchlichen Gesetz festgeschrieben und die Datenschutzaufsichten sind verpflichtet, Geldbußen zu verhängen, nicht zuletzt um den Einklang zu den staatlichen Regelungen aufrecht zu erhalten.

Wohl vor diesem Hintergrund gab es bereits einige Anfragen, insbesondere von Mitarbeitervertretungen, wer durch die Datenschutzaufsicht mit einem Bußgeld belegt werden kann.[7]

Nach § 51 Abs. 1 KDG kann die Datenschutzaufsicht gegen einen Verantwortlichen oder einen Auftragsverarbeiter eine Geldbuße verhängen. Bei Auftragsverarbeitern handelt es sich regelmäßig um externe (juristische oder natürliche) Personen. Verantwortlicher ist die natürliche oder juristische Person bzw. Einrichtung, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (§ 4 Nr. 9 KDG). Mitarbeitende, die im Rahmen ihres Dienstvertrages unselbständige Arbeit für den Dienstgeber verrichten, haben die Entscheidungen über Zweck und Mittel der Verarbeitung, die der Dienstgeber trifft zu akzeptieren und umzusetzen. Ausdrücklich verlangt das Gesetz vom Verantwortlichen, dass Personen, die Zugang zu personenbezogenen Daten haben diese nur auf dessen Anweisung hin verarbeiten (§26 Abs. 5 KDG). Eine Entscheidung über Zweck und Mittel steht Mitarbeitenden ausdrücklich nicht zu. Somit sind sie keine Verantwortlichen und deshalb auch nicht Adressat eines Bußgeldbescheides.

7 Ausführlich Ullrich in ZMV 2020, 1 ff.

Etwas anderes kann ausnahmsweise dann gelten, wenn ein/e Mitarbeiter/in personenbezogene Daten, die ihm/ihr dienstlich zugänglich geworden sind für rein private Zwecke nutzt, die jeden Bezug zum Arbeitsverhältnis vermissen lassen. (Beispiel: Ein Arzt nutzt die Kontaktdaten einer Patientin für den Versuch sich mit ihr privat zu verabreden.) In diesem Fall bestimmt der/die Mitarbeiter/in selber über Zweck und Mittel der Datenverarbeitung und schwingt sich so zum Verantwortlichen auf, mit der Konsequenz mit Geldbuße belegt werden zu können.

3.4 Facebook Fanpage

Nach einer Entscheidung des Bundesverwaltungsgerichts in Leipzig kann der Betreiber eines im sozialen Netzwerk Facebook unterhaltenen Unternehmensauftritts (Fanpage) verpflichtet werden, seine Fanpage abzuschalten, falls die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist.

Das Bundesverwaltungsgericht hatte diese Frage bereits im Jahr 2016 dem Europäischen Gerichtshof vorgelegt, der im Jahr 2018 entschieden hatte, dass der Betreiber einer Fanpage für die durch Facebook erfolgende Datenverarbeitung mitverantwortlich ist. Denn er ermöglicht durch den Betrieb der Fanpage Facebook den Zugriff auf die Daten der Fanpage-Besucher.[8]

In einem darauf erfolgten Beschluss vom 11. September 2019[9] hat das Bundesverwaltungsgericht nach mündlicher Verhandlung entschieden, dass eine Datenschutzbehörde den Betrieb einer Facebook-Fanpage untersagen kann. Die Datenschutzaufsicht kann sich danach bei der Auswahl unter mehreren datenschutzrechtlichen Verantwortlichen vom Gedanken der Effektivität leiten lassen. Da der EuGH festgestellt hatte, dass sowohl der Seitenbetreiber als auch Facebook gemeinsam verantwortlich sind, ist die Aufsicht nicht verpflichtet, zunächst gegen Facebook oder eine von deren Untergliederungen oder Niederlassungen vorzugehen. Dies auch deshalb, weil wegen der fehlenden Kooperationsbereitschaft von Facebook mit erheblichen tatsächlichen und rechtlichen Unsicherheiten zu rechnen ist.

8 Siehe 3. TB 2018 S. 44
9 BVerwG, Urteil vom 11. September 2019 - BVerwG 6 C 15.18

Die Einrichtungen, die eine Facebook Fanpage betreiben sind aufgefordert zu überprüfen, ob sie die Informationspflichten nach dem KDG im Hinblick auf die Fanpage gegenüber den betroffenen Personen erfüllen können. Unabhängig davon, ob der Besucher einer Fanpage selber bei Facebook registriert ist, muss jeder in transparenter und verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und den Betreiber der Fanpage verarbeitet werden. Derzeit greift Facebook bei jedem Aufruf der Fanpage auf personenbezogene Daten der Nutzer zu, ohne dass diese darüber unterrichtet werden. Die Einrichtungen, die eine Fanpage unterhalten, müssen dafür sorgen, dass sie von Facebook die Informationen zur Verfügung gestellt bekommen, die sie zur Erfüllung ihrer Informationspflichten benötigen. Weiterhin müssen die Betreiber eine Vereinbarung gem. § 28 KDG mit Facebook abschließen.

Um zu überprüfen, welche Einrichtungen den Anforderungen gerecht werden, werden die Datenschutzaufsichten einen Fragebogen an die Betreiber der Fanpages versenden. Es ist davon auszugehen, dass ein großer Teil der Einrichtungen die geforderten Informationen nicht zur Verfügung stellen kann. Deshalb wird seitens der Datenschutzaufsichten bereits jetzt geraten, die Fanpage zu deaktivieren.

4 Datenschutz in Kindergärten

Kindertageseinrichtungen im kirchlichen Bereich, die sich in Trägerschaft von Pfarreien oder Caritasverbänden befinden oder auch selbstständig sind, unterliegen ebenso dem KDG. Aber auch wenn diese Einrichtungen nicht dem KDG unterliegen, würden diese zumindestens in den Bereich der DS-GVO fallen, was im Hinblick auf die einzuhaltenden Datenschutz-Vorschriften kaum einen Unterschied machen würde.

In Kindertagesstätten werden personenbezogene Daten u.a. der Kinder, Eltern bzw. Sorgeberechtigten und Beschäftigten verarbeitet. Diese stellen somit den Kreis der Betroffenen dar.

Weiterhin ist bei Bildungseinrichtungen zu beachten, dass auch wertende Aussagen (z.B. Schulfähigkeit, Videoaufzeichnungen) und Beobachtungen,

die von Erziehern in Berichten festgehalten werden, personenbezogene Daten sind.

4.1 Kinder

Die wichtigste Betroffenengruppe, deren Persönlichkeitsrechte es durch die Vorschriften des Datenschutzes zu schützen gilt, sind in Kindertagesstätten die Kinder.

Kinder sollten einen besonderen Schutz ihrer personenbezogenen Daten genießen, da sie die Risiken und Folgen einer Verarbeitung ihrer personenbezogenen Daten überhaupt noch nicht abschätzen können[10].

Folgende personenbezogene Daten werden üblicherweise in Betreuungseinrichtungen verarbeitet:

- Name, Vorname
- Geburtsdatum
- Besondere Kategorien personenbezogener Daten wie Gesundheitsdaten (Impfstatus, Allergien, Behinderungen)
- Fotos

Die Angaben zum Namen und dem Geburtsdatum erfüllen den Zweck einer ordnungsgemäßen Betreuung des Kindes. Das Kind muss während der Betreuungszeit durch die Erzieher mit Namen angesprochen werden können. Zudem ist das Alter des Kindes wichtig, um dieses pädagogisch entsprechend zu betreuen und zu fördern.

Die gesundheitlichen Angaben dienen dazu, lebenswichtige Interessen des Kindes zu schützen. So muss den Erziehern zum Beispiel bekannt sein, dass ein Kind eine Nahrungsmittelunverträglichkeit hat oder wichtige Medikamente verabreicht bekommen muss. Auch Behinderungen wie z.B. Sehschwächen oder eingeschränktes Hörvermögen müssen gegenüber den Erziehern bekannt sein, damit diese in der Betreuung und in den pädagogischen Angeboten berücksichtigt werden können. Weiterhin können Be-

10 Erwägungsgrund 38, DS-GVO

hinderungen auch einen erhöhten Personalschlüssel fordern, welcher dann vom Träger bedacht werden muss.

Diese sensiblen Informationen eines oder mehrerer Kinder sollten nur einem beschränkten Personenkreis zugänglich sein. So muss beispielsweise der Essensversorger wissen, dass es eine bestimmte Anzahl von Kindern mit einer Fruktose Intoleranz gibt, aber nicht welche Kinder es sind.

Auch Fotoaufnahmen sind personenbezogene Daten bzw. Sozialdaten der Kinder. Für die Betreuung der Kinder sind Fotos nicht erforderlich. Sie können jedoch in der Bildungs- und Entwicklungsdokumentation Aussagen unterstreichen oder anschaulich darstellen.

In Punkt 4.4 wird nochmals detailliert auf das Thema Fotos in Kindertagesstätten eingegangen.

4.2 Eltern und Sorgeberechtigte

Neben den Daten von den Kindern, werden folgende Daten von den Eltern bzw. Sorgeberechtigten u.a. erfasst:

- Name, Vorname
- Anschrift
- Kontaktdaten (Telefon)
- Kontoinformation

Bis auf die Kontaktdaten sind die oben genannten Angaben zur Anbahnung und Abschluss des Betreuungsvertrages notwendig. § 6 Abs. (1) lit. d) KDG erlaubt diese Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung.

Bei der Angabe der Kontaktdaten sollte in der Regel eine Telefonnummer ausreichen, um die Sorgeberechtigten im Notfall zu verständigen.

Angaben zu Beschäftigungsverhältnissen, Staatsangehörigkeit oder Geburtsdatum der Eltern sind dagegen nicht erforderlich, werden aber immer noch häufig in den Aufnahmebögen der Kinderbetreuungseinrichtungen abgefragt.

Die Angabe der Konfession kann bei einem festgelegten pädagogischen Konzept erforderlich sein. Ist dagegen die Angabe der Konfession der Eltern für die Aufnahme des Kindes nicht entscheidend, so ist auch diese Abfrage zu unterlassen.

4.3 Beschäftigte

Die Haupt- und ehrenamtlichen Mitarbeiter in den Bildungseinrichtungen müssen zum einen die Datenschutz-Vorschriften einhalten, zum anderen schützt das KDG aber auch ihre Persönlichkeitsrechte.

Im Arbeits- und Privatleben der Kita-Erzieher ist wie auch in anderen beruflichen Feldern eine deutliche Zunahme von Entgrenzung zu beobachten. So ist es selbstverständlich, dass sich die Mitarbeiter am Wochenende fortbilden, am Nachmittag Kitafeste gestalten und am Abend Elternabende ausrichten oder Elterngespräche führen. Teilweise zählen diese aufgebrachten Zeiten noch nicht mal als Arbeitszeit, sondern gelten als ehrenamtliches Engagement.

All dieses stellt einen Übergriff des Arbeitgebers in die Privatsphäre oder das Persönlichkeitsrechts der Mitarbeiter dar, die es nach § 1 KDG zu schützen gilt.

Welche Angaben von Beschäftigten sind denn nun erforderlich und müssen dem Dienstgeber mitgeteilt werden?

Die Bekanntgabe des Namens, der Anschrift und des Geburtsdatums sind zur Erfüllung des Arbeitsvertrages notwendig. Darüber hinaus ist auch die Bekanntgabe der Kontoinformation notwendig, da die Gehälter üblicherweise bargeldlos gezahlt werden. Gleiches kann auch für die Zahlung von Aufwandsentschädigungen für Ehrenamtliche gelten. Darüber hinaus kann es auch notwendig sein, dass gesundheitliche Angaben z.B. zum Impfstatus gemacht werden müssen, da eine Kindertagesstätte sicherstellen muss, dass die Erzieher keine ansteckenden Krankheiten haben.

Dagegen ist es nicht erforderlich, dass der Dienstgeber private Telefonnummern und E-Mailadressen der Mitarbeiter benötigt. Es besteht dadurch die Gefahr, dass Frei- und Ruhezeiten durch die Erreichbarkeit des Mit-

arbeiters verletzt werden[11]. Bereitschaftsdienste können über ein Bereitschaftshandy abgedeckt werden. Dieses ist vom Dienstgeber zur Verfügung zu stellen. Zudem sind die Bereitschaftszeiten zu entgelten.

4.4 Fotos in Kindertagesstätten

Gut eineinhalb Jahre nach Einführung des KDGs und der DS-GVO gibt es immer noch Unklarheiten wie mit dem Anfertigen und Veröffentlichen von Fotos in Kindertageseinrichtungen umzugehen ist oder was eine Einverständniserklärung für das Anfertigen von Fotos beinhalten muss. Oft wird die Meinung vertreten, dass der Datenschutz bzw. das KDG das Anfertigen und Nutzen jeglicher Fotos verbiete.

Aus dem am 04.04.2019 gefassten Beschluss der Konferenz der Diözesandatenschutzbeauftragten geht eindeutig hervor, dass für die Veröffentlichung von Bildern von Kindern und Jugendlichen als einer Form der Verarbeitung entweder eine Einwilligung oder ein berechtigtes Interesse nach § 6 Abs. 1 lit. g) KDG vorliegen muss.

Das berechtigte Interesse als Erlaubnis der Verarbeitung von Fotos von Kindern kann aber nur zum Tragen kommen, wenn die Interessen oder Grundrechte und Grundfreiheiten der Kinder, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Demgemäß dürfte die Anwendung des berechtigten Interesses in einer Bildungseinrichtung oder Kindertagesstätte kaum möglich sein, da es Aufgabe dieser Einrichtungen ist die Grundrechte und Grundfreiheiten der Kinder zu schützen und Bildung zu vermitteln bzw. Betreuung zu leisten. Daher bleibt nur die Einwilligung nach § 8 KDG um das Erstellen, Speichern und Veröffentlichen von Fotos der Kita-Kinder zu legimitieren.

4.4.1 Einwilligungserklärung

Die Einwilligungserklärung für Fotos in Kindertagesstätten muss dabei folgende Grundsätze einhalten:

- Freiwillig

11 DANA 4/2019 – S. 180 – 184 „Datenschutz im Kindergarten“, Susanne Holzgraefe

- Informiert
- Zweckbestimmung
- Widerrufsmöglichkeit
- Schriftlich

In der Einwilligungserklärung ist zu beschreiben warum im allgemeinen Fotos in der Einrichtung und Aufnahmen von dem Kind gemacht werden sollen.
Diese Zwecke müssen genau beschrieben werden und können wie in dem nachfolgenden Beispiel sehr umfangreich sein:

( ) für die Entwicklungsdokumentation / Portfolio des eigenen Kindes

( ) für die Entwicklungsdokumentation / Portfolio eines anderen Kindes

( ) innerhalb der Kindertagesstätte für Einblicke in den Kita-Alltag (digitalen Bilderrahmen)

( ) in Schaukästen / Infowänden im Kitabereich

( ) auf der Homepage der Kita....

( ) in (Print-)Publikationen (Flyer) des Fördervereins

( ) in regionalen Presseerzeugnissen (z.B. Tagesblatt sowie deren Internetbeiträgen)

Weiterhin muss für die Erziehungsberechtigten erkennbar sein, dass sie die einzelnen Zwecke selbst auswählen dürfen, z.B. durch ankreuzen oder einer ja/nein-Auswahl.

Können Fotos der Kinder durch die Auswahl der Zweckbestimmung auch im Internet veröffentlicht werden, so muss die Information erfolgen, dass Fotos im Internet weltweit von beliebigen Personen abgerufen werden können und es trotz aller technischen Vorkehrungen nicht ausgeschlossen werden kann, dass die Fotos weiterverwendet werden.

In einfacher und verständlicher Sprache ist darzustellen, dass die Einwilligungserklärung freiwillig ist und gegenüber der Kindertagesstätte jederzeit mit Wirkung für die Zukunft widerrufen werden kann. Der Widerruf darf keine negativen Auswirkungen haben.

Weiterhin ist eine solche Fotoerlaubnis mindestens einmal im Jahr zu erneuern, da sich Sorgerechtskonstellationen ändern können, aber auch Auffassungen der Eltern zum Anfertigen und Veröffentlichen von Fotos des eigenen Kindes. Der Widerruf muss nicht begründet werden.

Unabhängig davon, ob eine gültige Einwilligungserklärung der Erziehungsberechtigten vorliegt, die das Fotografieren des Kindes erlaubt, sollte auch das Recht des Kindes beachtet werden. Macht ein Kind durch Gesten und Mimik oder Worte deutlich, dass es nicht fotografiert werden möchte, so ist dieses zu respektieren. Das Kind wird nicht fotografiert!

4.4.2 Fotos auf Kindergartenfesten

Im Kindergartenalltag gibt es immer wieder Feste und Veranstaltungen, die zum Teil auch öffentlich sind, wie beispielsweise ein Sommerfest oder der Tag der offenen Tür. Zu diesen Festen wird oft auch ein Programm der Kinder aufgeführt und es gibt neben den Eltern auch Verwandte und Freunde, die die Einrichtung dann aufsuchen. Daneben kann auch die Presse anwesend sein.

Bei solchen Festen kann das Fotografieren der eigenen Kinder erlaubt werden. Dies ist jedoch nur schwer einzuhalten bzw. zu kontrollieren, da bei Programmaufführungen immer mehr Kinder auf dem Bild sein können.

Auch kann erlaubt werden nur für private Zwecke Fotografien anzufertigen. Dies ist aber von dem Verantwortlichen, in der Regel die Einrichtungsleitung, nur schwer zu kontrollieren. So werden die Bilder meist recht schnell in das Facebook Profil hochgeladen oder über WhatsApp verschickt. Beides entspricht einer Veröffentlichung und ist damit verboten. Auch erlauben sich viele Handy Apps Zugriff auf die Bilder.

Da die Einrichtungsleitung die oben genannten Erlaubnisse nur schwer kontrollieren kann, empfiehlt es sich das Fotografieren im Kindergarten und dem Gelände komplett zu untersagen. Sollen doch Bilder gemacht werden, so können z.B. ein professioneller Fotograf oder ein Kindergartenmitarbeiter damit beauftragt werden. Dieses muss dann am Eingang durch Aushänge und durch eine Ansage zur Begrüßung mitgeteilt werden. Zudem muss es die Möglichkeit geben, Kinder und Erwachsene, die nicht

fotografiert werden sollen, einfach und nicht stigmatisierend zu kennzeichnen. Dies kann durch Buttons oder kindgerechte Sticker (z.B. Smileys) geschehen. Das Tragen von Leibchen oder Westen ist dagegen zu markant und sollte unterbleiben.

4.4.3 Fotos innerhalb der Einrichtung

Zunehmend ist festzustellen, dass Garderoben in den Kindertagestätten nicht mehr mit Symbolen wie Ball, Gießkanne oder Blume versehen werden, sondern mit dem Foto der Kinder. Zudem gibt es Monitore oder digitale Bilderrahmen, die anhand von Fotos einen Einblick in den Kita-Alltag geben. Grundsätzlich spricht nichts dagegen, da es sich bei einer Kindertagestätte um einen Nicht-Öffentlichen Raum handelt, der nur von einem begrenzten Publikum (Eltern, Abholende, Großeltern etc.) betreten wird.

Trotzdem sollte das Zeigen dieser Fotos in der Einwilligungserklärung inkludiert werden. Wichtig ist auch, dass jegliches Abfotografieren dieser Fotos sowie das Fotografieren insgesamt in der Betreuungseinrichtung untersagt werden.

4.4.4 Fotos in Portfolios / Entwicklungsdokumentationen

Das Anlegen und Führen von Entwicklungsdokumentationen oder Portfolios gehört in den meisten Kindertagesstätten zur fachlichen Arbeit. Sie dienen u.a. als Nachweis der Aufgabenerfüllung und spiegeln den Entwicklungsstand des Kindes wieder. Fotos können dabei helfen einen Sachverhalt besser darzustellen. Voraussetzung für das Verarbeiten von Bildern im Portfolio ist natürlich eine gültige Einwilligungserklärung.

Sollte eine Bedingung nach § 6 Abs. (1) lit. a) KDG in den Kinderförderungsgesetzen vorliegen, die die Dokumentation ausdrücklich anhand von Fotos vorsieht, so bedürfte es keiner Einwilligung durch die Sorgeberechtigten.

Neben Fotos sind in den Portfolios auch andere personenbezogene Daten eines Kindes enthalten. Angaben vom Kind selbst und den Sorgeberechtigten zu Familie, Hobbies, Lieblingsessen, Freizeitgestalten etc. lassen

schnell wertende Aussagen über die Lebensumstände zu. Weiterhin ist ein Kind durch diese zusätzlichen Angaben leichter zu identifizieren.

Daher sollten die Portfolios nicht frei im Gruppenraum herumstehen und für andere einsehbar sein.

Nach Beendigung der Kindergartenzeit sind die angelegten Portfolios den Eltern zu übergeben. Einen Zweck zur Aufbewahrung in den Einrichtungen gibt es nicht.

4.4.5 Fazit / Empfehlungen

Fotos, die in der Kindertagesstätte durch die Einrichtung angefertigt werden z.B. für das Portfolio oder als Erinnerung, sollten unmittelbar danach ausgedruckt und auf dem Speicherchip gelöscht werden. Sollen die Bilder der Kinder auf dem PC oder Laptop gespeichert werden, um diese dann für einen späteren Zweck zu nutzen oder an einen Fotoentwickler zu übersenden, so müssen diese während dieser Zeit angemessen gesichert werden.

Beim Versenden dieser Bilder an einen Fotoentwickler ist zu beachten, dass dies nur über eine gesicherte Verbindung geschieht. Weiterhin muss geprüft werden, ob es sich nicht um eine Auftragsverarbeitung nach § 29 KDG handelt, für welche dann ein entsprechender Vertrag abzuschließen wäre.

Zudem sind für jedes Anfertigen von Fotos, unabhängig von dem Zweck, Löschfristen festzulegen. Spätestens nach Beendigung der Kindergartenzeit sind Garderobenbilder oder Bilder, die für die Identifizierung des Kindes notwendig sind, zu löschen. Fotos für das Portfolio können direkt nach dem Entwickeln gelöscht werden, weil es keinen Zweck mehr gibt diese aufzubewahren. Auch für Fotos von Veranstaltungen und Festen der Einrichtung sollten angemessene Löschfristen festgelegt sein.

Der betriebliche Datenschutzbeauftragte einer Kindertagesstätte bzw. der Verantwortliche selbst sollte die Einhaltung der Löschfristen regelmäßig kontrollieren, da dieses im Alltag der Einrichtung oft vernachlässigt wird.

Ferner ist es auch ratsam das Fotografieren durch Eltern, Sorgeberechtigte oder Abholende Personen in der Einrichtung bzw. auf dem Grundstück der Einrichtung zu verbieten. Dieses Verbot kann über die Hausordnung für alle

festgeschrieben werden, so dass die Einrichtung bei Nicht-Beachtung auch von dem Hausrecht mit dem Vollzug von Konsequenzen Gebrauch machen kann.

Im wiederholten Fall kann das auch die Kündigung des Betreuungsvertrages bedeuten.

4.5 Datenschutzvorfälle im Kindergarten

Auch in Bildungseinrichtungen und Kindertagesstätten kommt es zu Datenschutzvorfällen.

So kam es in einer Einrichtung zum Einbruch. Dabei wurde ein Aktenschrank aufgebrochen, indem die Personalakten der Mitarbeiter waren. Weiterhin standen die Notfallkontakte (Telefonnummern) der Kinder offen in einem Regal. Zudem war der PC noch eingeschaltet und nicht durch eine Bildschirmsperre geschützt. Ein Protokoll der letzten Dienstbesprechung war noch geöffnet.

Dadurch können personenbezogene Daten der Kinder und Mitarbeiter, unter Umständen auch besondere Kategorien personenbezogener Daten, in unbefugte Hände gelangen.

Sicherlich können sich derartige Vorfälle immer wieder ereignen und vor einem Einbruch lässt es sich auch nur schwer schützen. Trotzdem hätte man in diesem Fall durch geeignete technische oder organisatorische Maßnahmen das Risiko für die Verletzung von Rechten und Freiheiten natürlicher Personen deutlich reduzieren können.

In einem weiteren Fall wurden bei einem Einbruch ein Laptop, Fotoapparate und eine externe Festplatte gestohlen. Zum Zeitpunkt des Diebstahls befanden sich noch Fotos von den Kindern auf den Fotoapparaten. Der Speicher bzw. die Speicherkarte von Fotoapparaten oder Digitalkameras sind zudem selten verschlüsselt oder durch eine andere Sperre geschützt, so dass die Bilder der Kinder leicht zur Verfügung stehen

Hier hätte das Risiko hauptsächlich dadurch minimiert werden können, indem erst gar keine Fotos von den Kindern in der Kindertagesstätte ge-

macht worden wären bzw. indem man die Fotos nach dem Anfertigen gleich ausgedruckt hätte.

Anhand dieser Datenschutzvorfälle sieht man, dass Fotos als personenbezogene Daten doch recht schnell verloren gehen oder in unbefugte Hände gelangen können.

Da es sich zudem um Fotos von Minderjährigen also Schutzbefohlenen handelt, sollten vom Verantwortlichen ausreichende Technische und Organisatorische Maßnahmen getroffen werden, um zum einen die Eintrittswahrscheinlichkeit und zum anderen die Schwere des Risikos beim Verlust von Fotos zu reduzieren.

5 Datenschutz in Schulen

5.1 I-Pad-Klassen

Es gab im Berichtszeitraum verschiedentlich Anfragen zur Verwendung von Microsoft Office 365. Konkret wurde die Frage nach der Zulässigkeit dieser Cloud-Anwendung in den Schulen eines Bistums gestellt.

Das Thema ist derzeit hoch umstritten und eine einheitliche Stellungnahme der Datenschutzaufsichten liegt noch nicht vor.

Zunächst gab es diesbezüglich eine Stellungnahme des hessischen Datenschutzbeauftragten vom 09.07.2019, der Cloud-Lösungen wegen der Intransparenz in Abweichung seiner früheren Beurteilung für unzulässig erachtet. Im Wesentlichen geht es bei der Ablehnung um eine Fülle von Telemetriedaten die an den Anbieter übertragen werden. Die Inhalte dieser Daten werden von den Unternehmen nicht bzw. nicht hinreichend erläutert. So besteht die Gefahr, dass Persönlichkeitsprofile der Nutzer erstellt werden, weil nicht geklärt ist, welche personenbezogenen oder personenbeziehbaren Daten das Gerät über das Internet verlassen. In einer weiteren Stellungnahme der selben Aufsicht vom 02.08.2019 wurde die Aussage vom Juli zwar etwas relativiert, aber dennoch nicht von einer Unbedenklichkeit gesprochen. Bereits hieran ist erkennbar, wie schwierig eine Einschätzung ist.

Die Datenschutzaufsichtsbehörden der Länder, der sich auch die Konferenz der Diözesandatenschutzbeauftragten angeschlossen hatte, hat mehrfach zum Ausdruck gebracht, dass gegen eine Anwendung dieser Dienste derzeit keine aufsichtlichen Unterlassungsverfügungen möglich sind. Dies hängt aber maßgeblich damit zusammen, dass die diesbezüglichen Überprüfungen komplex sind und die Anbieter sich einer konstruktiven Zusammenarbeit verweigern. Die Aufsichten sind sich darüber einig, dass eine Anerkennung als datenschutzrechtlich unbedenklich einer Zertifizierung eines Dienstes gleichkäme. Aus diesem Grunde wird eine solche Erklärung jeder einzelnen Behörde im Alleingang unterbleiben.

Für die Anwender bedeutet dies konkret, dass sie bei der Einführung von I-Pad-Klassen derzeit zwar nicht damit rechnen müssen, eine entsprechende Unterlassungsaufforderung durch die Aufsicht zu erhalten. Diese Aussage steht aber unter dem Vorbehalt weiterer Prüfungen. Die Verwender gehen mit der Anschaffung bzw. Installation der benannten Technik das Risiko ein, bei Vorliegen neuer Erkenntnisse die Cloud-Lösungen nicht mehr verwenden zu dürfen. Ob sich vor diesem Hintergrund die anstehenden Investitionen lohnen muss jeder Verantwortliche für sich entscheiden

Dabei ist auch zu berücksichtigen, dass die Daten aus Microsoft-Office 365 bei Microsoft gehostet werden, also in den USA. Microsoft hat sich nach den Regeln des „EU-U.S. Privacy-Shield“ selbst auditiert und in die Privacy-Shield-Liste eintragen lassen. Damit ist zunächst die Zulässigkeit einer Verarbeitung außerhalb der EU in den USA zulässig. Dieses Abkommen gerät aber zunehmend in die Kritik und es erscheint nicht ausgeschlossen, dass es das gleiche Schicksal erleiden wird, wie die Vorgängerregelung „Save Harbour“. Damit wäre eine Nutzung bereits aus diesem Grund obsolet.

6 Datenschutz im Personalbereich

6.1 Inhalt der Personalakte

Eine Petentin forderte gegenüber ihrem Dienstgeber Einsicht in die Personalakte. Dieses Recht steht Mitarbeitenden gem. § 3 Abs. 5 DVO; § 6 AVR zu. Die Einsicht wurde ihr auch gewährt. Die Petentin fragt aber nunmehr

bei unserer Dienststelle an, welche personenbezogenen Daten in der Personalakte abgelegt werden dürfen, insbesondere ob auch Arbeitsunfähigkeitsbescheinigungen sowie „Kind-krank-Bescheinigungen“ darin enthalten sein dürfen.

Regelmäßig werden die Bewerbungsunterlagen des eingestellten Bewerbers in die Personalakte übernommen. Dieses Verfahren steht häufig nicht mit den datenschutzrechtlichen Forderungen in Einklang. Es ist immer zu fragen, ob die eingereichten Unterlagen für die Durchführung des Arbeitsverhältnisses konkret erforderlich sind. Dieser Zweckbindungsgrundsatz wird durch die Forderung nach Datensparsamkeit ergänzt. Danach ist die Verarbeitung (also die Speicherung) auf das notwendige Maß zu beschränken. Daraus ergibt sich die Verpflichtung des Arbeitgebers, vor Übernahme der Bewerbungsunterlagen in die Personalakte zu prüfen, welche Unterlagen für das Arbeitsverhältnis erforderlich sind. Beurteilungen früherer Arbeitgeber sind ebenso wenig in die Personalakte aufzunehmen, wie ggf. vorgelegte Führungszeugnisse oder das Abiturzeugnis.

6.1.1 Zweck von Personalakten

Zweck von Personalakten ist es nicht, Vorgesetzten eine Grundlage für eine Laudatio zum Betriebsjubiläum zu geben oder Stoff für die Abschiedsrede beim Ausscheiden aus dem Unternehmen zu liefern. Das Einsichtsrecht hat sich auf einen möglichst kleinen Kreis zu beschränken. Dabei ist in einem Verfahrensverzeichnis festzulegen, wer berechtigt ist, Einsicht zu nehmen. Da Personalakten in der Regel aus mehreren Teilen bestehen, ist ggf. festzulegen für welche Aktenteile wem ein Einsichtsrecht zu gewähren ist. Dabei ist das Einsichtsrecht strikt an die Aufgabe zu binden. Nur wer zur Erfüllung seiner dienstvertraglichen Verpflichtungen zwingend in die Personalakte einsehen muss, bekommt ein solches Einsichtsrecht übertragen (z. B. Gehaltsabrechnung). Unsachgemäß ist die Vergabe eines Einsichtsrechts aufgrund der Funktion. So hat auch ein Abteilungsleiter nicht per se das Recht, in die Personalakten seiner Mitarbeiter/innen Einsicht zu nehmen.

6.1.2 AU-Bescheinigungen in Personalakten

Arbeitsunfähigkeitsbescheinigungen (AU-Bescheinigungen) enthalten personenbezogene Daten besonderer Kategorie. Aus ihnen gehen neben dem Namen des/der Mitarbeiters/in auch die Krankenkasse, die Versicherungsnummer, der behandelnde Arzt u.a. hervor. Diese Bescheinigungen sind deshalb mindestens so in die Personalakte aufzunehmen, dass eine auch zufällige oder ungewollte Wahrnehmung nicht erfolgen kann, also z.B. in einem verschlossenen Umschlag. Besser ist eine separate Aufbewahrung an anderer Stelle. Auf jeden Fall muss in einem Löschungskonzept geregelt sein, nach welcher Frist diese Bescheinigungen aus der Personalakte zu entfernen sind. Die AU-Bescheinigungen werden gem. der Regelung zum Betrieblichen Eingliederungsmanagement gem. 167 SGB IX zumindest ein Jahr und höchstens drei Jahre aufzubewahren sein. Danach sind sie datenschutzkonform zu vernichten.

„Kind-krank-Bescheinigungen", die der/die Mitarbeiter/in gem. § 45 Abs. 3 SGB V vorlegt, sind nach Ablauf des Kalenderjahres aus der Personalakte zu entfernen, da sich der Anspruch des Elternteils jeweils auf ein Kalenderjahr bezieht.

6.1.3 Aufbewahrung

Akten mit personenbezogenen Daten, zu denen Personalakten unzweifelhaft gehören, sind durch besondere Sicherungsmaßnahmen, die in den „Technisch organisatorischen Maßnahmen" zu beschreiben sind, in erforderlichem Umfang zu schützen. Personalakten, auch solche ausgeschiedener Mitarbeiter/innen, sind in verschlossenen Schränken aufzubewahren. Dies gilt auch dann, wenn das Büro in dem die Akten lagern, stets verschlossen gehalten und nur von autorisierten Mitarbeitenden betreten wird, aber Dritte, wie z. B. das Reinigungspersonal, Zugang zu diesem Büro haben. Finanzielle Mängel, bzw. die Nichteinstellung entsprechender Mittel im Etat der Einrichtung sind nicht geeignet, den Verstoß zu rechtfertigen. Der ungehinderte Zutritt bzw. Zugang Dritter zu personenbezogenen Daten ist auszuschließen.

6.1.4 Aufbewahrung von Personalunterlagen nach Ausscheiden der/des Mitarbeiters/in

§ 19 Abs. 1 lit. a) KDG gibt Betroffenen das Recht vom Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, wenn die personenbezogenen Daten für die Zwecke für die sie erhoben oder in sonstiger Weise verarbeitet worden sind, nicht mehr notwendig sind. Im Falle der Personalakten sind Betroffene die Beschäftigten gem. § 4 Nr. 24 KDG. Also neben den in einem Beschäftigungsverhältnis stehenden Personen, Nr. 24 c) auch Bewerbende und ehemalige Beschäftigte, Nr. 24 i). Nach Beendigung des Beschäftigungsverhältnisses dürften für den Arbeitgeber die meisten Unterlagen in der Personalakte keine Relevanz mehr besitzen. Dies betrifft insbesondere Zwischenzeugnisse, Abmahnungen[12] aber auch Qualifizierungsnachweise u. ä. Es ist hierbei nicht erforderlich, dass sich aus den Unterlagen in der Personalakte negative Gesichtspunkte für Mitarbeitende ergeben können. Der Entfernungsanspruch des ausgeschiedenen Mitarbeiters besteht allein auf datenschutzrechtlicher Grundlage.[13] Es ist Arbeitgebern anzuraten, die Personalakte bei Ausscheiden von Mitarbeitenden zu überprüfen und die Unterlagen, die -z. B. aus steuerlichen oder sozialversicherungsrechtlichen Gründen- nicht mehr benötigt werden dem/der Mitarbeiter/in auszuhändigen oder ordnungsgemäß zu vernichten. Um der Regelung des § 14 Abs. 2 TzBfG gerecht zu werden, sind Vorbeschäftigungszeiten zumindest nach Art, Umfang und Dauer festzuhalten. Da nach der Rechtsprechung des Bundesverfassungsgerichts[14] eine Karenzzeit in diese Vorschrift nicht gegen den Gesetzeswortlaut hineingelesen werden darf, sind diese Daten 30 Jahre aufzubewahren.[15]

6.2 Erhebung von Personaldaten bei Einstellung

Im Hinblick auf eine datenschutzkonforme Verarbeitung von Personaldaten in den kirchlichen Einrichtungen der ostdeutschen Bistümer gab es im Berichtszeitraum einen Dialog, an dem zum einen Personalverantwortliche

12 LAG Sachsen-Anhalt 23.11.2018 - 5 Sa 7/17
13 Möllenkamp NZA-RR 2019, 355
14 Bundesverfassungsgericht Urteil vom 06.06.2018 BvL 7/14, 1 BvL 7/14, 1 BvR 1375/14
15 Nach Urteil des BAG vom 23.1.2019 - 7 AZR 733/16 ist auch eine achtjährige Karenzzeit nicht ausreichend.

aus den Bistümern und die Kirchliche Datenschutzaufsicht teilgenommen haben.

Ziel dieses Dialoges war die Entwicklung eines einheitlichen Fragebogens für die Abfrage von Personaldaten bei Einstellung neuer Mitarbeiter zu entwickeln, Doppelabfragen zu vermeiden und benötigte Einzelangaben mit einer Grundlage zu hinterlegen, für welchen Zweck die Angabe benötigt wird.

6.2.1 Abfrage der Personaldaten bei den Bistümern

Als erster Schritt zur Entwicklung dieses Fragebogens wurden alle Personalverwaltungen bzw. Verantwortliche der ostdeutschen Bistümer angeschrieben mit der Bitte uns ihr derzeitig genutztes Formular zuzusenden. Daraufhin haben wir eine Fülle unterschiedlicher Fragebögen zurückbekommen. In einigen Bistümern werden unterschiedliche Fragebögen für Haupt- und Nebenbeschäftigungen bzw. geringfügige Beschäftigte verwendet, ferner gibt es noch Zusatzbögen für Priester bzw. geistliche Beschäftigte. Teilweise werden Lebensläufe aus der Bewerbung des Mitarbeiters direkt in die Personalakte übernommen.

Um die Entwicklung eines einheitlichen Fragebogens nicht ausufern zu lassen, haben wir uns entschieden den Fragebogen für hauptamtlich Beschäftigte (Voll- und Teilzeit), die nicht im priesterlichen Dienst stehen, zu beurteilen.

6.2.2 Feststellen der Datenschutzrechtlichen Fragwürdigkeit einzelner Angaben

Im zweiten Schritt wurden alle Angaben, die uns unter datenschutzrechtlichen Gesichtspunkten als fragwürdig erschienen bzw. für die es nach unserer Sicht keine Notwendigkeit oder gesetzliche Grundlage gibt, zusammengetragen und die entsprechenden Bistümer dazu befragt.

Beispiele:

In einem Bistum wurden folgende Angaben zum Ehepartner abgefragt:

- Name, Geburtsname, Vorname
- Geburtsort, Geburtsdatum
- Arbeitsstelle, Anschrift der Arbeitsstelle, ausgeübte Tätigkeit, Umfang der Beschäftigung

Angaben zum Ehepartner dürfen nicht erhoben werden, da es dafür keine Erforderlichkeit und keine Rechtsgrundlage gibt.

Folgende Angaben zur Schwerbehinderung müssen in einigen Bistümern gemacht werden:

- Vorliegen einer Schwerbehinderung
- Grad und Art der Behinderung

Angaben zur Schwerbehinderung sollten freiwillig sein, weil es sich um eine Bekanntgabe personenbezogener Daten besonderer Kategorie nach § 4 Nr. 2 KDG bzw. um Gesundheitsdaten nach § 4 Nr. 17 KDG handelt. Der Mitarbeiter darf selbst entscheiden, ob er diese Daten besonderer Kategorien preisgibt und die damit verbundenen Vorteile wie Zusatzurlaub oder Freistellungen in Anspruch nimmt oder ob er darauf zugunsten seines Persönlichkeitsrechts verzichtet[16].

In einem Bistum wurde nach dem Tag, dem Datum und dem Ort der kirchlichen Eheschließung gefragt.

Angaben zur kirchlichen Eheschließung sind nicht erforderlich, auch wenn die meisten Dienstvertragsordnungen bei Eheschließungen und Ehejubiläen Sonderurlaub vorsehen. Es ist ausreichend bei der Beantragung von Sonderurlaub für einen dieser Zwecke einen Nachweis vorzulegen. Dieses liegt dann aber in der freien Entscheidung des Mitarbeiters, diesen zu beantragen. Der Ort, wo die Eheschließung stattfand, ist ebenso unerheblich.

16 ZMV 5/2019 – S. 1-4, Offenbarungspflicht Schwerbehinderteneigenschaft und Persönlichkeitsrecht, Matthias Ullrich

Die Angaben zu weiteren Beschäftigungsverhältnissen mit Angabe des Arbeitgebers und der Anschrift des Arbeitgebers wurde auch von einigen Bistümern abgefragt.
Angaben zu einem weiteren Beschäftigungsverhältnis sind für die sozialversicherungsrechtliche Beurteilung der Arbeitsverhältnisse erlaubt. Zum einen richten sich die Höhe der Sozialabgaben immer nach dem Beschäftigungsverhältnis mit dem größten Beschäftigungsumfang. Zum anderen muss der Mitarbeiter auch seine Arbeitszeit sicherstellen können. So kann er z.B. nicht 2 Vollzeitbeschäftigungen gleichzeitig ausführen. Jedoch ist es nicht erforderlich, dass der Dienstgeber weiß, wo der Mitarbeiter noch beschäftigt ist.

Anhand dieser Beispiele ist schon ersichtlich, dass einige Angaben datenschutzrechtlich zweifelhaft sind. Weiterhin besteht auch Verunsicherung darüber welche Angaben zur Staatsangehörigkeit, Religion, Kindern und berufliche Werdegang bzw. Abschlüsse gemacht werden müssen.

6.2.3 Dialog zur Erarbeitung eines Standardformulars

Nachdem wir die Stellungnahmen unserer Fragen von den Bistümern zurückerhalten und zusammengetragen haben, wurde alle Personalverwaltungen zu einer gemeinsamen Diskussionsrunde eingeladen. In dieser Runde hat die kirchliche Datenschutzaufsicht die aus ihrer Sicht zweifelhaften Abfragen dargestellt und mit den Teilnehmern gemeinsam über dessen Notwendigkeit diskutiert.

Das Ergebnis war dahingehend interessant, dass vor allem die von den Personalern genutzten Meldeprogramme für die Sozialversicherungen und Steuern Angaben benötigen, die aus datenschutzrechtlicher Sicht nicht erfasst werden müssten bzw. deshalb mehrfach erfasst werden.

Weiterhin herrschte noch bei einigen Teilnehmern die Meinung, dass bestimmte Angaben für etwaige Sonderzahlungen aus dem alten Tarif- und Beamtenrecht notwendig sind. Diese Sonderzahlungen sind zum großen Teil abgeschafft und treffen auf Neueinstellungen meistens nicht mehr zu.

Weiterhin wurde diskutiert, warum es ausreichend ist nur bestimmte berufliche Stationen als Berufserfahrung in den Personalbogen aufzunehmen

und nicht einfach den beim Bewerbungsprozess eingereichten Lebenslauf als Bestandteil in die Personalakte zu nehmen.

Ein Lebenslauf enthält in der Regel den kompletten Bildungsweg und alle beruflichen Stationen, so dass Zeiten über Erwerbsunfähigkeit, Kindererziehung, Wehrdienst, Zivildienst etc. daraus hervorgehen können. Diese Angaben sind aber in der Regel für die auszuübende Tätigkeit oder der Eingruppierung in die Gehaltsklasse nicht relevant. Weiterhin werden in einem Lebenslauf meist möglichst viele Kontaktangaben gemacht, da man als Bewerber schnell erreicht werden möchte. Ein Teil dieser Angaben sind für den Arbeitgeber im laufenden Arbeitsverhältnis nicht mehr erforderlich.

Am Ende wurden die Teilnehmer auch darüber informiert, dass alle abgefragten Angaben und deren Zweck in den Informationspflichten nach §§ 15, 16 KDG enthalten sein müssen.

6.2.4 Ergebnis des Dialogs – Ausarbeitung des Standardformulars

Im Ergebnis des gemeinsamen Austauschs konnte ein Standardformular entworfen werden, welches zum einen den datenschutzrechtlichen Anforderungen entspricht und zum andern die sozialversicherungsrechtlichen Erfordernisse einhält.

Persönliche Daten

Familienname: _____ Vorname: _____

Geburtsname: _____ Staatsangehörigkeit: _____

Geburtsdatum: _____ Geburtsort: _____
(wenn Rentenversicherungsnummer unbekannt)

Anschrift: _____

_____

Konfession: _____ (1)

Sofern Sie nicht der römisch-katholischen Kirche angehören: (2)
Hiermit versichere ich, dass ich nie Mitglied der römisch-katholischen Kirche war und nicht aus dieser ausgetreten bin.

_____ _____
Ort, Datum Unterschrift

Familienstand: ☐ ledig ☐ verheiratet (3)

☐ getrennt lebend seit: _____ ☐ geschieden seit: _____ ☐ verwitwet seit: _____

Kontaktdaten:
(Die Kontaktdaten sind freiwillige Angaben und nicht zwingend erforderlich. Sie sind für einen schnelleren Kommunikationsweg vorteilhaft. Eine Weitergabe an Dritte erfolgt nicht bzw. nur mit Einwilligung.)

Telefon: _____ Mobil: _____

E-Mail:

Muster

Die Angabe, zu welcher Konfession ein Mitarbeiter gehört, darf weiterhin erfasst werden. Ferner muss der Mitarbeiter auch versichern, dass er nie aus der Katholischen Kirche ausgetreten ist. Bewusst ausgetretenen Mitarbeitern identifizieren sich nicht mehr mit den Grundwerten der Kirche. Dagegen kann sich ein konfessionsloser Mitarbeiter mit den Grundwerten der Kirche identifizieren bzw. diese anerkennen.

Bei bestimmten Angaben zum Familienstand (getrennt lebend, geschieden, verwitwet) ist es auch erlaubt zu fragen, ab wann dieser Zustand eingetreten ist. Grund dafür ist, dass sich Steuerklassen in den Übergangszeiten ändern können und dieses muss bei der Gehaltszahlung berücksichtigt werden.

Außer der Anschrift muss der Beschäftigte keine weiteren Kontaktdaten angeben. Es ist ausreichend, wenn er unter dieser postalisch zu erreichen ist. Trotzdem können weitere Angaben freiwillig gemacht werden, um Kommunikationswege abzukürzen.

Bei den Angaben zu Beruf und Bildung ist es ausreichend, wenn nur der höchste maßgebende Schulabschluss angegeben wird. Zudem müssen nur die Abschlüsse (z.B. Meister, Diplom, Staatsexamen) und Berufserfahrungen angegeben werden, die für die auszuübende Tätigkeit und die Eingruppierung relevant sind.

Einige Bistümer haben auch sehr umfangreiche Angaben zu Kindern der Beschäftigten abgefragt. So wurde beispielsweise neben dem Geburtsdatum auch die Konfession erfragt. Dagegen ist es hinreichend, wenn nur die Kinder angegeben werden, für die nach dem Bundeskindergeldgesetz Kindergeld oder eine vergleichbare Leistung gezahlt wird. Ferner dient diese Angabe zur Berechnung des Pflegeversicherungsbeitrag und Sonderzahlungen wie z.B. Kinderweihnachtsgeld. Dazu ist nur das Geburtsjahr der Kinder wichtig, da nur bei Volljährigen weitere Nachweise erbracht werden müssen.

Sollte jemand bereits eine Rente bekommen, so spielt der Betrag nur eine Rolle, wenn dadurch die Hinzuverdienstmöglichkeit überschritten wird, da dieses bei den Sozialabgaben berücksichtigt werden muss.

Für Arbeitnehmer, die nicht zur EU gehören, reicht es aus nach der Arbeitserlaubnis zu fragen. In der Regel setzt die Arbeitserlaubnis die Aufenthaltserlaubnis voraus.

Fazit:

Die Verarbeitungsgrundsätze nach § 7 KDG gilt es auch für die Erhebung von Personaldaten einzuhalten. In Personalakten sollten auch wirklich nur die erforderlichen Daten enthalten sein (Prinzip der Datensparsamkeit). Zudem sollten nicht mehr erforderliche Daten zum gegebenen Zeitpunkt gelöscht werden.

Weiterhin sind für Personaldaten, unabhängig ob Papierakten oder digitale Akten, geschützt aufzubewahren und mit einem Berechtigungskonzept zu versehen.

7 Technischer Datenschutz

7.1 Menschen schützen

Der Begriff „Datenschutz" ist bei vielen negativ konnotiert. Er steht dann für Arbeits- und Aufgabenbeeinträchtigung, keine Fotos mehr, WhatsApp im betrieblichen Einsatz verboten, Abmahnungen u.v.m.

Datenschutz hat aber keinen Selbstzweck. Geschützt werden sollen nicht in erster Linie Daten, sondern der Mensch, seine Persönlichkeitsrechte. Um diesen Schutz gewährleisten zu können, bedarf es auch technischer Maßnahmen.

7.1.1 Fallbeispiele und das Ausmaß

a) Ein Krankenhaus verschickt Befunde einer Person an einen falschen Empfänger (Patienten).

b) In einer Tageskindereinrichtung wird eingebrochen und es werden elektronische Geräte wie Digitalkamera, Smartphone, PC und Notebook gestohlen. Auf allen Geräten befinden sich Daten der Kinder, wie Fotos, Berichte über Verhaltensauffälligkeiten, Adress- und Kon-

taktdaten sowie Informationen welche Person zu welchem Zeitpunkt abholberechtigt ist. Ein Zugriffsschutz sowie eine Verschlüsselung der Datenträger waren nicht gegeben und ein Notfallkonzept war nicht verfügbar.

c) In einer Geschäftsstelle (Pfarrbüro) arbeiten haupt- und ehrenamtliche Personen welche Adressdaten von Kindern und Jugendlichen sowie erweiterte Adressdaten mit Bankverbindungen erfassen und aktualisieren und somit personenbezogen Daten verarbeiten. Häufig erledigen Mitarbeiter Aufgaben von zu Hause und verarbeiten Daten auf ihren privaten Endgeräten. Der Transfer der betrieblichen Daten zwischen dem Büro und dem „privaten Heimarbeitsplatz" erfolgt in der Praxis auf unterschiedlichstem Weg:

- Per USB-Stick (meist unverschlüsselt und überwiegend ein privater USB-Stick)
- Per E-Mail (zum Teil auf einen privaten kostenfreie E-Mail Account im Ausland)
- Per Cloud Dateitransfer (zum Teil über einen privaten kostenfreien Account und einen Cloud-Service im Ausland)
- Microsoft OneDrive aus Windows 10 Home Edition
- u.ä., dem Einfallsreichtum sind hier offenbar keine Grenze gesetzt

In so einer Home-Office-Umgebung sind betriebliche und private Daten auf einem privaten Endgerät vermischt. Zumal der Computer und oftmals auch der E-Mail Account mehreren Familienangehörigen zur Verfügung stehen. Bei dieser Konstellation kann es zu einem unkontrollierten Datenleck (Datenabfluss oder Bekanntgabe von Informationen an Dritte) betrieblicher personenbezogener Daten kommen. In den uns bisher bekannt gewordenen Fällen gab es keine Verschlüsselung der Datenträger sowie der Daten beim Datenaustausch. Eine verbindliche Richtlinie zum Löschen oder zur Übergabe betrieblichen Daten gab es nicht.

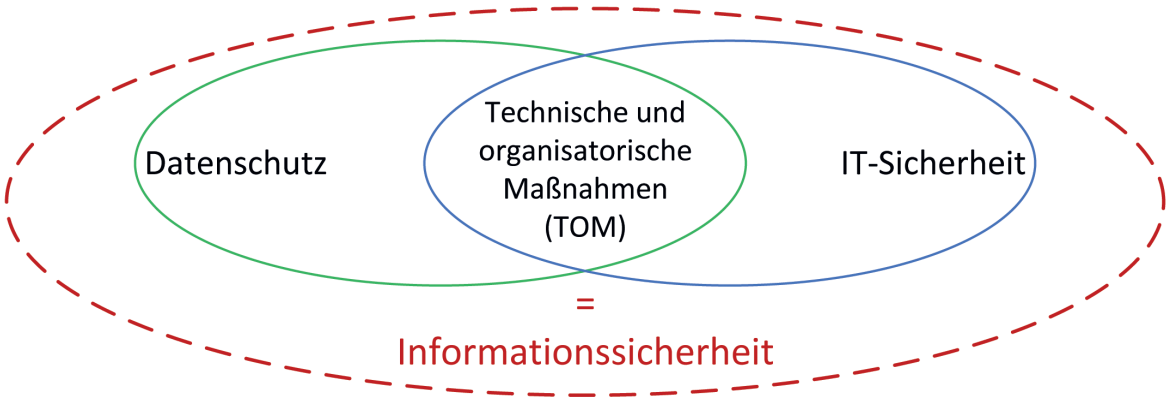
Die Fallbeispiele zeigen, dass personenbezogene Daten ohne Eigenverschulden und ohne Wissen der Betroffenen an Fremde (Datenabfluss an Dritte) gelangen können. Solche Daten können nicht nur für Marketing und

Werbung von großem Interesse sein, sondern auch für Straftaten wie Identitätsdiebstahl, CyberMobbing, telefonisches Social Engineering[17] (Enkeltrick) oder gezielte Einbrüche Verwendung finden.

Die Folgen sollten nicht unterschätzt werden! All diese Verletzungen können physische, materielle oder immaterielle Schäden für die betroffenen Personen nach sich ziehen. Desweiterem können persönliche Informationen über Jemanden für weitere gezielte Straftaten missbraucht werden.

7.2 Daten schützen

Um Daten schützen zu können bedarf es technischer und organisatorischer Maßnahmen. Die IT-Sicherheit ist dabei ein Baustein.



Der Begriff „Technischer Datenschutz“ findet zwar im KDG keinen Niederschlag, dennoch nehmen einige Vorschriften Bezug auf technische Standards und technisch organisatorische Maßnahmen. § 7 KDG Abs. 1: Personenbezogene Daten müssen in einer Weise verarbeitet werden,

- die eine angemessene Sicherheit gewährleistet,
- Schutz vor unbefugter oder unrechtmäßiger Verarbeitung bieten
- Schutz vor unbeabsichtigtem Verlust und unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung bieten

17 Beeinflussung mit Hilfe von Informationen über Jemanden, um ein Ziel zu erreichen

Nach § 26 KDG müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Aber auch die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) stellt wichtige Anforderungen an die IT-Systeme sowie an das Schutzniveau verschiedener Datenschutzklassen. Bereits ab einer Datenschutzklasse I müssen wichtige Kriterien für die IT-Sicherheit bei der Datenverarbeitung erfüllt werden. In den §§ 19-20 KDG-DVO wird u.a. die Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken sowie die Nutzung privater IT-Systeme zu dienstlichen geregelt. Besonders zu beachten sind in dem Zusammenhang die im § 20 Abs. 2 KDG-DVO erwähnte Kriterien zur Nutzung privater Systeme mit denen betrieblichen bzw. dienstliche Daten verarbeitet werden.

Strukturelle technisch- organisatorische Defizite werden soweit sie der Datenschutzaufsicht insbesondere im Bereich des Patientenmanagements bekannt werden deutliche Sanktionen nach sich ziehen. Gerade im Bereich des Gesundheitswesens wird die Datenschutzaufsicht eine besondere Wachsamkeit an den Tag legen.

Der technische Datenschutz wird häufig auch die Grundlagen liefern für das im Gesetz verankerte Recht auf Auskunft der betroffenen Person nach § 17 KDG[18]. Solange die „Datenstraßen" (Datenfluss-Wege) der Daten welche verarbeitet werden nicht bekannt und/oder klar geregelt sind, wird es schwierig einem Auskunftsanspruch gerecht zu werden.

7.3 IP-Telefonie und die Umstellung der Telefonanschlüsse auf das All-IP Netz

Die unausweichliche Umstellung der leitungsbasierten Telefonanschlüsse, wie der analoge Telefonanschluss oder der digitale ISDN Anschluss, ist weiterhin im vollen Gange. Auf Grund des doch erheblichen Aufwands ist eine Umstellung auf die neuen All-IP Anschlüsse noch nicht flächendenkend abgeschlossen.

18 Betroffenenrechte, KDG-Praxishilfe 6

Hier sollte man zwischen der IP-Telefonie welche die Festnetz-Telefonie ersetzt und anderen VoIP Diensten unterscheiden. Auch wenn die IP-Telefonie u.a. die Bezeichnung VoIP (Voice over Internet Protokoll) trägt, so ist sie nicht zu verwechseln mit der sonstigen Internet-Telefonie wie z.B. Skype, WhatsApp o.ä. Dienste, welche kein eigenes Infrastruktur-Netz betreiben und das Trägermedium dann das öffentliche Internet ist. Die Bezeichnung VoIP ist als Begriff für die Technologie Sprache über das Internet-Protokoll zu übertragen, zu sehen.

Die großen Telekommunikationsanbieter in Deutschland transportieren die Daten für Festnetz-Telefonate über ihr eigenes Infrastruktur-Netz (Routing innerhalb des eigenen IP-Backbone). Der Dienst „Telefon-Service" ist dabei von anderen Diensten wie z.B. einem Datendienst (typische Webdienste und E-Mail) logisch getrennt. Telefongespräche unter diesen Telekomunikations-Anbietern werden über deren eigen Infrastruktur-Netze geroutet (Routing innerhalb des eigenen IP-Backbone).

Anders verhält es sich jedoch, sobald die Telefongespräche die eigenen Netze der Telekommunikations-Anbieter verlassen müssen. Dann können unter Umständen die Datenpakete (Gespräche) über das öffentliche Internet zum angerufenen Partner gelangen. In diesem Fall hängt die Sicherheit der übertragenen VoIP Datenpakete von allen daran beteiligten Netzen ab.

7.3.1 Zur Frage der Sicherheit bei VoIP

Bei den leitungsbasierten Telefonanschlüssen gab es einen nicht vernachlässigbaren Vorteil gegenüber der neuen Technologie. Diese Anschlüsse wurden zentral mit Spannung versorgt. Die direkt am Telekom-Anschluss angesteckten Telefone waren somit auch bei einem Stromausfall betriebsbereit. Bei den Telefon-Anschlüssen konnte damit die Aufrechterhaltung der Telefonfunktion gewährleistet werden.

Das ist bei den neuen All-IP Anschlüssen nicht mehr vorgesehen. Im Gegenteil, damit ein Telefon angeschlossen werden kann, wird (je nach Anschlusstyp) ein VoIP fähiges Modem mit Router benötigt, welches ständig mit Strom versorgt werden muss.

Ein weiterer Vorteil der herkömmlichen Telefonanschlüsse war es, dass diese gegenüber Störeinflüssen wie sie bei Datenleitungen auftreten können relativ unempfindlicher waren. Damit sind die neuen All-IP Anschlüsse empfindlicher in Bezug auf eine Auslastung der Datenverbindungen.

Auf Arten der Bedrohung und Schwachstellen soll hier nicht weiter eingegangen werden, nur folgendes sei noch erwähnt. Sobald ein Angreifer physischen Zugang und Zugriff auf wichtige Infrastruktur-Endpunkte erhält, ist die Sicherheit unabhängig von der Technologie gefährdet. Bei der herkömmlichen analogen Telefonie konnte ohne größeren technischen Aufwand durch paralleles Aufschalten auf den Anschluss mitgehört werden. Bei den ISDN Anschlüssen musste dafür bereits mehr Aufwand investiert werden, wobei der Missbrauch (z.B. Daten über den D-Kanal senden) schon mehr Schadenspotential hatte. Bei den neuen IP-Netzen ist das schon komplizierter, weil u.a. die Daten als Datenpakete sich auf mehrere Protokollschichten verteilen. Das macht auch ein mitschneiden des VoIP Datenverkehr aufwendig und benötigt eine entsprechende technische Ausrüstung.

Aufgrund der neuen Technologien und der globalen Datennetze wird es immer wieder eine gewisse Unsicherheit geben, die es allerdings in der Vergangenheit auch immer wieder gab. Das liegt aber nicht an der Einführung von VoIP bzw. der IP-Telefonie. In Zeiten der Cyberangriffe (Cyber-Attacke) ist das Risiko durch Stören einer Funktion oder der Verfügbarkeit größer geworden. Als Beispiel sei hier der Denial-of-Service Angriff (DoS) erwähnt. Ein Ziel dabei ist es, einen Dienst bzw. einen verfügbaren Service so zu stören (durch überlasten), dass dieser in seiner Verfügbarkeit stark eingeschränkt wird – bis hin zur Nichtverfügbarkeit.

Durch entsprechende technische und organisatorische Maßnahme ist zu gewährleisten, dass Angriffspunkte für Bedrohungen minimiert werden.

7.4 Das Telefax im IP-Netz

Früher noch als Fernkopieren bezeichnet hat sich seit ca. 20 Jahren bis heute das Telefax als weit verbreitetes Kommunikationsmittel im Geschäftsverkehr und zur Dokumentenübertragung etabliert. Die beweistragende

Dokumenteneigenschaft sowie eine Empfangsbestätigung in Form eines qualifizieren Sendeberichts sind Vorteile bei der Wahl zur Dokumentenübertragung per Telefax ungeachtet vom Übertragungsweg.

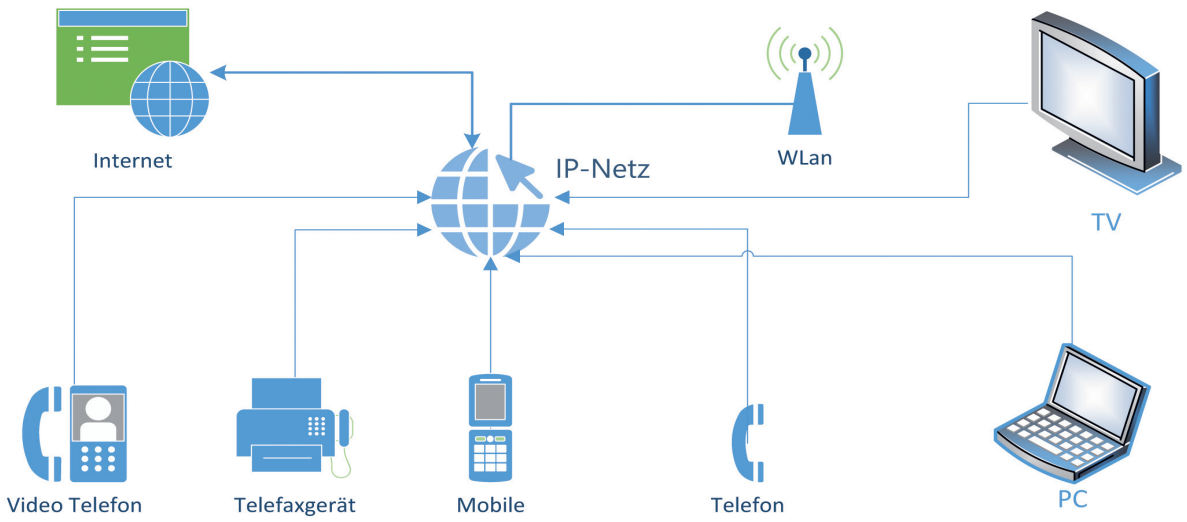
Im Zusammenhang mit der Umstellung auf die IP-Telefonie (All-IP Netz) gibt es eine immer wieder gestellte Frage:

- Was mache ich mit meinem Telefaxgerät
- und ist ein Telefax weiterhin noch ein ebenso „sicheres" Übertragungsmittel wie das beim leitungsbasierten Telefonanschluss der Fall war?

Die Frage, ob ein versendetes Telefax im IP-Netz „sicher" oder „unsicher" ist, lässt sich weder mit einem „ja" noch mit „nein" beantworten. Das galt jedoch auch in Bezug auf die herkömmliche Technik. So sind z. B. fehlgeleitete Telefaxe kein Phänomen unterschiedlicher Übertragungswege, sondern sie kommen da wie dort vor.

7.4.1 Fax-zu-Fax im All-IP Netz

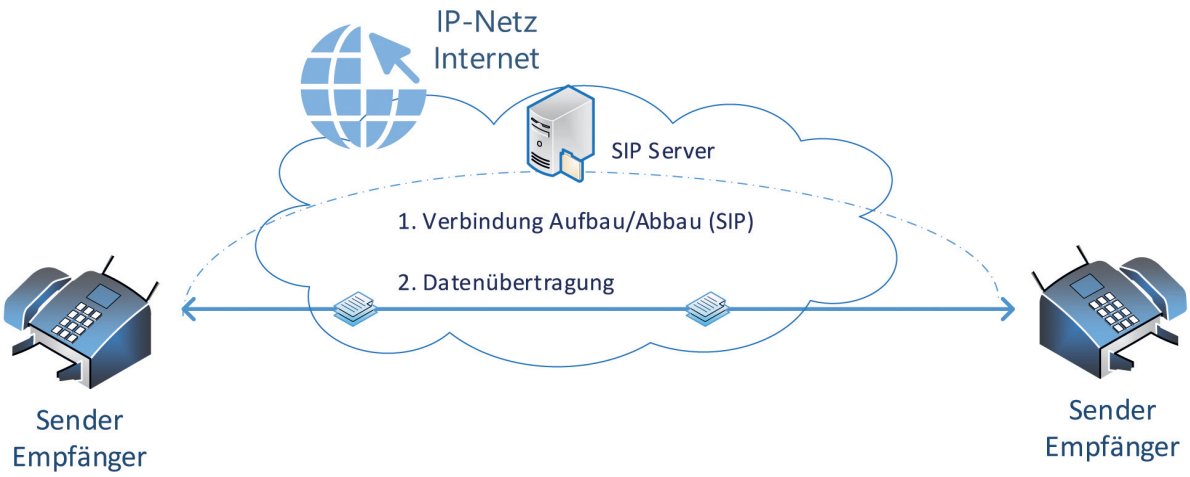
Im Rahmen der Umstellung auf das All-IP Netz wird das Telefax manchmal, zu Unrecht, als unsicher bezeichnet. Es wurde bereits die unausweichliche Umstellung der leitungsbasierten Telefonanschlüsse auf das digitale All-IP Netz erwähnt. Das bedeutet u.a., dass alles (z.B. Telefon, Datenverkehr,



Multimedia, TV, etc.) nur noch über eine Leitung, den sogenannten digitalen IP-Anschluss (IP-Netz) verfügbar ist.

Im Zeitalter der Digitalisierung sowie des papierlosen Büros nimmt die analoge Datenspeicherung in Papierform immer mehr ab. Kommunikation wird per E-Mail geführt und die Datenablage erfolgt zunehmend in Dokumenten Management Systemen (DMS). Nachrichten werden am Computer, Smartphone etc. erstellt und zeitnah verteilt. Dabei erhalten die Empfänger ebenfalls die Daten zur weiteren Verarbeitung in elektronischer Form.

Dennoch mag es Gründe geben, ein Dokument nicht elektronisch weiterzuleiten, sondern per Telefax zu übermitteln. Und hier kommen unterschiedliche Möglichkeiten zum Einsatz: Der herkömmliche Weg ist, dass Dokument aus der Anwendung (z.B. Patienteninformationssystem) auszudrucken und per physischem (also echtem) Telefaxgerät an die Gegenstelle zu senden, wo auch ein Telefaxgerät angeschlossen ist (Fax-zu-Fax). Dabei kann es sich auch um ein zentrales internes Telefax-System handeln. Allerdings hat heutzutage nicht jeder ein Telefaxgerät bzw. ein internes Telefax-System zur Verfügung, sondern bedient sich oftmals eines Dienstleisters der einen solchen TelefaxService anbietet (E-Mail/Dokument-zu-Fax).



Schematische Darstellung für eine direkte Fax-zu-Fax Datenübertragung

Fax-zu-Fax

Wie bei der herkömmlichen Variante wird ein Papierdokument oder ein elektronisches Dokument per Telefax übermittelt. Es besteht nach dem Verbindungsaufbau eine eins-zu-eins Verbindung zwischen beiden Telefaxgeräten. Bei dieser Variante steht beiden Kommunikationspartnern ein physisches Telefax Gerät zur Verfügung.

Dokument zu Fax-zu-Fax

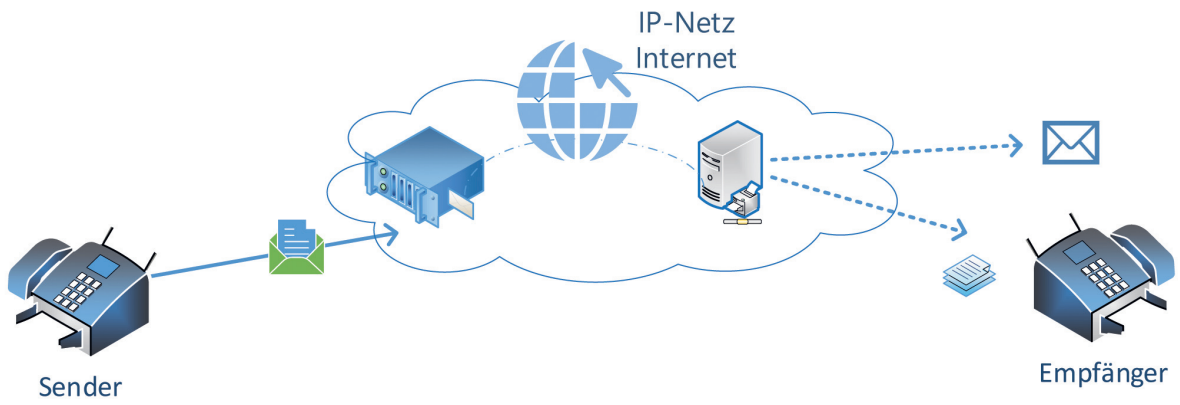
Ähnlich wie bei „Fax-to-Fax" wird jedoch hier ein elektronisches bzw. digitales Dokument aus einer Anwendung an ein internes Fax-System (Fax-Service) übermittelt, welches dann den Faxversand übernimmt (z.B. wie der Fax-Service einer Fritzbox).

Fax-zu-E-Mail

Es erfolgt ein Verbindungsaufbau zu einem Fax-to-E-Mail Gateway (evtl. über Zwischenstationen). Nach dem Empfang der Daten beim Fax-Gateway werden diese an den E-Mailserver des Empfängers übermittelt und in das Empfängerpostfach bis zur Abholung abgelegt. Bei dieser Variante steht dem Empfänger kein Telefax-Gerät/-Service zur Verfügung.

E-Mail-zu-Fax

Es erfolgt ein Verbindungsaufbau zum eigenen E-Mail Server (SMTP Einstellungen) und danach eine Weiterleitung (evtl. Zwischenstationen) zum Fax-Gateway. Als nächstes erfolgt die ein Versenden der Daten per Fax-Service an die Faxnummer des Empfängers. Ggfs. gehen



Schematische Darstellung für keine direkte Fax-zu-Fax Datenübertragung

Statusinformation per E-Mail zurück an den Absender. Bei dieser Variante steht dem Absender kein Telefax-Gerät/-Service zur Verfügung.

7.4.2 Telefax-Daten im digitalen IP-Netz

Bei der Übertragung in den neuen IP-Netzen müssen die analogen Tonsignale des Telefaxgerätes in ein digitales Signal umgewandelt werden. Aus technischer Sicht werden die Telefaxe per G.711 Protokoll (Audio Codec) übertragen was auch aktuelle Analog-Telefonadapter unterstützen. Damit dies jedoch zukünftig und auch in nicht so performanten IP-Netzen funktioniert, wurde dafür das T.38 (RFC 3362) [19] Protokoll entwickelt. Dabei werden die analogen Informationen umgewandelt, um sie anschließend als Datenpakete übertragen zu können. Da bei T.38 keine Konvertierung in einen Audiostream erfolgen muss, wird Bandbreite eingespart und der Verlust an Datenpaketen reduziert. Das T.38 Protokoll wird von immer mehr Providern und Geräten unterstützt (u.a. unterstützt auch die Fritzbox T.38). Damit kann von einer sicheren Datenübertragung ausgegangen werden.

Demnach kann man annehmen, dass eine direkte Fax-zu-Fax Verbindung bei der Übertragung der Daten nicht unsicherer ist, als bei den herkömmlichen leitungsbasierten Netzen. Nach einem Verbindungsaufbau der durch das SIP Protokoll erfolgt, wird eine direkte eins-zu-eins Verbindung hergestellt. Übrigens, das SIP Protokoll kann man sich so vorstellen, wie die herkömmlichen Vermittlungsstellen welche die Verbindung zu den Rufnummern hergestellt haben (z.B. auch per Hubdrehwähler).

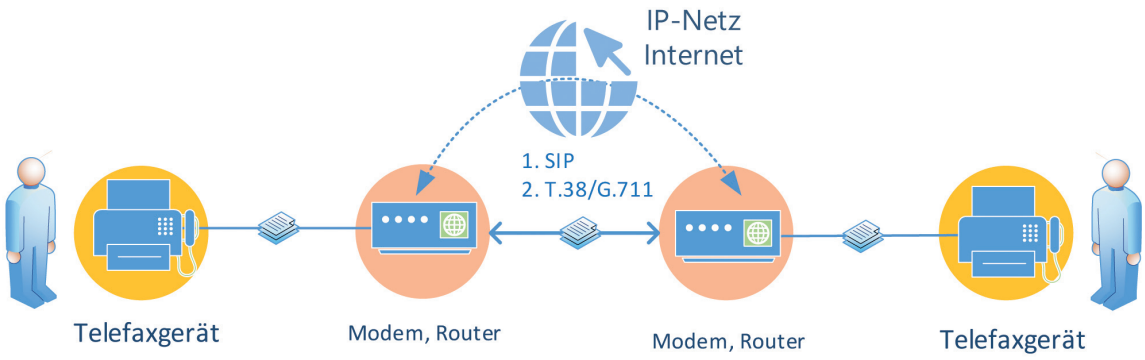
7.4.3 Der Datenschutz und ein zentrales Telefaxgerät

Beim Datenschutz ist ein nicht unerheblicher Punkt der Standort des Telefaxgerätes. In der Praxis hat nicht immer jeder Mitarbeiter ein eigenes Telefaxgerät, sondern es gibt ein zentrales Gerät welches meistens an einem zentralen Punkt aufgestellt ist. Zur Sicherstellung einer direkten Verbindung zwischen Sender (Absender) und Empfänger können sich beide Partner vorab telefonisch auf eine Sendezeit einigen, wo der Empfänger das Dokument (Fax) direkt aus dem Gerät entnehmen kann und den ordnungs-

19 http://www.faqs.org/rfcs/rfc3362.html

gemäßen Empfang bestätigt. Damit wäre u.a. einer Offenbarung fremder Geheimnisse nach § 203 StGB vorgebeugt.

Ergänzend sind die Vorschriften des § 24 der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) zu beachten.



7.4.4 Zustellmethode vs. Beweis

Beim Telefax erfolgt eine Datenübertragung immer direkt von Gerät zu Gerät, unabhängig vom Übertragungsweg. Für jedes versendete Fax erhält der Absender einen Sendebericht mit Empfangsquittierung und je nach Telefaxgerät inklusive einer Kopie der ersten gesendeten Seite als Nachweis, was an wen und zu welchem Zeitpunkt gesendet wurde.

Beim Telefax erfolgt eine Datenübertragung immer direkt von Gerät zu Gerät, unabhängig vom Übertragungsweg. Für jedes versendete Fax erhält der Absender einen Sendebericht mit Empfangsquittierung und je nach Telefaxgerät inklusive einer Kopie der ersten gesendeten Seite als Nachweis, was an wen und zu welchem Zeitpunkt gesendet wurde.

7.5 Gute Kennwörter nicht ständig wechseln, aber geheim halten

Eine sichere Authentifizierung sowie Autorisierung für Geräte als auch für Dienste als eine erste Schutzmauer ist bereits in unterschiedlichsten Gesetzen und Regelungen fest verankert. Ein in der Praxis übliches Verfahren zur Authentifizierung besteht aus einer Kombination aus Anmeldename mit Passwort (Anmeldekombination).

In Artikel 32 DS-GVO stellt diese Kombination zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten, Systeme und Dienste eine technische und organisatorische Maßnahme dar.

Auch im Gesetz über den kirchlichen Datenschutz (KDG) sowie in der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) gibt es mehrere Anforderungen die eine sichere Authentifizierung mittels Anmeldekombination verlangen (u.a. § 6 KDG-DVO). Nach § 11 KDG-DVO wird bereits für eine Anmeldung an ein IT-System für eine Datenverarbeitung von personenbezogenen Daten der Datenschutzklasse I, die Eingabe eines geeigneten benutzerdefinierten Kennwortes oder eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens notwendig.

Zur Sicherheit sowie zum Schutz, falls ein Passwort ggfs. bekannt geworden war, wurde von Sicherheitsbehörden und Organisationen empfohlen, Passwörter regelmäßig zu ändern. Technisch erreicht man das u.a. durch die Einrichtung von Mechanismen wie lange ein Passwort seine Gültigkeit behält. Die Lebenszeit eines Passworts (Laufzeit bis zum nächsten Wechsel) war mitunter so kurz, dass was gut gedacht war, sich als ein erhöhtes Risiko darstellte. Zum Beispiel durch das Notieren des aktuellen Passworts auf einen Zettel im Klartext, weil es schwer zu merken ist oder das alte Passwort wurde nur teilweise geändert indem die ersten oder der letzten Stellen abgeändert wurden. In Anbetracht dieser Erfahrungen wird heute nicht mehr der ständige Wechsel des Passworts durch Systeme empfohlen, sondern stattdessen sollte ein komplexes Passwort (ein gutes Passwort) verwendet werden welches geheim zu halten ist.

In einer Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) heißt es wörtlich unter: ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme [IT-Betrieb] (B)[20]

> *IT-Systeme oder Anwendungen sollten nur mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel sollten vermieden werden. Es nüssen Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Ist dies*

20 BSI - ORP.4 Identitäts- und Berechtigungsmanagement

nicht möglich, so sollte geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden.

Zu beachten ist folgender Hinweis: Es müssen Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Das bedeutet u.a., dass ein Wechsel des Passwortes möglich sein muss und unter bestimmten Umständen durchgeführt werden muss. Bei einer Datenverarbeitung von Daten der Datenschutzklasse II wird laut § 12 Abs.2 KDG-DVO folgende alternative Möglichkeit zum regelmäßigen systemweiten Passwortwechsel genannt: Alternativ ist die Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens möglich.

7.5.1 M1nPaßßw0rT – Mein Passwort

Doch wie kann ein „gutes Passwort" aussehen und natürlich sollte man sich dieses auch irgendwie merken können? Dabei hat sich die Bildung eines Satzes oder einer Textkombination mit unterschiedlichen Zeichen bewährt. Daraus wird ein (Pass)Wort mit unterschiedlichem Zeichenvorrat (Buchstaben, Zahlen, Sonderzeichen) gebildet.

Ein Passwort sollte mindestes 10 Zeichen lang sein (je länger desto besser), aus einer Kombination aus Buchstaben und Zeichen bestehen und sollten nicht mehrfach verwendet werden. Es sollten unbedingt unterschiedliche Passwörter für unterschiedliche Authentifizierungen/Anmeldungen (Webportal, Smartphone, PC, etc.) verwendet werden, unabhängig davon ob der Benutzername identisch bleibt (z.B. die E-Mail-Adresse). Falls dann eine Anmeldekombination aus Benutzername und Passwort bekannt geworden ist, wären in so einem Fall die anderen Portale weiterhin durch die andere Anmeldekombination geschützt. Weitere Hinweise sind unter dem Absatz „ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, ITBetrieb] (B)“ zu finden.

In der Praxis lassen leider nicht alle Portale Sonderzeichen zu. Auch die Anzahl der Zeichen die eingegeben werden können entspricht nicht immer einer angemessenen Länge. In so einem Fall muss ein alternatives Password ohne Sonderzeichen, jedoch mit ähnlicher Sicherheit, gewählt werden.

Falls das Passwort nur innerhalb eines lokalen Bereichs, wie z.B. im Betrieb, verwendet wird, können auch deutsche Sonderzeichen zum Einsatz kommen. Aber Vorsicht: Falls das System in dem Sie sich anmelden möchten keinen deutschen Zeichensatz kennt, dann können Sie das gewählte Passwort unter Umständen nicht eingeben. Ein Beispiel dazu wäre ein englisches Windows 10 mit einer deutschen Tastatur oder umgedreht wo keine deutschen Umlaute zu finden sind.

Hier als Beispiel einiger TOP Passwörter in öffentlichen Passwortlisten, **die nicht verwendet** werden sollten. Auch eine Kombination dieser Passwörter wie z.B. „secret1234“ sollte unbedingt vermeiden werden.

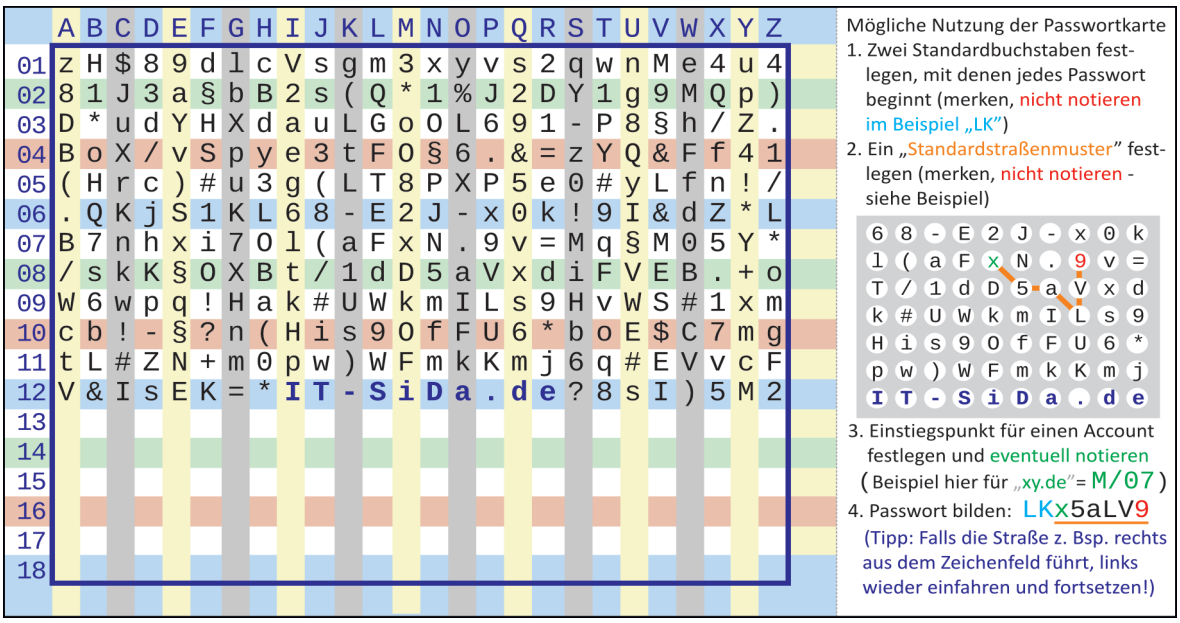
123456	123456789	password	adobe123
12345678	qwerty	1234567	111111
photoshop	123123	1234567890	000000
abc123	1234	adobe1	macromedia
azerty	iloveyou	aaaaaa	654321
fdsa	753951	chocolate	fuckyou
soccer	tigger	asdasd	thomas
asdfghjkl	internet	asdfghj	admina
secret	matrix	123123123	test
7777777	asdasd	master	computer

Es sei hier noch erwähnt, dass durch zwei- bzw. mehrstufige Authentisierungsverfahren eine zusätzliche Erhöhung der Sicherheit, unabhängig davon wie das Passwort gestaltet wird, gegeben ist.

7.5.2 Passwort managen lassen

Eine bereits oben genannte Sicherheitsvorkehrung ist es, dass dieselben Passwörter nicht mehrfach verwendet werden sollen. Auf Grund der vielen unterschiedlichen Portale und Anwendungen die eine Benutzeranmeldung (ZugangsAccount) erfordern und es werden immer mehr, erweist es sich in der Praxis als schwierig, so eine Anforderung immer konsequent umzusetzen. In dem Fall hilft nur eine regelmäßige Sensibilisierung z.B. auf das Thema Identitätsdiebstahl.

Eine in der Praxis eingesetzte Methode zur Verwaltung von komplexen Passwörtern und unterschiedlichen Zugangs-Accounts für die verschiedenen Anwendungen und Portale sind Passwortkarten oder ein Passwort-Safe- Programm oder auch verschlüsselte USB-Sticks die zentral verwaltet und gelagert werden.



Muster-Passwortkarte von IT-SiDa.de zum Merken von Passwörtern

Programme, die Passwörter bzw. komplette Zugangs-Accounts verwalten, haben den Vorteil, dass sie hoch komplexe Passwörter generieren können. Weil man sich die automatisch generierten Passwörter nicht mehr merken muss, schreibt man sich diese auch nicht mehr ungesichert auf. Ein weiterer Vorteil ist, dass die Daten in einer zentralen verschlüsselten Datenbank gespeichert sind. Die Passwort-Datenbank liegt praktischer Weise auf einem gemeinsamen betrieblichen und sicher gemanagten Datenlaufwerk. Bei dieser Methode wären auch zentrale ZugangsAccounts (z.B. für Einkaufsportale etc.) für mehrere autorisierte Personen verfügbar, ohne dass sich jeder selbst die sensiblen Daten in einer eigenen „unsichere Schattendatei" notieren muss.

Im Rahmen einer Konzeption zum Passwort-Management für betriebliche Zugangs-Accounts sollte das Thema Vertreterregelung sowie Datensicherung (Backup) und Benutzer-Management ein fester Bestandteil im Passwort-Management sein.

7.6 Der Stand der Technik

„Was ist der Stand der IT-Sicherheitstechnik ist, kann aufgrund permanenter Weiterentwicklung nicht in den Datenschutzgesetzen geregelt sein, die typischer Weise weit statischer sind.

Als Orientierung hat der Bundesverband IT-Sicherheit e.V.[21] eine Handreichung zum „Stand der Technik" technischer organisatorischer Maßnahmen herausgegeben. Darüber hinaus finden sich auch Ausführungen zum Thema auch auf der Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung unter anderem des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko an-

21 https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf

gemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können.

Zur Gewährleistung der Sicherheit der Verarbeitung ist bei den getroffenen technischen und organisatorischen Maßnahmen (TOM) durch den Verantwortlichen ein Verfahren zu etablieren, welches eine Anpassung an den aktuellen Stand der Technik erlaubt.

In einem weiteren Abschnitt heißt es u.a., dass Sicherheitsmaßnahmen für die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu treffen sind, um ein angemessenes Schutzniveau zu gewährleisten. Der „Stand der Technik" neben den physischen Geräten, der Hardware, auch Software sowie weitere Komponenten welche zur Datenverarbeitung erforderlich sind.

Als Beispiel für ein Zusammenspielen mehrere Komponenten sei eine Website mit einem Formular womit personenbezogene Daten wie z.B. die E-Mail-Adresse und der Name erfasst werden genannt, die die Daten aber im Klartext über eine nichtgesicherte Verbindung (http) übermittelt. In dem Fall gäbe es für die Datenübertragung zwischen Webbrowser und Webserver keinen gesicherten Transportweg (kein TLS/SSL; somit kein https) was aktuell für eine Verarbeitung personenbezogener Daten nicht mehr dem „Stand der Technik" entspricht.

Lebenszyklus vom Microsoft Produkten als Beispiel zum „Stand der Technik"

Ein aktuelles Beispiel was ab Januar 2020 nicht mehr unter dem „Stand der Technik" zu verstehen ist, ist das Microsoft Betriebssystem Windows 7.

Im Anhang befindet sich ein Auszug weiterer Microsoft Produkte, welche noch in vielen Einrichtungen aktiv genutzt werden und bei denen demnächst die Softwarepflege und der Support ausläuft - demzufolge der Lebenszyklus beendet ist.

7.7 Webseiten und HTTP(s)

Immer öfter ist zu hören, dass jeder der eine Website betreibt diese doch zeitnah auf „HTTPS" (TLS/SSL Verschlüsselung) umstellen sollte.

Zur Begrifflichkeit: Das Hypertext Transfer Protocol „HTTP“ ist ein Protokoll welches zur Übertragung von Daten (auf Anwendungsschicht) Verwendung findet. Es wird vorwiegend zum laden von Webseiten aus dem Internet im Zusammenhang mit einem Webbrowser verwendet (im Web surfen). Allerdings verläuft bei „HTTP“ die Datenübertragung zwischen den beiden Stationen (Webserver und Webbrowser) im Klartext, also unverschlüsselt. Alle Daten werden im Klartext übertragen. Bespielhaft wird dafür der Versand von Informationen auf einer offenen Postkarte genannt. Jemand der die Karte in der Hand hält, könnte Zugriff auf die Informationen, falls er der Sprache der geschriebenen Information mächtig ist, erlangen. Damit sensible Daten über einen sicheren Übertragungsweg geschickt werden können, wurde das Hypertext Transfer Protocol Secure „HTTPS“ eingeführt und technisch in die Systeme integriert. „HTTPS“ stellt somit die Möglichkeit einer Transportverschlüsselung (Transport Layer Security oder TLS genannt) zwischen beiden Stationen zur Verfügung. Mit TLS (manchmal auch noch als SSL bekannt) ist eine abhörsichere Datenübertragung sensibler Daten möglich.

„TLS“ bietet u.a. auch die Fähigkeit zum Integrationsschutz.

Bei der Diskussion, weshalb eine „normale“ Website ohne jegliche Formulare und andere Eingabemöglichkeiten (z.B. Kontaktformular), auf „HTTPS“ umgestellt werden soll, hört man öfter das Argument, dass die IP-Adresse der Kommunikationspartner schließlich auch ein personenbezogenes Datum sei.

Ohne weiter technisch auf das Protokoll einzugehen ist es gut zu wissen, dass die IP-Adressen im Zusammenhang mit „HTTPS“ für einen Verbindungsaufbau der Kommunikationspartner (wer will wohin) zwingend erforderlich sind und deshalb nicht verschlüsselt werden können. Aus der netzwerktechnischen Protokollsicht setzt TLS erst nach dem Verbindungsaufbau in der Sitzungs- und Präsentationsschicht ein. Demzufolge werden die IP-Adressen der Kommunikationspartner, auch durch Umstellung auf „HTTPS“, nicht verschlüsselt.

Es gibt aber andere Argumente welche für eine Umstellung auf „HTTPS“ interessant sind, wie z.B. die zunehmende Kennzeichnung der Webbrowser bei „nicht HTTPS“ Websites als „Unsicher“ und der evtl. Nachteil beim Ran-

king von Suchmaschinen. Ein weiterer Vorteil von „HTTPS“ ist eine Überprüfung der Kommunikationspartner (Authentifikation) und die Sicherstellung der Integrität der transportierten Daten, also dass diese während des Transports nicht verändert wurden.

7.7.1 Mixed Content - unverschlüsselte Downloads in verschlüsselten Websites

Damit ist ein „Gemischter Content“ in einer per „HTTPS“ (TLS/SSL) abrufbaren Website gemeint, bei der im Hintergrund Ressourcen über eine nicht verschlüsselte „HTTP“ Verbindung abgerufen (Download) werden. Das können beispielsweise Dateien, Bilder, Scripts, etc. sein.

Website Betreiber sollten ihrer Website überprüfen, ob dort Mixed-Content Downloads integriert ist. Falls diese vorhanden sind, sollte geprüft werden wie diese umgestellt werden können. Denn in naher Zukunft werden Webbrowser einen Download einiger Content-Typen bei Mixed Content ggfs. blockieren.

Auszug aus der W3C Candidate Recommendation[22] Spezifikation:

Die Spezifikation „Mixed Content“ beschreibt, wie ein Benutzeragent (z.B. der Webbrowser) das Abrufen von Inhalten über unverschlüsselte oder nicht authentifizierte Verbindungen im Kontext eines verschlüsselten und authentifizierten Dokuments behandeln soll. Als Beispiel sei hier der Aufruf der Website „https://secure.meinewebsite.xy/“ mit gemischten Inhalten genannt:

a) Eine Anforderung für das Skript http://meinewebsite.xy/script.js besteht aus gemischtem Inhalt (weil diese nicht per „https“ übertragen wird). Da Skriptanforderungen blockierbar sind, gibt der Benutzeragent einen Netzwerkfehler zurück, anstatt die Ressource zu laden.

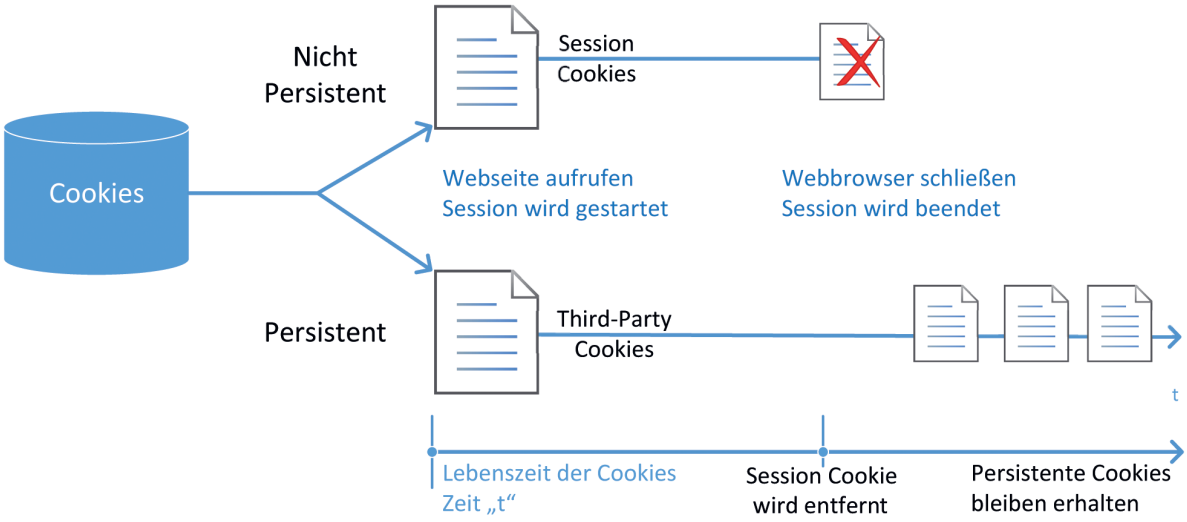
b) Eine Anfrage für das Bild http://meinewebsite.xy/bild.png besteht aus gemischtem Inhalt. Da Bildanforderungen optional blockierbar sind, lädt der Benutzeragent möglicherweise das Bild. In diesem Fall handelt es sich bei der Bildressource selbst um gemischten Inhalt.

22 World Wide Web Consortium (W3C) Mixed Content https://www.w3.org/TR/mixed-content

Datenschutzrelevant wären dann gemischte Inhalte, sobald personenbezogene Daten zwar über einen „HTTPS“ Link aufgerufen werden, diese dann innerhalb der Website über eine nicht gesicherte Verbindung (nur HTTP) weiter übertragen werden. Ein Beispiel dafür wäre ein Kontaktformular welches die Eingabedaten an einen „HTTP“ Link übermittelt und die personenbezogenen Daten im Klartext (unverschlüsselt) übertragen werden. In so einem Fall würden die Datenschutzaufsichtsbehörden einen datenschutzrelevanten Verstoß feststellen und Bußgelder verhängen können.

7.8 Cookie-Banner, jetzt mehr Klarheit oder mehr Unsicherheit

Wir möchten hier keine technische Abhandlung von Server und Website Cookies erläutern, sondern informationshalber und zum besseren Verständnis die zwei Cookie-Arten, um die es im Grunde genommen geht, erwähnen.



Nicht persistente Cookies

Diese Art der Cookies wird nach der Sitzung (Session) automatisch entfernt. Beispiele dafür sind Session-Cookies oder Warenkorb Cookies. Session-Cookies werden für jede neue Sitzung (Session) vom Webserver erzeugt und nach Beenden des Webbrowsers aus dem

Speicher entfernt. Sie werden auch nicht innerhalb einer Webanwendung durch den Websitebetreiber eingerichtet, sondern sind meistens technisch bedingte Informationen vom Server die eine ordnungsgemäße Funktion der Webanwendung sicherstellen.

Persistente Cookies

Bei dieser Art von Cookies handelt es sich um dauerhaft auf dem Client gespeicherte Informationen die erneut abrufbar sind. Beispiele dafür sind die Verwendung im Rahmen von Online-Marketing (Third-Party Cookie) oder Tracking (Analytics). Die Cookies können vom Benutzer manuell gelöscht werden oder verfallen nach Ablauf einer festgelegten Zeit (Lebenszyklus eines Cookies).

Grundsätzlich richten Cookies keinen technischen Schaden an. Es handelt sich um kleine Textdateien mit Informationen die der Webserver oder eine Website hinterlassen kann. Mit Hilfe der Einstellungen im Webbrowser kann das Verhalten von Cookies in einem gewissen Rahmen konfiguriert werden, wie das Löschen aller Cookies beim Schließen des Webbrowsers.

Nach einem Urteil des EuGH[23] zur Rechtssache „Planet49" gibt es noch immer Unsicherheit was die kleinen Textinformationen in Form von Cookies, welche beim Aufruf von Webseiten auf einem Gerät hinterlegt (gespeichert) werden, betrifft. Betrachtet man die geltenden Datenschutzgesetze, so gibt es eigentlich nichts was neu wäre, denn auch hier gelten zumindest die Informationspflichten nach § 15 KDG (Art.13 DS-GVO). Allerdings wurde durch das Urteil mehr Klarheit im Zusammenhang mit der Verwendung von nicht unbedingt benötigten Cookies geschaffen. Und trotzdem scheint es in der Praxis eine gewissen Unstimmigkeit zu geben, was auch an der noch immer im Gesetzgebungsprozesses befindlichen ePrivacy-Verordnung liegen könnte.

Sobald eine Website aufgerufen wird, wird man mit den unterschiedlichsten Einblendungen (den Cookie-Banner) zur Information über die Verwendung von Cookies konfrontiert. Einige dieser Cookie-Banner geben uns transparente Informationen darüber wozu auswählbare Cookies verwendet werden und wie lange deren normale Laufzeit ist. Andere wiede-

23 EuGH Urteil vom 1.10.2019, C-673/17

rum können nur bestätigt werden damit der Inhalt der Website überhaupt angezeigt wird und das ohne weitere Informationen. In einigen Fällen ist der Cookie-Banner derart gestaltet, dass weder Website noch Pflichtinformationen gelesen werden können was u.a. auch abhängig von dem Gerät sein kann, von welchem die Website aufgerufen wird. Eine transparente und für uns leicht verständliche Form der Information mit der wir als Anwender verstehen und damit entscheiden können welche Art von Cookies wir zulassen möchten ist nicht immer erkennbar. Das liegt u.a. auch daran, dass hier mehrere Interessen aufeinanderstoßen. Zum einen ist es der Datenschutz und zum anderen die Wirtschaft für die unsere Informationen ein wichtiger Rohstoff in Form der Daten sind.

Unabhängig von der Rechtslage gibt es durch die Einblendung der Cookie-Banner einen positiven Effekt, auch wenn die Website manchmal durch den Hinweis nicht zu lesen ist. Der User wird darauf aufmerksam gemacht, was so alles an Daten beim normalen Surfen im Internet gesammelt und verarbeitet wird. Damit sind nicht immer nur personenbezogene Daten gemeint, sondern auch statistische Daten welche für die Wirtschaft von Bedeutung sind.

Zum weiteren Verständnis einige Informationen, weshalb die Rechtsache „Planet49“ auch für den Datenschutz so interessant ist. Das Setzen von nicht notwendigen Cookies erfordert die aktive Einwilligung des Internetnutzers, so der Europäische Gerichtshof. Bei einem bereits voraktiviertem Bestätigungskästchen (Checkbox) kann eine freiwillige Einwilligung nicht wirksam erteilt werden!

In der Rechtssache Planet49 hat der EuGH entschieden, dass keine wirksame Einwilligung vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein mit einem voreingestellten Häkchen versehenen Ankreuzkästchen erlaubt wird. Das gilt unabhängig davon, ob es sich bei den betreffenden Informationen um personenbezogene Daten handelt oder nicht. Der Gerichtshof hat ferner klargestellt, dass der Diensteanbieter dem Nutzer mitteilen muss, welche Funktionsdauer die Cookies haben und ob Dritte Zugriff auf sie erhalten können.

In der Zusammenfassung zum Urteil heißt es weiter: Die klaren und umfassenden Informationen müssen den Nutzer in die Lage versetzen, die Konsequenzen einer etwaigen von ihm erteilten Einwilligung leicht zu ermitteln, und gewährleisten, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird. Angaben zur Funktionsdauer der Cookies und dazu, ob Dritte Zugriff auf die Cookies erhalten können, zählen zu den klaren und umfassenden Informationen, die der Diensteanbieter dem Nutzer einer Website zu geben hat.

Im Ergebnis des EuGH Urteils wird seitens unserer Aufsichtsbehörde die Rechtsauffassung vertreten, dass eine Einwilligung für unbedingt notwendige Cookies wie technisch bedingte Session-Cookies welche vom Webserver gesetzt werden und nach dem Beenden der Sitzung wieder entfernt werden, nicht erforderlich ist. Als Rechtsgrundlage nach den Datenschutzgesetzen könnte ggfs. der § 6 KDG (Art. 6 DS-GVO) herangezogen werden.

Daraus würde sich u.a. folgender Handlungsbedarf ableiten lassen.

- Website auf Cookies prüfen, ggfs. vom Entwickler oder der WebsiteAgentur beraten lassen
- Website auf Inhalte prüfen ob dort durch eine Verlinkung oder ein IFrame Cookies von anderen Websites gesetzt werden. Ggfs. das auf „Gemeinsame Verantwortliche“ prüfen.
- Datenschutzerklärung auf die Informationspflicht prüfen und ggfs. überarbeiten.
- Bestandsaufnahme aller Persistent-Cookies und Rechtslage klären, Einwilligung einholen und klären wie der Widerspruch organisiert wird.
- Website prüfen lassen

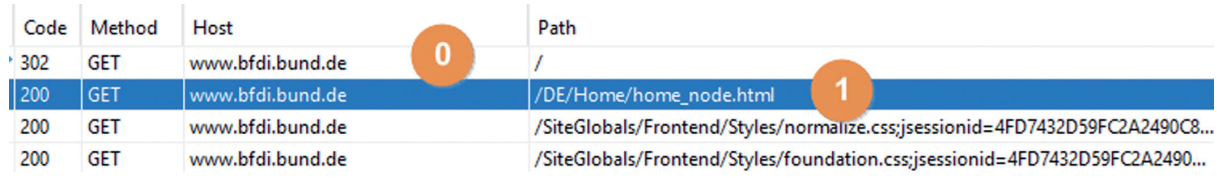
Session-Cookies aus technischer Sicht

Sobald eine Verbindung durch Aufruf eines Weblinks mit einem Webserver besteht, sendet der Webserver Informationen an den Webclient. Die folgende Grafik verdeutlicht beispielhaft den Aufruf eines Weblinks.

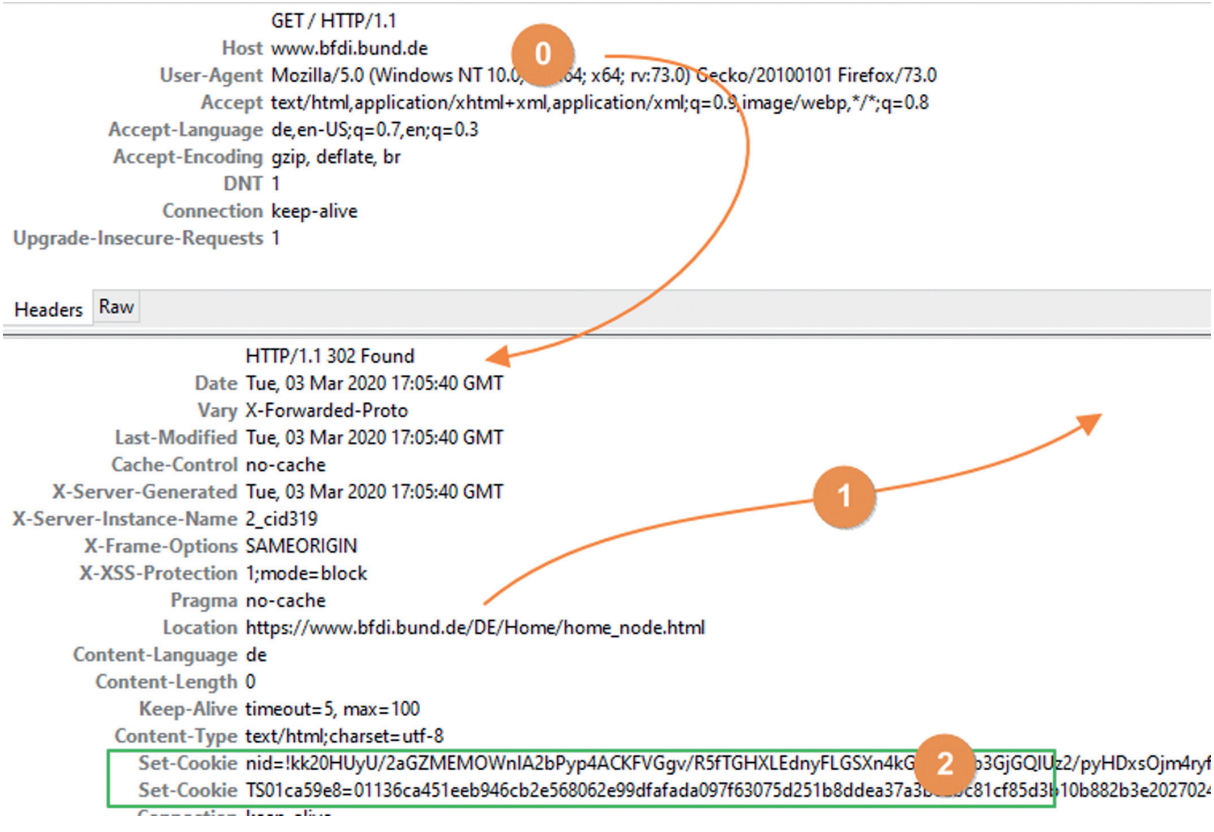
Phase 0:
Ein Weblink (WWW Adresse, URL) wird im Webbrowser aufgerufen und der

Webbrowser erhält vom Webserver den Hinweis auf die eigentliche Webseite die angezeigt werden soll (.../home_node.html)

Phase 1:
Der Webbrowser folgt dem Hinweis und ruft automatisch die Webseite ab (folgt dem Link/Verweis)



Phase 2:
In der folgenden Grafik ist zu erkennen, dass bereits in der Aufrufphase des Weblinks (0) ein Session-Cookie gesetzt wird, ohne dass wir eine Webseite im Webbrowser sehen werden. Denn die Webseite ist noch nicht vorhanden, sondern wird erst noch abgerufen (1).



An diesem Beispiel ist gut zu erkennen, dass bei den hier technisch bedingten Session-Cookies die vom Webserver benötigt werden, noch kein Cookie-Banner erscheinen kann. Es gibt bis zum Abschluss von Phase 2 noch keine Webseite mit Inhalt obwohl Webbrowser und Webserver miteinander kommuniziert haben.

7.9 Bin ich noch Sicher?

Im Zeitalter der immer fortschreitenden Digitalisierung und des immer zunehmenden Datenverkehrs wird es keine absolute Sicherheit geben können. Datenschutz und Datensicherheit fängt aber immer beim Einzelnen an. Deshalb kann jeder dazu beitragen, die eigene und die Sicherheit seiner Klienten und Geschäftspartner zu erhöhen. Ein wesentlicher Punkt ist es dabei, im Rahmen der Datensparsamkeit nur die Daten zu verarbeiten, welche für den erforderlichen Zweck zwingend notwendig sind.

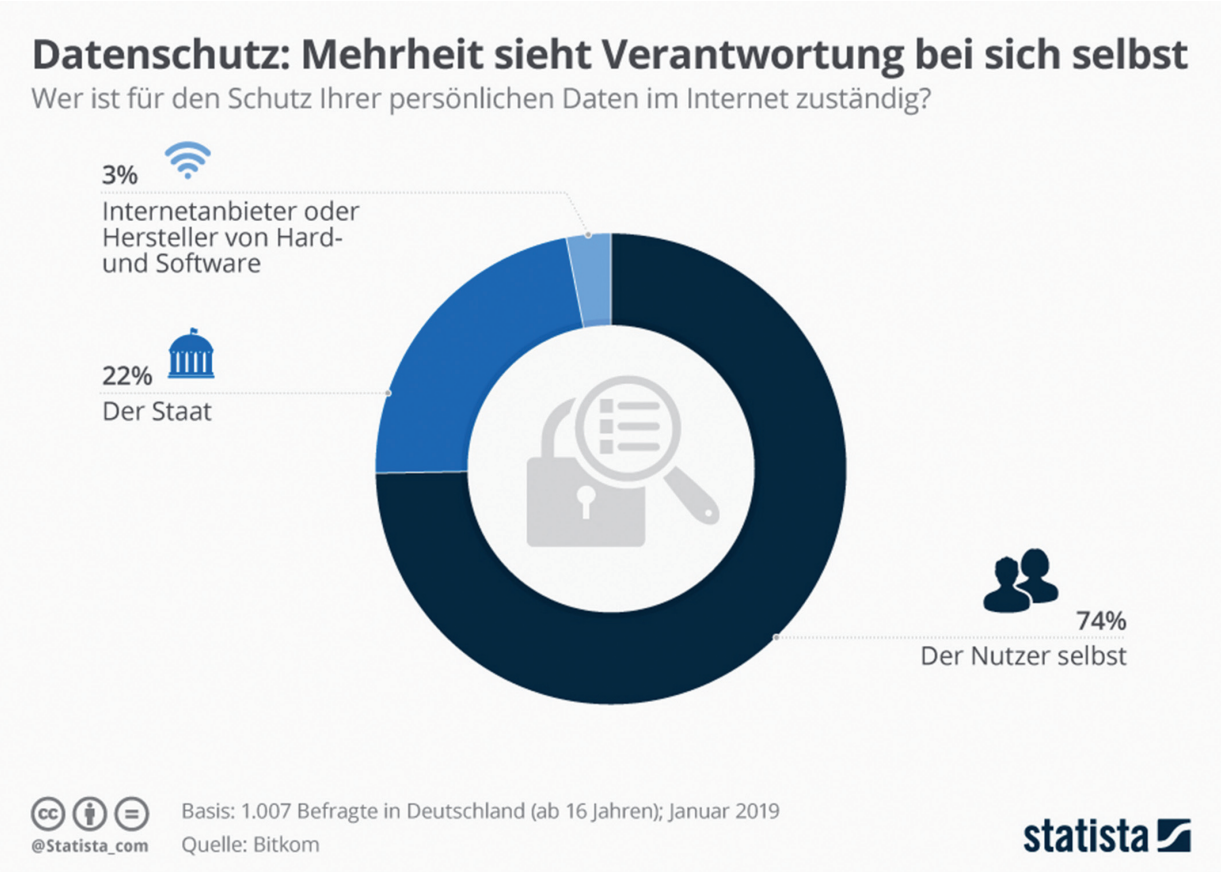
Cyberkriminalität ist ein global wachsendes und ausgeklügeltes Geschäftsmodell. Davon betroffen können alle Marktteilnehmer sein, unabhängig von der Größe der Einrichtung oder davon ob es sich um geschäftliche oder private Tätigkeiten handelt. Je mehr personenbezogene Daten über jemanden bekannt sind, umso besser kann ein Cyberangriff vorbereitet und durchgeführt werden. Dieser muss sich dann nicht nur auf einen Datendiebstahl oder einen Identitätsmissbrauch beschränken, sondern kann auch zu einem physischen Einbruch führen.

Wenn personenbezogene Daten freiwillig und in nicht erforderlichem Umfang preisgegeben werden, (z.B. durch Synchronisation von Kontakten oder Bildmaterial), können Datenschutzgesetze vor einem Missbrauch dieser Daten und Informationen nicht schützen.

Datenschutz fängt bei uns selbst an!

Nach einer Umfrage von BITCOM und Statista ist diese Einsicht bei der Mehrheit der Internetnutzer bereits angekommen.[24]

24 https://de.statista.com/infografik/16771/umfrage-zur-verantwortung-beim-thema-datenschutz/



8 Datenschutzvorfälle

8.1 Datenschutz in der Pfarrei

Pfarreien unterliegen gem. § 3 Abs. 1 Nr. 1 KDG ausdrücklich dem Anwendungsbereich dieses Gesetzes. Dabei wird nicht danach unterschieden, wer in der Pfarrei personenbezogene Daten verarbeitet. Dies kann durch hauptamtlich tätige Mitarbeiter ebenso wie durch Ehrenamtliche geschehen.

Wenn Gremien einer Pfarrei Protokolle über ihre Sitzungen erstellen, ist dabei darauf zu achten, ob diese personenbezogene Daten enthalten. Ist dies der Fall sind insbesondere bei der Versendung und der Veröffentlichung die datenschutzrechtlichen Anforderungen zu berücksichtigen.

In einem konkreten Fall ging es um die Veröffentlichung eines Protokolls des Pfarrgemeinderates (PGR) durch eine Kirchengemeinde im Internet.

In diesem Protokoll wurden personenbezogene Daten gem. § 4 Nr. 1 KDG verarbeitet i. S. v. § 4 Nr. 3 KDG.

Eine solche Verarbeitung personenbezogener Daten ist nur rechtmäßig i. S. d. § 6 Abs. 1 KDG, wenn eine der dort genannten Bedingungen erfüllt ist. Das war vorliegend nicht der Fall!

In dem Protokoll findet sich unter Punkt 8. Verschiedenes h) der Hinweis

> „Jugendkeller:
>
> Sehr schmutzig,
>
> X.Y. ist für den Keller verantwortlich.
>
> Pfr. Z. wird mit ihr zu ihrer Verantwortlichkeit sprechen."

Aus dieser Darstellung erwächst nachvollziehbar der Eindruck, dass X.Y. für den Keller und somit auch für die Verschmutzung verantwortlich ist. Durch die Veröffentlichung im Internet wird dies einer zahlenmäßig nicht bestimmbaren, weltweiten Öffentlichkeit mitgeteilt. Darüber hinaus sind damit die Daten verbunden, X.Y. ist katholisch und in der Pfarrei St. M engagiert. Hinzu kam vorliegend die Tatsache, dass die Petentin sich gerade um eine Ausbildungsstelle bemüht und die Sorge hat, dass ihr aus dieser kompromittierenden Darstellung bei potentiellen Arbeitgebern ein Nachteil erwächst.

X.Y. (Betroffener) hat sich an den Vorstand des Pfarrgemeinderates gewandt. In diesem Schreiben verlangt die Betroffene die Löschung ihres Namens im Internet im Zusammenhang mit dem PGR-Protokoll.

Der Vorstand hat unter Berufung auf eine Auskunft der betrieblichen Datenschutzbeauftragten der Kirchengemeinde die Ansicht vertreten, zu einer Veröffentlichung personenbezogener Daten im Rahmen des Protokolls berechtigt zu sein und hat eine Entfernung aus dem Protokoll und damit eine Löschung im Internet abgelehnt. Darüber hinaus hat sie die Betroffene aufgefordert im Rahmen eines persönlichen Gespräches das „berechtigte Interesse" darzulegen und hat das persönliche Erscheinen der Betroffenen zu diesem Termin angeordnet.

Entgegen der Rechtsauffassung des betrieblichen Datenschutzbeauftragten ist keine der Bedingungen des § 6 Abs. 1 KDG erfüllt.

Anders als von der betrieblichen Datenschutzbeauftragten dargestellt, ist die Verarbeitung nicht zur Wahrnehmung einer Aufgabe erforderlich, die im kirchlichen Interesse steht.

Ein Protokoll richtet sich zunächst an die Teilnehmer der Sitzung. Diese sollen im Nachgang der Sitzung feststellen können, ob die Inhalte der Sitzung korrekt erfasst worden sind. Darüber hinaus sollen Verantwortlichkeiten für in der Sitzung ggf. besprochene oder verteilte Aufgaben nachvollzogen werden können. Das Protokoll dient also der Unterstützung der Arbeit des Gremiums. Bereits an dieser Stelle ist festzustellen, dass es der Namensnennung der Betroffenen an der betreffenden Stelle nicht bedurft hätte. „Erforderlich" i. S. der Vorschrift ist nur eine Verarbeitung, die zwingend notwendig ist um den Zweck zu erreichen. Dieses Kriterium trifft auf die streitige Datenverarbeitung nicht zu.

Für die Arbeitsfähigkeit des Gremiums hätte die Feststellung: „Pfarrer Z spricht mit der Verantwortlichen." völlig ausgereicht.

Soweit die betriebliche Datenschutzbeauftragte ausführt, es sei die Meinung vertretbar, Protokolle des PGR und deren Veröffentlichung seien Teil der Gemeindearbeit und die Information der Gemeindemitglieder liege im kirchlichen Interesse, verkennt diese Darstellung, dass es vorliegend darum nicht geht. Es steht dem PGR frei, über seine Arbeit zu berichten. Diese Freiheit endet aber dort, wo Persönlichkeitsrechte Dritte verletzt werden. Um von seiner Arbeit zu berichten, ist es für den PGR nicht erforderlich, wertende Aussagen über konkret benannte Personen zu veröffentlichen.

Die Pfarrei als Verantwortlicher (§ 4Nr. 9 KDG) wird vom Kirchenvorstand vertreten. Vorsitzender des Kirchenvorstandes ist in diesem Fall der Pfarrer. Dieser hat den Schriftwechsel erst nach Rückkehr aus seinem Urlaub zur Kenntnis genommen, dann aber unverzüglich im Sinne der datenschutzaufsichtlichen Weisung gehandelt. Die Petentin erklärte die Angelegenheit daraufhin für erledigt.

8.2 Datenschutz im Krankenhaus

Einen besonderen Schutz genießen nach § 4 Nr. 2 KDG personenbezogene Daten besonderer Kategorie. Dazu gehören u. a. auch Gesundheitsdaten gem. § 4 Nr. 17 KDG, also solche Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Der Begriff ist weit auszulegen und erfasst auch die Tatsache einer klinischen Behandlung. Somit unterfällt bereits die Auskunft über den Aufenthalt eines Betroffenen in einem Krankenhaus oder über dessen Patienteneigenschaft bei einer Ärztin dem Kriterium der „personenbezogenen Daten besonderer Kategorie".

Solche personenbezogenen Daten besonderer Kategorie unterliegen dem Verarbeitungsverbot des § 11 Abs. 1 KDG. Dies gilt nur in den Fällen nicht, für die Abs. 2 der Vorschrift eine Ausnahme vorsieht.

Zu den Ausnahmen in § 11 Abs. 2 KDG gehört zunächst die Einwilligung des Patienten. Eine Einwilligung nach § 4 Nr. 13 KDG ist jede freiwillige für den bestimmten Fall in informierter Weise abgegebene Willensbekundung.

8.2.1 Hauptverstoß im Krankenhaus: vertauschte Patientenakten

Einer der häufigsten Datenschutzverstöße besteht in der falschen Versendung von Arztbriefen. Dies ist nicht nur in den Krankenhäusern, die unserem Aufsichtsbereich unterliegen so, sondern stellt sich deutschlandweit und trägerübergreifend als Problem dar.[25]

Aus den Stellungnahmen der Krankenhäuser lässt sich gelegentlich vermuten, dass die Ernsthaftigkeit dieses Problems nicht hinreichend wahrgenommen wird. Die Tatsache wird zwar regelmäßig bedauert, oftmals aber mit hoher Arbeitsbelastung, situationsbedingter Hektik o. ä. erklärt. Es ist davon auszugehen, dass nur ein Bruchteil der falsch versendeten Unterlagen bekannt wird und in diesem Bereich eine hohe Dunkelziffer besteht.

25 https://www.medical-tribune.de/praxis-und-wirtschaft/praxismanagement bereits 23.04.2017, zuletzt eingesehen am 19.02.2020; Zeit online vom 3.12.2019 „Sensible Patientendaten landen häufig bei der falschen Adresse" zuletzt eingesehen am 19.02.2020

Gerade weil das Problem bekannt ist, sind erhöhte Sicherheitsmaßnahmen gefordert. Dazu gehört in erster Linie eine an der Praxis orientierte, belastbare Verfahrensanweisung, für den Umgang mit Entlassungsbriefen.

Bei den Informationen in den Entlassungsbriefen handelt es sich um personenbezogene Daten besonderer Kategorie gem. § 4 Nr. 2 KDG. Dabei handelt es sich um Gesundheitsdaten gem. § 4 Nr. 17 KDG.

Mit der Offenlegung gegenüber Dritten werden diese personenbezogenen Daten besonderer Kategorie „verarbeitet" im Sinne des § 4 Nr. 3 KDG. Die Verarbeitung von personenbezogenen Daten besonderer Kategorie ist gem. § 11 Abs. 1 KDG unzulässig. Der Gesetzgeber macht durch diese Vorschriften deutlich, dass es für diese Daten eines besonders hohen Schutzes bedarf. Weiterhin sind diese Daten auch durch andere gesetzliche Vorschriften geschützt. Insbesondere ist hier auch § 203 StGB zu beachten. Diese Vorschrift verlangt eine vorsätzliche Begehung der Tat. Sollte ein Krankenhaus innerhalb einer kürzeren Zeitspanne vermehrt und trotz entsprechender Korrekturhinweise falsche Empfänger informieren, könnte ihm strafrechtlich aber ein „bedingter Vorsatz" unterstellt werden. In einem solchen Fall sähe sich die Aufsicht verpflichtet, den Sachverhalt durch die Staatsanwaltschaft prüfen zu lassen.

Weil es sich um besonders sensible Daten handelt und das Problem bekannt ist, erscheinen bloße Verwarnungen oder Anordnungen durch die Aufsicht unangebracht. Aus Sicht der Datenschutzaufsicht ist vielmehr der „Vermeidungsdruck" bei den Verantwortlichen durch eine spürbare Geldbuße zu erhöhen. Bei der Festlegung der Höhe dieser Geldbuße wird u. a. zu berücksichtigen sein, ob der Verantwortliche einen verbindlichen Ablauf definiert und in einem Prozess festgeschrieben hat. Weiterhin ist nachzuweisen, dass Mitarbeiter/innen diesen Prozess kennen und auch anwenden und eine regelmäßige Überprüfung erfolgt.

8.2.2 Herausgabe an Hausarzt

In diesem Zusammenhang ist darauf hinzuweisen, dass auch die Herausgabe des Entlassungsbriefes an den Hausarzt einer Einwilligung des Patienten bedarf. Die vom Patienten im Aufnahmebogen oder Behandlungsvertrag

enthaltene Mitteilung des Hausarztes ist nicht als stillschweigende Einwilligung in die Versendung von Patientenunterlagen an diesen zu werten. Es steht dem Patienten frei, die Unterlagen statt seinem bisher behandelnden Hausarzt einem anderen Arzt zu übergeben.

8.2.3 Herausgabe an Familienangehörige

Empfangsberechtigt für den Entlassungsbrief, wie für andere Patientendaten ist ausschließlich der Patient selber. Eine Herausgabe von Patientendaten an Dritte ist nur bei Vorliegen einer entsprechenden Vollmacht erlaubt. Für nahe Angehörige, wie Ehepartner oder Kinder gilt diesbezüglich keine Ausnahme.

8.2.4 Sichern von Rechnern

In einem Fall hat uns ein Petent folgenden Datenschutzverstoß gemeldet:

Der Petent war mit seiner Tochter in der Notfallambulanz eines Krankenhauses. Der Arzt pflegte im Rahmen des Gespräches die Informationen gleich in die elektronische Akte ein. Aufgrund eines Notfalls wurde der Arzt kurzfristig aus dem Behandlungszimmer gerufen und ließ den Vater mit seiner Tochter allein in dem Raum zurück. Der Vater nutzte diesen Umstand, ging um den Tisch herum und bediente selbständig den Rechner. Dabei schaffte er es die Akten von weiteren Patienten zu öffnen.

Man kann sich an dieser Stelle zwar Gedanken machen, inwieweit der Petent mit den Grundregeln des Anstands vertraut war, bzw. seine Dreistigkeit kritisieren, das ändert aber nichts daran, dass das Verhalten des Arztes einen Datenschutzverstoß darstellte. Auch in dem Fall der kurzfristigen Abberufung aus dem Behandlungszimmer ist der Arzt verpflichtet, den Rechner vor dem Verlassen des Raumes zu sperren. Dafür sind Voraussetzungen zu schaffen, damit dies mit einem Schalter oder einer einfachen Tastenkombination möglich ist. Die Aufhebung der Sperrung darf dann nur mit einem Passwort möglich sein.

8.2.5 Offenes Behandlungszimmer

Eine Petentin beschwerte sich darüber, dass während sie behandelt wurde, die Tür zum daneben liegenden Behandlungsraum nicht verschlossen war.

Auch dieser Umstand stellt einen Datenschutzverstoß dar. Das Gespräch zwischen Arzt und Patient ist vertraulich. Steht während dieses Gespräches die Tür zum Nachbarraum offen, in dem sich ein weiterer Patient oder Dritter aufhält, findet eine Bekanntgabe personenbezogen Daten besonderer Kategorie an Dritte statt. Ein solches Verhalten ist weder durch ein hohes Patientenaufkommen, einen Arbeitsdruck oder sommerliche Temperaturen noch aus anderen Gründen gestattet. Seitens des Krankenhauses sind hier eindeutige Regelungen erforderlich, die ein solches Verhalten untersagen. Setzt sich ein Arzt darüber hinweg, in der Annahme das wohl nichts passieren wird, liegt bedingter Vorsatz vor, der eine strafrechtliche Verfolgung rechtfertigt.

8.2.6 Unbeobachteter Aufenthalt in Patientenzimmern

Um die Abläufe in einer Krankenhaussprechstunde zu beschleunigen, werden Patienten häufig gebeten in einem Behandlungszimmer Platz zu nehmen und dort auf den Arzt zu warten. Gegen ein solches Verfahren ist nichts einzuwenden, wenn die datenschutzrechtlichen Voraussetzungen beachtet werden. Ein in einem solchen Behandlungszimmer stehender Rechner muss gesperrt und gegen entsperren gesichert sein. Behandlungsunterlagen (Akten) anderer Patienten dürfen nicht in dem Zimmer liegen.

8.2.7 Mitteilung an den/die Krankenhausseelsorger

Die Kirche betrachtet es regelmäßig als ihre Aufgabe, Gemeindemitglieder, die sich im Krankenhaus befinden seelsorgerisch und karitativ zu betreuen. Darüber hinaus wird eine umfassende Betreuung des/der Patienten in medizinischer, pflegerischer und seelsorgerischer Hinsicht angestrebt. Dennoch gelten die datenschutzrechtlichen Vorschriften vollumfänglich auch für die Krankenhausseelsorge. Aus dem Ausnahmekanon, der in § 11 Abs. 2 KDG abschließend aufgezählt ist, ist eine Weiterleitung von Patientendaten nur aus einer Einwilligung des Patienten abzuleiten.

Vielfach wird bei Aufnahme in ein Krankenhaus nach der Konfession gefragt. Gibt ein Patient an einer Konfession anzugehören, wird daraus die Einwilligung abgeleitet, den entsprechenden Krankenhausseelsorger informieren zu dürfen. Bereits die Abfrage der Konfession ist aber unzulässig, da es eine Rechtsgrundlage für diese Frage nicht gibt. Für die Behandlung des Patienten ist es unerheblich, welcher Religion oder Konfession er angehört. Es ist also bereits kein Zweck zu erkennen, der die Frage rechtfertigen kann.

Selbst wenn der/die Patient/in unter Hinweis auf die Freiwilligkeit dieser Angabe eine Konfession angegeben hat, ist daraus nicht zu schließen, dass er/sie in die Weitergabe dieses personenbezogenen Datums einwilligt. Eine informierte Einwilligung setzt voraus, dass die Umstände der Datenverarbeitung bekannt sind. Ein Besuch des/der Krankenhausseelsorgers ist deshalb nur auf der Grundlage einer konkreten Einwilligung möglich. Der/die Patient/in ist dazu im Aufnahmeformular direkt zu befragen:
„Sind Sie damit einverstanden, dass die Tatsache Ihres Aufenthaltes in unserem Haus einem/r Krankenhausseelsorger/in mitgeteilt wird?“

An den/die Krankenhausseelsorger/in welcher Konfession soll eine Mitteilung erfolgen?

Dem/der Krankenhausseelsorger/in dürfen dann nur die Kontaktdaten der/des Patienten/in mitgeteilt werden: Name, Vorname, Station.

8.2.8 Auskünfte der Rezeption des Krankenhauses

Wie oben bereits dargestellt, ist allein die Mitteilung über die Behandlung in einem Krankenhaus ein personenbezogenes Datum besonderer Kategorie. In einigen Krankenhäusern kommt es zu datenschutzrechtlichen Unkorrektheiten, wenn Besucher an der Rezeption nach der Aufenthaltsstation konkret von ihnen benannter Patienten fragen. In diesen Fällen ist schon nicht sicher, ob die Besucher tatsächlich wissen, ob sich der/die Benannte in dem Krankenhaus befinden oder ob es sich dabei nur um eine Vermutung handelt. Auch hier gilt es in jedem Fall das Persönlichkeitsrecht zu schützen. Eine Auskunft über den Aufenthalt in einem Krankenhaus oder einer Pflegeeinrichtung ist grundsätzlich nur bei Vorliegen einer Einwilli-

gungserklärung des/der Patientin zu erteilen. Auf der Einwilligungserklärung ist die Möglichkeit vorzusehen, den Kreis der Besuchsberechtigten etwa auf Familienangehörige oder namentlich genannte Personen zu beschränken.

8.2.9 Patientenarmbänder

Anlässlich einer Beratung mit betrieblichen Datenschutzbeauftragten von Krankenhäusern teilte eine Person aus dem Teilnehmerkreis mit, dass in ihrem Krankenhaus Patienten der Isolierstation verpflichtet seien, ein farbiges Patientenarmband zu tragen. Dies sei erforderlich, um diese Patienten im Krankenhausbetrieb zu erkennen und unverzüglich auf ihr Zimmer zurück zu bringen, wenn diese unerlaubt die Isolierstation verlassen hätten.

Patientenarmbänder sind gerade in großen Krankenhäusern ein probates Mittel, die Identität von Patienten sicherzustellen. Dem behandelnden Personal wird die Möglichkeit erleichtert nachzuvollziehen, ob der Patient, den sie vor sich haben, auch der Patient ist, dessen Patientenunterlagen sie in den Händen halten. So können Verwechslungen leichter vermieden werden, insbesondere z. B. bei Patienten, die nur eingeschränkt in der Lage sind, zu kommunizieren.

Bei der Verwendung von Patientenarmbändern muss aber sichergestellt sein, dass durch diese selbst nicht schon Daten an unberechtigte Dritte bekannt gegeben werden. Das ist jedoch der Fall, wenn aus den Farben der Patientenbänder die Abteilung erkennbar ist, in der der/die Patient/in untergebracht ist. So weiß in dem dargestellten Fall jeder, dass der Patient an einer infektiösen Krankheit leidet. Auch wenn dies aus Sicherheitsgründen zunächst durchaus erstrebenswert erscheinen mag, ist aus datenschutzrechtlicher Sicht zu fragen, ob nicht eine mildere oder andere Maßnahme den Zweck erreicht ohne personenbezogene Daten besonderer Kategorie mitzuteilen. Vorliegend erscheint es sinnvoller und dem Zweck angemessener, die Isolierstation so zu organisieren, dass dem infektiösen Patienten ein Verlassen nicht möglich ist.

Auch sonst dürfen Patientenarmbänder nur solche Informationen enthalten, die für einen vorher festgelegten Zweck erforderlich sind. Der vorher

festgelegte Zweck ist die Identifizierung. Demnach dürfen auf dem Armband nur der Name, Vorname, das Geburtsdatum und ggf. die Abteilung gespeichert sein.

8.2.10 Akteneinsicht nur gegen Kopie des Personalausweises?

Eine Petentin stelle einen Antrag auf Einsicht in ihre Patientenakte an das Krankenhaus, in dem sie behandelt worden ist. Daraufhin wurde ein Termin mit ihr vereinbart. Bei dem Termin wurde die Petentin aufgefordert, ihren Personalausweis vorzulegen, damit eine Kopie erstellt werden kann. Ohne eine Kopie des Personalausweises sei eine Einsicht in die Patientenakte nicht möglich.

Die Petentin fragt an, ob dies rechtmäßig sei.

Ein Personalausweis enthält typischer Weise personenbezogene Daten. Namen, Vornamen, Geburtsort, Geburtstag, Größe, Augenfarbe, Adresse.

Die Kopie eines Dokumentes mit personenbezogenen Daten stellt eine Verarbeitung personenbezogener Daten gem. § 4 Nr. 3 KDG in Form der Erhebung, Erfassung bzw Speicherung dar.

Eine solche Verarbeitung ist nur rechtmäßig, wenn eine der Bedingungen des § 6 Abs. 1 KDG erfüllt ist. Hier könnte die Verarbeitung erforderlich sein, um einer rechtlichen Verpflichtung nachkommen zu können. Die §§ 14 ff. KDG legen für den Verantwortlichen Auskunftsverpflichtungen fest. Danach ist Patienten auch ein Einsichtsrecht in die Patientenakte zu gewähren. § 17 Abs. 3 KDG legt fest, dass der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind zur Verfügung stellt. § 630g BGB gewährt Patienten ein unverzügliches Einsichtsrecht in ihre Patientenakte. Der Verantwortliche ist also rechtlich verpflichtet, der Patientin eine Akteneinsicht zu gewähren. Allerdings lässt sich daraus ein Recht oder sogar eine Pflicht den Personalausweis der Patientin zu kopieren nicht herleiten. Zwar muss der Verantwortliche in diesem Fall die Identität der Patientin feststellen, dem ist aber mit Vorlage und Kontrolle des Personalausweises genüge getan. Weder legt das Gesetz dem Verantwortlichen die Pflicht auf, mit der Kopie eines Dokumentes die durchge-

führte Identitätskontrolle nachzuweisen, noch wird der betroffenen Person die Pflicht auferlegt eine Identitätsdokument in Kopie abzugeben. Durch die Regelung des Krankenhauses wird der Auskunftsanspruch von einer im Gesetz nicht geregelten zusätzlichen Bedingung abhängig gemacht bzw. erschwert. Das ist unzulässig. Die Petentin hat einen Anspruch auf sofortige Vernichtung der Personalausweiskopie.

Das Krankenhaus wurde aufgefordert die Vernichtung der Kopie sofort durchzuführen und ihre Regeln dahingehend zu ändern, dass eine Identitätsfeststellung ohne eine Kopie des Personalausweises erfolgt.

Im vorliegenden Fall war nicht zu entscheiden, wie bei einer schriftlichen Anfrage zu verfahren ist.

Um sicherzustellen, dass Auskunftsbegehren von nicht berechtigten Personen gestellt werden, kann zum Nachweis der Legitimation die schriftliche Vorlage einer Ausweiskopie gefordert werden. Von diesen werden aber „regelmäßig nur Name, Anschrift, Geburtsdatum und Gültigkeitsdauer benötigt“ die weiteren Angaben dürfen und sollten vom Antragsteller geschwärzt werden.

Auch in diesem Fall ist es selbstverständlich, dass die Daten auf der Ausweiskopie einer strengen Zweckbindung unterliegen und ausschließlich zur Identitätsprüfung verwendet werden, nicht aber in den Datenbestand der verantwortlichen Stelle einfließen dürfen.

Bei einer Anfrage per E-Mail ist das Abverlangen einer Kopie des Personalausweises auch dann problematisch, wenn, wie oben dargestellt, weitere Angaben geschwärzt sind. Auch bei den verbleibenden Angaben handelt es sich um personenbezogene Daten. Solche unverschlüsselt per E-Mail zu übermitteln, verstößt gegen datenschutzrechtliche Grundregeln. In diesem Fall hat also der Verantwortliche einen sicheren Zugangsweg bereitzustellen. Dies kann in Form der Bereitstellung eines öffentlichen Schlüssels des Verantwortlichen, mit dem die betroffene Person die Ausweiskopie Ende-zu-Ende-verschlüsselt per E-Mail übermitteln kann, geschehen. Ebenso kommt die Bereitstellung eines Links zu einer HTTPS-geschützten Website in Betracht, über die die betroffene Person die Ausweiskopie (ohne weitere selbst zu ergreifende Maßnahmen) sicher an den Verantwortlichen übermitteln kann.

8.3 Beschäftigtendatenschutz

8.3.1 Zulässigkeit der Frage nach Religionszugehörigket

In Folge der Rechtsprechung des Europäischen Gerichtshofs darf die Religionszugehörigkeit als Voraussetzung für eine Einstellung nicht mehr für jede Stelle pauschal verlangt werden. Der EuGH verlangt dagegen einen objektiv überprüfbaren direkten Zusammenhang zwischen der Religionszugehörigkeit und der fraglichen Tätigkeit. Dieser kann sich aus der Art der Tätigkeit (z. B. Aufgaben der Verkündigung) oder aus den Umständen ihrer Ausübung ergeben. Dies wird insbesondere bei Leitungspositionen der Fall sein, in denen der Amtsinhaber die Position der Kirche glaubwürdig vertreten muss (etwa Leitung einer katholischen Kindertagestätte oder anderer kirchlicher Einrichtungen). Eine generelle Abfrage der Religionszugehörigkeit unabhängig von der zu besetzenden Stelle ist unzulässig.[26]

8.3.2 Namensschilder im dienstlichen Kontext, insbesondere an der Dienstkleidung

Aus einem Krankenhaus ist eine Beschwerde aus dem Kreis der Mitarbeiter eingegangen. Darin wird auf ein Verfahren verwiesen, welches in dem Haus im Hinblick auf die Angaben von Namen auf, bzw. an der Dienstkleidung praktiziert wird. Eine Anweisung an die Mitarbeitenden verpflichtet diese, sich zu entscheiden, ob sie auf den verpflichtend zu tragenden Namensschildern Vor- und Zuname oder alternativ die Personalnummer angeben wollen.

Bereits in früheren Tätigkeitsberichten war dieses Thema Gegenstand von Erörterungen[27].

Vorname, Zuname und Personalnummer sind jeweils einzeln „personenbezogene Daten“ im Sinne des § 4 Nr. 1 KDG.

Die Verpflichtung solche personenbezogenen Daten an Dritte bekannt zu geben stellt eine „Verarbeitung“ im Sinne des § 4 Nr. 3 KDG dar.

26 Amtsblatt Bistum MD 2019/Nr. 7, Nr. 78
27 TB 2017 Punkt 7.3.4.

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn eine der Bedingungen des § 6 Abs. 1 lit a – g KDG vorliegt.

Weiterhin müssen auch bei einer rechtmäßigen Verarbeitung die Grundsätze der Verarbeitung personenbezogener Daten gem. § 7 KDG eingehalten werden.

Das Tragen von Namensschildern in einem Krankenhaus entspricht sozialer bzw. gesellschaftlicher Üblichkeit und dient damit grundsätzlich der Wahrung des berechtigten Interesses des Verantwortlichen (also des Krankenhauses). Dies gilt allerdings nur soweit, wie die Persönlichkeitsrechte des Betroffenen (also des Mitarbeiters) nicht überwiegen.

Die Persönlichkeitsrechte des Betroffenen überwiegen dann, wenn die Grundsätze der Verarbeitung personenbezogener Daten nicht eingehalten werden.

Der Zweck der Verpflichtung Namensschilder zu tragen, dürfte zum einen darin bestehen, ein persönliches Verhältnis zwischen Patienten und Personal aufzubauen. Weiterhin dürfte ein Grund darin bestehen, mögliche Beschwerden oder Belobigungen des Patienten konkretem Personal zuordnen zu können.

Für die Erreichung dieses Zwecks ist die Verarbeitung von personenbezogenen Daten auf das notwendige Maß (§ 7 Abs. 1 lit. c) KDG) zu beschränken. Je nach Gepflogenheit in der Einrichtung ist die Angabe des Nachnamens oder des Vornamens dafür ausreichend. Die Bekanntgabe weiterer personenbezogener Daten, also des vollständigen Vor- und Zunamens, ist zur Zweckerreichung nicht erforderlich und damit unzulässig.

Die Angabe der Personalnummer ist bereits nicht geeignet den Zweck –Aufbau eines persönlichen Verhältnisses- zu erreichen. Außerdem liegt es auf der Hand, dass Patienten das Personal trotzdem mit Namen benennen werden, da eine Ansprache von Personen nur unter einer Personalnummer unüblich (wenn nicht weltfremd) ist. Muss der Betroffene aber aufgrund des sozialen, gesellschaftlichen Umgangs seinen Vor- oder Nachnamen ohnehin bekannt geben, stellt die weitere Verarbeitung der Personalnummer eine überflüssige Bekanntgabe personenbezogener Daten dar. Die Ver-

pflichtung zur Angabe der Personalnummer anstelle des Namens auf dem entsprechenden Schild ist also ebenfalls unzulässig.

8.3.3 Namensnennung im öffentlichen Telefonverzeichnis

Aus einem Ordinariat wurde angefragt, ob der Dienstgeber berechtigt sei, Vor- und Zunamen, die dienstliche Telefonnummer sowie die dienstliche E-Mailadresse im Internet zu veröffentlichen.

Zunächst ist festzustellen, dass es sich bei Vor- und Zunamen um personenbezogene Daten des/der Mitarbeiter/in handelt.

Ein Dienstgeber ist grundsätzlich befugt die organisatorische Struktur seiner Einrichtung zu regeln. Daraus ergibt sich auch, dass der Dienstgeber ohne ausdrückliche gesetzliche Ermächtigung berechtigt ist, dem außenstehenden Benutzer, für dessen Bedürfnisse die Einrichtung eingerichtet worden ist, einen Hinweis darauf zu geben, welche natürlichen Personen mit der Erfüllung einer bestimmten Aufgabe betraut und damit in einer auf Außenkontakt gerichteten Einrichtung für das Publikum der zuständige Ansprechpartner sind. Diese Feststellung gilt grundsätzlich unabhängig davon, auf welchem Weg die Einrichtung die Ansprechpersonen veröffentlicht. Auch eine Veröffentlichung in moderner Weise durch entsprechende Verlautbarungen auf der Internetseite liegt im organisatorischen Ermessen des Dienstgebers. Der Dienstgeber kann bestimmen, ob und gegebenenfalls auf welche Weise er die tatsächliche Erreichbarkeit seiner Mitarbeiter/innen durch Außenstehende sicherstellen will. Kein/e Mitarbeiter/in hat Anspruch darauf, von Publikumsverkehr und von der Möglichkeit, postalisch oder elektronisch von außen mit ihm Kontakt aufzunehmen, abgeschirmt zu werden, es sei denn, legitime Interessen z.B. der Sicherheit gebieten dies.

Demgegenüber dürfen die Rechte Mitarbeitender aber nicht unberücksichtigt bleiben. Der Dienstgeber ist gehalten, personenbezogene Daten der Beschäftigten nur insoweit zu verarbeiten, als diese zur Erfüllung des Zwecks erforderlich sind. Daraus ergibt sich zunächst die Forderung, nur die Personen in einem, im Internet zugänglichen Telefonverzeichnis aufzu-

führen, die ansprechbar für externe Benutzer oder Klienten der Einrichtung sein sollen. Mitarbeiter/innen, deren Arbeitsgebiet sich ausschließlich auf die innere Verwaltung der Einrichtung bezieht fallen nicht darunter (Hausmeister, Buchhaltung u. ä.). Weiterhin sind die personenbezogenen Daten der Mitarbeiter/innen, die veröffentlicht werden dürfen auf das notwendige Maß zu beschränken. Die Angabe des Vornamens ist deshalb regelmäßig unzulässig, weil diesbezüglich keine Erforderlichkeit besteht. Selbst eine Verwechslungsgefahr bei Namensdopplungen dürfte durch die Beifügung des Aufgabengebietes bestenfalls selten vorkommen.

Bei der Nennung des Nachnamens, der Dienstbezeichnung, der dienstlichen Telefonnummer und der dienstlichen E-Mail-Adresse Mitarbeitender, die durch ihre Arbeitsaufgabe die Einrichtung nach außen vertreten, überwiegt das Interesse des Dienstgebers an einer Funktion der Einrichtung das Interesse Mitarbeitender auf Schutz dieser personenbezogenen Daten .

8.3.4 GPS in Dienstfahrzeugen

Bereits im letzten Tätigkeitsbericht wurde darauf hingewiesen, dass die Überwachung von Dienstfahrzeugen mit Hilfe von GPS (Global Positioning System) nur unter strengen Voraussetzungen möglich ist.[28]

Nunmehr hat eine Entscheidung des Niedersächsischen Verwaltungsgerichtes die diesbezügliche Rechtsauffassung bestätigt.

Das Verwaltungsgericht hatte einem Unternehmen untersagt, zukünftig weiterhin eine GPS-Überwachung seiner Dienstfahrzeuge durchzuführen.

Das Unternehmen hatte vorgetragen, die Ortung sei betrieblich notwendig, um Touren zu planen, Mitarbeiter und Fahrzeuge zu koordinieren, Nachweise gegenüber den Auftraggebern zu erbringen, Diebstahlsschutz zu gewährleisten und eventuell gestohlene Fahrzeuge aufzufinden.

Das Verwaltungsgericht ist diesem Vortrag nicht gefolgt.

Unsere Dienststelle sieht sich auch aufgrund dieses Urteils in ihrer Rechtsauffassung unterstützt. GPS-Systeme werden häufig im mobilen Pflegedienst eingesetzt. Die Argumentation der Verantwortlichen entspricht

28 3. TB 4.9. Seite 37

dabei in der Regel der oben dargestellten. Diese Darlegungen können aber datenschutzrechtlich nicht überzeugen.

Die Tourenplanung ist zukunftsorientiert. Informationen über aktuelle und vergangene Standorte der Einrichtungsfahrzeuge sind planungsunerheblich.

Für eine womöglich außerplanmäßig (z.B. infolge von Krankheitsausfällen, Staus, Unfällen) akut werdende zentrale Koordination von Mitarbeitern und Fahrzeugen würde als weniger stark eingreifende Maßnahme die Gewährleistung einer Erreichbarkeit von Mitarbeitern per Mobiltelefon genügen.

Ein Nachweis über Tätigkeiten am/im Objekt eines Klienten kann mittels Ortungsdaten nicht geführt werden. Über diese Daten könnte allenfalls nachgewiesen werden, dass ein bestimmtes Firmenfahrzeug am Objekt bzw. in der Nähe des Klienten für einen bestimmten Zeitraum anwesend gewesen ist. Somit ist die Erfassung solcher Daten zur Erreichung des Zwecks völlig ungeeignet.

Weiterhin sind Ortungssysteme für präventiven Diebstahlsschutz völlig ungeeignet. Für das Wiederauffinden womöglich entwendeter Firmenfahrzeuge reicht die anlassbezogene Erhebung im Falle eines festgestellten Fahrzeugverlustes aus.[29]

Demgegenüber sieht sich der Mitarbeiter im Falle einer GPS-Überwachung des Dienstfahrzeuges einer anlasslosen Überwachung ausgesetzt, durch die ein permanenter Kontrolldruck entsteht. Für derartige Kontrollen bedarf es aber konkreter tatsächlicher Anhaltspunkte.

8.3.5 Kopie des Führerscheins

Ein Petent beschwerte sich über eine Regelung seines Arbeitgebers, nach der Mitarbeitende die Dienstfahrzeuge nutzen möchten bzw. müssen, vor der ersten Nutzung eine Kopie des Führerscheins beim Arbeitgeber einzureichen haben.

Der Führerschein enthält personenbezogene Daten. Neben dem Vor- und Zunamen auch das Geburtsdatum und den Geburtsort. Außerdem ein Foto.

29 VG Lüneburg, Teilurteil vom 19.03.2019 – 4 A 12/19

Die Anfertigung einer Kopie stellt eine Verarbeitung i. S. v. § 4 Nr 3 KDG dar. Eine solche Verarbeitung ist nur dann zulässig, wenn eine der Bedingungen des § 6 Abs. 1 KDG gegeben ist. In Betracht kommt hier § 6 Abs. 1 lit. d), wenn der Arbeitgeber mit der Verarbeitung eine rechtliche Verpflichtung erfüllt. Nach

§ 21 Abs. 1 Nr. 2 StVG darf der Arbeitgeber seine Fahrzeuge nicht Personen überlassen, die keine Fahrerlaubnis besitzen:

> *„Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer*
>
> *1. …*
>
> *2. als Halter eines Kraftfahrzeugs anordnet oder zulässt, dass jemand das Fahrzeug führt, der die dazu erforderliche Fahrerlaubnis nicht hat oder dem das Führen des Fahrzeugs nach § 44 des Strafgesetzbuchs oder nach § 25 dieses Gesetzes verboten ist."*

Diese Vorschrift verpflichtet den Arbeitgeber sich bei jeder Inanspruchnahme eines Dienstfahrzeuges davon zu überzeugen, dass der Betroffene über eine gültige Fahrerlaubnis verfügt. Mit einer einmaligen Kopie des Führerscheines vor der ersten Benutzung eines Dienstfahrzeuges wird dieser Zweck aber nicht erfüllt, da dem Mitarbeiter inzwischen seine Fahrerlaubnis dauerhaft oder zeitweise entzogen worden sein kann. Daraus ist nun nicht zu schließen eine Kopie bei jeder Entleihung für erforderlich zu halten. Vielmehr steht dem Arbeitgeber als milderes Mittel die bloße Einsichtnahme in das Dokument zu, die mit einem Vermerk festgehalten wird.[30]

Da zumindest eine Erforderlichkeit für eine Kopie nicht gegeben ist, war der Arbeitgeber zu beauflagen, das dargelegte Verfahren einzustellen.

8.3.6 Anschwärzen unter Mitarbeitern

Uns erreichte eine Anfrage einer Mitarbeitervertretung (MAV) einer Schule. Darin wurde dargestellt, dass ein Lehrer seit einem längeren, nicht näher bestimmbaren Zeitraum, schriftlich über Kollegen und Vorgesetzte Auslassungen verfasst. Diese Schreiben werden an die Schulverwaltung im

30 Bremer LBfD 38. TB 2018 S. 38

Bischöflichen Ordinariat geschickt. Bei einem Personalgespräch wurde ein Mitarbeiter auf diese Berichte angesprochen. Weil an diesem Gespräch auch eine Vertreterin der MAV teilnahm, wurde der Sachverhalt der MAV bekannt. Dabei stellte sich heraus, dass sich inzwischen mehrere tausend Seiten angesammelt haben. Die Schulverwaltung verwahrt die Ausführungen des Lehrers in dessen Personalakte auf. Die von den Ausführungen betroffenen Lehrer, bzw. Mitarbeiter wurde weder vom Vorliegen solcher Berichte noch über die Inhalte in Kenntnis gesetzt.

Nach der Rechtsprechung des BAG sind Personalakten Sammlung von Urkunden und Vorgängen, die die persönlichen und dienstlichen Verhältnisse des Mitarbeiters betreffen und in einem engen Zusammenhang mit seinem Dienstverhältnis stehen. Außerdem hat das BAG festgestellt, dass nicht nur der Teil einer Personalakte eine solche ist, die der Arbeitgeber auch tatsächlich als Personalakte bezeichnet und führt (formelle Personalakte). Vielmehr sind auch Urkunden und Vorgänge, die die persönlichen und dienstlichen Verhältnisse des Bediensteten betreffen und in einem inneren Zusammenhang mit dem Dienstverhältnis stehen, Bestandteil der Personalakte.[31] Generell dürfen Personalakten nur Informationen enthalten, die der Arbeitgeber rechtmäßig erworben hat und für die ein sachliches Interesse des Arbeitgebers besteht.[32]

Vor dem Hintergrund dieser Rechtslage erscheint die von der Schulabteilung praktizierte Verarbeitung der „Mitteilungen" eines Kollegen über andere Kollegen unzulässig.

Werden Daten verarbeitet gelten die Grundsätze der Datenverarbeitung gem. § 7 KDG. Dabei ist es unerheblich, auf welchem Weg der Verantwortliche die Daten erhalten hat. Zunächst gehören die über die Lehrer mitgeteilten „Informationen" grundsätzlich in die Personalakte der betroffenen Lehrer.

Für die betroffene Person müssten die Daten gem. § 7 Abs. 1 lit. a) rechtmäßig und in einer nachvollziehbaren Weise verarbeitet werden. Dies war in dem praktizierten Verfahren nicht der Fall, da die Kollegen über die die „Informationen" mitgeteilt worden sind, darüber nicht informiert wurden

31 BAG, Urt. v. 7.5.1980 –4 AZR 214/78
32 BAG, Urt. v. 13.04.1988 -5 AZR 537/86

und somit auch nicht nachvollziehen konnten, welche Daten über sie zu welchem Zweck verarbeitet werden.

Bei den „Informationen" über andere Lehrer, die ein Kollege an die Schulverwaltung geschickt hat, handelt es sich um personenbezogene Daten. Die Speicherung der Daten stellt eine Verarbeitung i. S. d. § 4 Nr. 3 KDG dar. Die Verarbeitung solcher Daten ist nur zulässig, wenn ein bestimmter, vorher festgelegter, rechtmäßiger Zweck verfolgt wird.

Vorliegend ist für die Verarbeitung dieser Daten ein Zweck nicht bestimmt. Deshalb ist eine Verarbeitung dieser Daten unzulässig.

Darüber hinaus wäre die Schulverwaltung verpflichtet gewesen, den Auskunfts- und Informationsverpflichtungen der §§ 14, 16 KDG nachzukommen.

Die Schulverwaltung war aufzufordern, den betroffenen Lehrern die über sie gespeicherten Daten unverzüglich zugänglich zu machen und ihnen die Möglichkeit einer Stellungnahme einzuräumen.

Soweit die Richtigkeit der „Mitteilungen" nicht belegbar sind, sind die Unterlagen unverzüglich zu entsorgen.

Bei weiteren Vorgängen der beschriebenen Art ist wohl auch ein disziplinarisches Vorgehen gegen den Schreiber erforderlich.

8.3.7 Nutzung privater Endgeräte für dienstliche Zwecke (BYOD)

Die Mitarbeitervertretung (MAV) einer Schule fragte uns, ob von den Mitarbeitern eine Abfrage der Direktorin zu beantworten sei. Die Anfrage richtete sich auf die „Verarbeitung von personenbezogenen Daten der Schule durch Lehrkräfte zu dienstlichen Zwecken auf privaten Endgeräten".

In einzelnen Anstrichen wurde gefragt

- welche privaten Endgeräte benutzt werden
- wer Zugang zu dem Gerät hat und ob es passwortgeschützt sei

- ob auf dem Endgerät ein eigenes für dienstliche Zwecke angelegtes Benutzerkonto eingerichtet sei
- wie personenbezogene Daten gespeichert würden
- welches Betriebssystem benutzt würde.

Seit dem 1. März 2019 ist die Durchführungsverordnung zum KDG (KDG-DVO) in Kraft getreten. Die von der MAV aufgeworfene Frage findet dort in § 20 Beantwortung.

§ 20 Nutzung privater IT-Systeme zu dienstlichen Zwecken

(1) Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu dienstlichen Zwecken ist grundsätzlich unzulässig. Sie kann als Ausnahme von dem Verantwortlichen unter Beachtung der jeweils geltenden gesetzlichen Regelungen zugelassen werden.

(2) Die Zulassung erfolgt schriftlich und beinhaltet mindestens

a) die Angabe der Gründe, aus denen die Nutzung des privaten IT-Systems erforderlich ist,

b) eine Regelung über den Einsatz einer zentralisierten Verwaltung von Mobilgeräten (z.B. Mobile Device Management) auf dem privaten IT-System des Mitarbeiters,

c) das Recht des Verantwortlichen zur Löschung durch Fernzugriff aus wichtigem und unabweisbarem Grund; ein wichtiger und unabweisbarer Grund liegt insbesondere vor, wenn der Schutz personenbezogener Daten Dritter nicht auf andere Weise sichergestellt werden kann,

d) eine jederzeitige Überprüfungsmöglichkeit des Verantwortlichen,

e) die Dauer der Nutzung des privaten IT-Systems für dienstliche Zwecke,

f) das Recht des Verantwortlichen festzulegen, welche Programme verwendet oder nicht verwendet werden dürfen sowie

g) die Verpflichtung zum Nachweis einer Löschung der zu dienstlichen Zwecken verarbeiteten personenbezogenen Daten, wenn die

Freigabe der Nutzung des privaten IT-Systems endet, das IT-System weitergegeben oder verschrottet wird.

Ergänzend ist dem betreffenden Mitarbeiter eine spezifische Handlungsanweisung auszuhändigen, die Regelungen zur Nutzung des privaten IT-Systems enthält.

(3) Der Zugang von privaten IT-Systemen über sogenannte webbasierte Lösungen kann mit den Mitarbeitern vereinbart werden, soweit alle datenschutzrechtlichen Voraussetzungen für eine sichere Nutzung gegeben sind.

(4) Die automatische Weiterleitung dienstlicher E-Mails auf private E-Mail-Konten ist in jedem Fall unzulässig.

Aus dieser Regelung ist zu ersehen, dass die dienstliche Nutzung privater Endgeräte nur im Ausnahmefall zulässig ist.

Wenn ausnahmsweise die Nutzung privater Endgeräte durch den Vorgesetzten erlaubt wird, was einer ausdrücklichen schriftlichen Genehmigung bedarf, sind die in § 20 KDG-DVO benannten Punkte vorher (!) zu regeln.

Die den Mitarbeitenden von der Vorgesetzten zur Beantwortung vorgelegten Fragen waren grundsätzlich sachgemäß und zu beantworten. Je nachdem wie diese Fragen beantwortet werden, wäre bei entsprechender Konstellation die private Nutzung sofort zu untersagen (z. B. wenn auch andere Personen Zugang zum Gerät haben und kein Passwort vergeben ist).

Grundsätzlich kann kein Arbeitnehmer verpflichtet werden, private Endgeräte für dienstliche Zwecke zu verwenden. Die Bereitstellung von Arbeitsmaterial ist Verpflichtung des Arbeitgebers. Wenn die Arbeitnehmer dennoch ihr eigenes Gerät benutzen möchten, muss es dafür konkrete Gründe geben. Außerdem ist die oben bezeichnete Erlaubnis erforderlich. Vorliegend war festzustellen, dass die Fragen der Vorgesetzten zwar in die richtige Richtung wiesen, aber längst nicht ausreichend waren, um die Voraussetzungen der KDG-DVO zu erfüllen.

Die MAV wurde auf ihre Verpflichtung aus der Mitarbeitervertretungsordnung hingewiesen, wonach sie darauf zu achten hat, dass alle Mitarbeiter/

innen nach Recht und Billigkeit behandelt werden. Unter diese Verpflichtung fällt es, alle Grundsätze des Rechts die das Arbeitsverhältnis gestalten und auf es einwirken zu wahren. Insoweit sollte bereits die MAV den Dienstgeber darauf hinweisen, dass die von ihm im Hinblick auf die zur Verwendung privater Endgeräte praktizierte Lösung den datenschutzrechtlichen Vorschriften nicht entspricht.

Aus aufsichtlicher Perspektive ist der Dienstgeber ebenfalls auf die Rechtslage verwiesen worden unter der Anordnung, kurzfristig einen rechtmäßigen Zustand herbeizuführen.

8.3.8 Datenschutz und Arbeitszeiterfassung

Der Europäische Gerichtshof (EuGH) hat am 14. Mai 2019 entschieden (Az: C-55/18), dass Arbeitgeber zukünftig dazu angehalten werden sollen, Systeme einzurichten, mit denen die täglich geleisteten Arbeitszeiten ihrer Mitarbeiter zuverlässig gemessen werden können.

Der Hintergrund dieser Entscheidung bestand darin, dass mit Mitarbeitenden eine „Vertrauensarbeitszeit" bzw. eine vermeintlich großzügige Gleitzeitregelung vereinbart worden ist, die Mitarbeiter/innen für die Erledigung der ihnen zugewiesenen Arbeitsaufgaben aber deutlich mehr Arbeitszeit aufwenden mussten als arbeitsvertraglich vereinbart. Da die Arbeitszeit aber nicht erfasst worden ist, konnte geleistete Mehrarbeit von den Beschäftigten nicht belegt und damit rechtswirksam gegenüber dem Arbeitgeber geltend gemacht werden.

Nunmehr kann jede/r Mitarbeiter/in darauf bestehen, dass seine/ihre Arbeitszeit erfasst wird.

Dem Arbeitgeber sind dazu keine bestimmten Erfassungssysteme vorgeschrieben. Jedoch ist bei Einführung solcher Systeme auf eine datenschutzkonforme Regelung zu achten.[33]

Insbesondere ist dabei zu berücksichtigen, dass es sich hierbei um personenbezogene Daten handelt, die Dritten grundsätzlich zugänglich nicht gemacht werden dürfen. Listen oder Kladden, in denen sich die Mitarbei-

33 Ausführlich dazu Ullrich in ZMV 2019, Seite 181 ff.

ter/innen beim Kommen und Gehen eintragen und die allen anderen somit zugänglich sind, entsprechen diesen Anforderungen nicht. Auch solche Systeme, die einen permanenten Zugriff für Vorgesetzte zulassen, sind aufgrund der damit bestehenden Unverhältnismäßigkeit unzulässig.

Bei Einführung von Zeiterfassungssystemen sind die Beschäftigten gem. §§ 14 ff. KDG zu unterrichten.

8.3.9 Versendung personenbezogener Daten an einen Gruppenaccount

Ein Petent beschwerte sich darüber, von der Verantwortlichen seines Dienstgebers zur Teilnahme an einem Gespräch im Rahmen des Betrieblichen Eingliederungsmanagements (BEM) gem. § 167 SGB IX per E-Mail über einen Gruppenaccount eingeladen worden zu sein. Auf diese Weise hätten mindestens zehn weitere Mitarbeiter/innen von diesem Termin Kenntnis erlangt, weil diese ebenfalls zu diesem Gruppenaccount gehören.

Nach dieser Vorschrift soll ein Arbeitgeber allen Beschäftigten, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig gewesen sind, ein BEM anbieten.

Die Mitteilung, dass ein BEM-Gespräch stattfinden soll, enthält personenbezogene Daten besonderer Kategorie gem. § 4 Nr. 2 KDG, weil daraus Gesundheitsdaten gem. § 4 Nr. 17 KDG hervorgehen, eben mindestens die Tatsache, dass der Mitarbeiter in den vergangenen 12 Monaten mehr als sechs Wochen arbeitsunfähig krank gewesen ist.

Eine Verarbeitung ist gem. § 4 Nr. 3 KDG u. a. gegeben, wenn eine Offenlegung durch Übermittlung erfolgt.

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist gem. § 11 Abs. 1 KDG untersagt. Eine Ausnahme gilt nur, wenn einer der Fälle des § 11 Abs. 2 KDG gegeben ist. Das Bestehen einer solchen Ausnahme ist von keiner Seite vorgetragen worden. Bei der Einrichtung bestand eine Verfahrensregelung, nach der Terminvereinbarung zum BEM mit dem betreffenden Mitarbeiter „direkt vor Ort“ abzusprechen sind. Über diese bestehende Regelung hat sich die einladende Mitarbeiterin hinwegge-

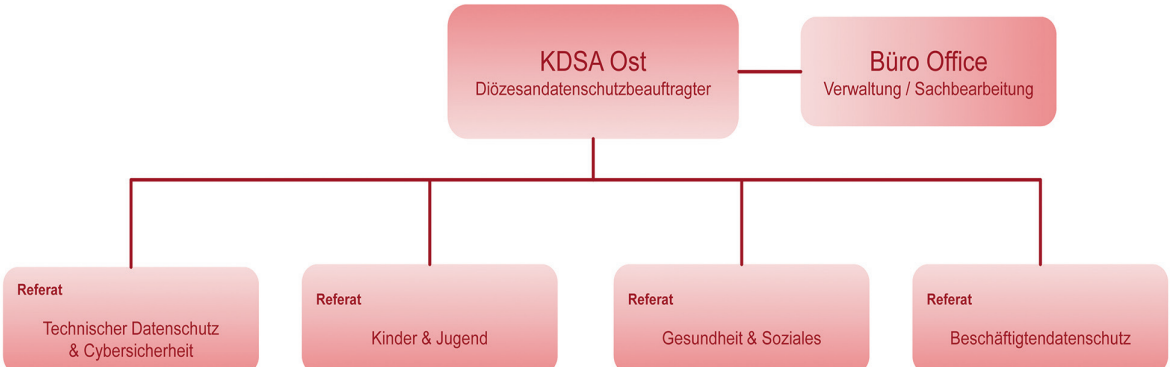
setzt. Da die Mitarbeiterin ausweislich der Einlassung der Einrichtungsleitung zum Kreis der Bereichsleitungen gehört, der zum Thema Datenschutz geschult ist und wiederholt auf den sensiblen Umgang mit personenbezogenen Daten verpflichtet wurde, war von einer mindestens grob fahrlässigen Handlung auszugehen. Da es sich zusätzlich um die Verarbeitung von personenbezogenen Daten besonderer Kategorie gem. § 4 Nr. 2 KDG, da Gesundheitsdaten gem. § 4 Nr. 17 KDG betroffen waren, handelte, wurde gegen die Einrichtung ein Bußgeld verhängt.

Die Kirchliche Datenschutzaufsicht Ost

KDSA Ost als Dienststelle

Die Kirchliche Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs mit Sitz in Schönebeck/Elbe unter Leitung des Diözesandatenschutzbeauftragten ist die zuständige Datenschutzaufsichtsbehörde für die ostdeutschen Bistümer und ihren Einrichtungen. Die kirchliche Datenschutzaufsicht ist oberste Dienstbehörde im Sinne des § 96 Strafprozessordnung und oberste Aufsichtsbehörde im Sinne des § 99 Verwaltungsgerichtsordnung.

Organisation/Dienststelle der KDSA Ost



Unsere Aufgaben und Befugnisse

Die kirchlichen Datenschutzaufsichtsbehörden haben zunächst die Aufgabe, die Einhaltung der Gesetze zum Datenschutz zu kontrollieren und bei Nichteinhaltung mit entsprechenden Sanktionen zu reagieren. **Bei Verstößen gegen die Bestimmungen des KDG sowie der KDG-DVO kann die Datenschutzaufsicht eine Geldbuße verhängen.**

Im Rahmen des Zuständigkeitsbereichs ergeben sich eine Reihe von weiteren Aufgaben (§ 44 KDG). Dazu gehören u.a.

- Die Durchführung von Untersuchungen in Form von Datenschutzüberprüfungen auch auf der Grundlage von Informationen einer anderen Datenschutzaufsicht oder einer anderen Behörde.
- Die Durchführung von Untersuchungen im Rahmen der technischen und organisatorischen Maßnahmen sowie zum Stand der Technik (KDG-DVO).
- Die Bearbeitung gemeldeter Beschwerden und gemeldeter Datenschutzvorfälle.
- Die Erstellung eines jährlichen Tätigkeitsberichts welcher u.a. Entwicklungen des Datenschutzes im nichtkirchlichen Bereich enthält.

Eine weitere Aufgabe ist die Durchführung von Untersuchungen im Rahmen der technischen und organisatorischen Maßnahmen sowie zum Stand der Technik (KDG-DVO), u.a. auch das Verfolgen zu Entwicklungen der Informations- und Kommunikationstechnologie soweit sie sich die Informationssicherheit auswirken.

Anhang

Lebenszyklus einiger Microsoft Produkte

Auszug aus der Liste von Microsoft Produkten, die im Jahr 2020 auslaufen oder das Ende des Supports erreichen. Nach Ablauf oder Ende des Supports werden keine neuen Sicherheitsupdates, nicht sicherheitsrelevante Updates, kostenlose oder kostenpflichtige Support-Optionen oder Online-Updates technischer Inhalte mehr angeboten. Eine vollständige Liste aller Produkte kann auf der Website von Microsoft (Microsoft Lifecycle-Richtlinie) eingesehen werden. Zu beachten sind dort die verschiedenen Richtlinien wie „Moderne Richtlinie“ und „Feste Richtlinie“ und die Produkte, die zum Erweiterten Support wechseln.

Liste ausgewählter Produkte aus der Rubrik „Feste Richtlinie“:

Ende des Supports am 14.01.2020

Hyper-V Server 2008
Hyper-V Server 2008 R2
Windows 7
Windows Server 2008 R2
Windows Server 2008
Windows Storage Server 2008 (alle Editionen)

Ende des Supports am 31.01.2020

Internet Explorer 10

Ende des Supports am 08.09.2020

Access Services in Microsoft SharePoint Server 2010
Excel Services in Microsoft SharePoint Server 2010
Access 2010
Dynamics GP 2010
Excel 2010
Excel Home & Student 2010
Microsoft Excel Mobile 2010
Microsoft Expression Studio 4

InfoPath 2010
Office 2010 (alle Editionen)
OneNote 2010
OneNote Home & Student 2010
Outlook 2010
Outlook 2010 mit Business Contact Manager
PowerPoint 2010
PowerPoint Home & Student 2010
Project 2010
Project Professional 2010
Project Server 2010
Microsoft Publisher 2010
Suchserver 2010
SharePoint 2010 for Internet Sites Enterprise
SharePoint 2010 for Internet Sites Standard
SharePoint Designer 2010
SharePoint Foundation 2010
SharePoint Server 2010
SharePoint Server 2010 Service Pack 2
SharePoint Workspace 2010
System Center Data Protection Manager 2010
System Center Essentials 2010
Visio 2010
Visio Professional 2010
Visio Standard 2010
Visual Basic 2010 Express
Word 2010
Word Home & Student 2010
Windows Embedded Standard 7
Excel 2016 für Mac
Office Home & Business 2016 für Mac
Office Home & Student 2016 für Mac
Office Standard 2016 für Mac
Outlook 2016 für Mac
PowerPoint 2016 für Mac
Word 2016 für Mac

Auszug aus der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)

§ 6 Technische und organisatorische Maßnahmen

(1) Je nach der Art der zu schützenden personenbezogenen Daten sind unter Berücksichtigung von §§ 26 und 27 KDG angemessene technische und organisatorische Maßnahmen zu treffen, die geeignet sind,

a) zu verhindern, dass unberechtigt Rückschlüsse auf eine bestimmte Person gezogen werden können (z.B. durch Pseudonymisierung oder Anonymisierung personenbezogener Daten),

b) einen wirksamen Schutz gegen eine unberechtigte Verarbeitung personenbezogener Daten insbesondere während ihres Übertragungsvorgangs herzustellen (z. B. durch Verschlüsselung mit geeigneten Verschlüsselungsverfahren),

c) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste zum Schutz vor unberechtigter Verarbeitung auf Dauer zu gewährleisten und dadurch Verletzungen des Schutzes personenbezogener Daten in angemessenem Umfang vorzubeugen,

d) im Fall eines physischen oder technischen Zwischenfalls die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen rasch wiederherzustellen (Wiederherstellung).

(2) Im Einzelnen sind für die Verarbeitung personenbezogener Daten in elektronischer Form insbesondere folgende Maßnahmen zu treffen:

a) Unbefugten ist der Zutritt zu IT-Systemen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle).

b) Es ist zu verhindern, dass IT-Systeme von Unbefugten genutzt werden können (Zugangskontrolle).

c) Die zur Benutzung eines IT-Systems Berechtigten dürfen ausschließlich auf die ihrer Zuständigkeit unterliegenden personenbezogenen Daten zugreifen können; personenbezogene Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Zugriffskontrolle).

d) Personenbezogene Daten sind auch während ihrer elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern gegen unbefugtes Auslesen, Kopieren, Verändern oder Entfernen durch geeignete Maßnahmen zu schützen.

e) Es muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung erfolgt (Weitergabekontrolle). Werden personenbezogene Daten außerhalb der vorgesehenen Datenübertragung weitergegeben, ist dies zu protokollieren.

f) Es ist grundsätzlich sicher zu stellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systemen verarbeitet worden sind (Eingabekontrolle). Die Eingabekontrolle umfasst unbeschadet der gesetzlichen Aufbewahrungsfristen mindestens einen Zeitraum von sechs Monaten.

g) Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle).

h) Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

i) Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Trennungsgebot).

j) Im Netzwerk- und im Einzelplatzbetrieb ist eine abgestufte Rechteverwaltung erforderlich. Anwender- und Administrationsrechte sind zu trennen.

(3) Absatz 2 gilt entsprechend für die Verarbeitung personenbezogener Daten in nicht automatisierter Form sowie für die Verarbeitung personenbezogener Daten außerhalb der dienstlichen Räumlichkeiten, insbesondere bei Telearbeit.

§ 19 Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken

Die Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken ist grundsätzlich unzulässig. Ausnahmen regelt der Verantwortliche unter Beachtung der jeweils geltenden gesetzlichen Regelungen.

§ 20 Nutzung privater IT-Systeme zu dienstlichen Zwecken

(1) Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu dienstlichen Zwecken ist grundsätzlich unzulässig. Sie kann als Ausnahme von dem Verantwortlichen unter Beachtung der jeweils geltenden gesetzlichen Regelungen zugelassen werden.

(2) Die Zulassung erfolgt schriftlich und beinhaltet mindestens

a) die Angabe der Gründe, aus denen die Nutzung des privaten IT-Systems erforderlich ist,

b) eine Regelung über den Einsatz einer zentralisierten Verwaltung von Mobilgeräten (z.B. Mobile Device Management) auf dem privaten

c) IT-System des Mitarbeiters,

d) das Recht des Verantwortlichen zur Löschung durch Fernzugriff aus wichtigem und unabweisbarem Grund; ein wichtiger und unabweisbarer Grund liegt insbesondere vor, wenn der Schutz personenbezogener Daten Dritter nicht auf andere Weise sichergestellt werden kann,

e) eine jederzeitige Überprüfungsmöglichkeit des Verantwortlichen,

f) die Dauer der Nutzung des privaten IT-Systems für dienstliche Zwecke,

g) das Recht des Verantwortlichen festzulegen, welche Programme verwendet oder nicht verwendet werden dürfen sowie

h) die Verpflichtung zum Nachweis einer Löschung der zu dienstlichen Zwecken verarbeiteten personenbezogenen Daten, wenn die Freigabe der Nutzung des privaten IT-Systems endet, das IT-System weitergegeben oder verschrottet wird.

Ergänzend ist dem betreffenden Mitarbeiter eine spezifische Handlungsanweisung auszuhändigen, die Regelungen zur Nutzung des privaten IT-Systems enthält.

(3) Der Zugang von privaten IT-Systemen über sogenannte webbasierte Lösungen kann mit den Mitarbeitern vereinbart werden, soweit alle datenschutzrechtlichen Voraussetzungen für eine sichere Nutzung gegeben sind.

(4) Die automatische Weiterleitung dienstlicher E-Mails auf private E-Mail-Konten ist in jedem Fall unzulässig.

Abkürzungen

AG	Amtsgericht
ArbG	Arbeitsgericht
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidung des Bundesgerichtshofes in Zivilsachen
BSI	Bundesamtes für Sicherheit in der Informationstechnik
BT-Drs	Bundestag Drucksache
BVerfGE	Bundesverfassungsgerichtsentscheidung
BZRG	Bundeszentralregister
CR	Computer und Recht (Zeitschrift)
DKWW	Däubler, Klebe, Wedde, Weichert
DoS	Denial-of-Service-Attacken
DSG-EKD	Datenschutzgesetz der Evangelischen Kirche
DS-GVO	Datenschutzgrundverordnung
DuD	Datenschutz und Datensicherheit
EuDSRL	Europäische Datenschutzrichtlinie
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
HTTP	Hypertext Transfer Protocol (unverschlüsselt)
HTTPS	Hypertext Transfer Protocol Secure (verschlüsselt)
IETF	Internet Engineering Task Force
IT-SiDa	Initiative für Sicherheit und Datenschutz im Netz
JGG	Jugendgerichtsgesetz
KDG	Kirchliches Datenschutzgesetz
KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz
KDO	Kirchliche Datenschutzordnung

KDR-OG	Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstl. Rechts
KUG	Kunsturhebergesetz
LAG	Landesarbeitsgericht
LbfDI, LfDI	Landesbeauftragter für Datenschutz und Informationsfreiheit
LG	Landgericht
NJW	Neue Juristische Wochenschrift
NZA	Neue Zeitschrift für Arbeitsrecht
OLG	Oberlandesgericht
RFC	Request for Comments, Sammlung von Dokumenten, herausgegeben von der IETF
SGB	Sozialgesetzbuch
SIP	Session Initiation Protocol, für Sprach- und Video-Verbindungen
SSL	Secure Sockets Layer (TLS)
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security (Verschlüsselung auf der Transport-schicht)
UrhG	Urhebergesetz
VG	Verwaltungsgericht
VoIP	Voice over Internet Protokoll, Sprach-Kommunikation im IP-Netzwerk
W3C	World Wide Web Consortium, Gremium zur Standardisierung im World Wide Web
WR	Weimarer Republik
WWW	World Wide Web
ZD	Zeitschrift für Datenschutz

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und des Katholischen Militärbischofs
Margaretenstraße 1 • 39218 Schönebeck
Telefon: 03928 7287181
www.kdsa-ost.de • kontakt@kdsa-ost.de