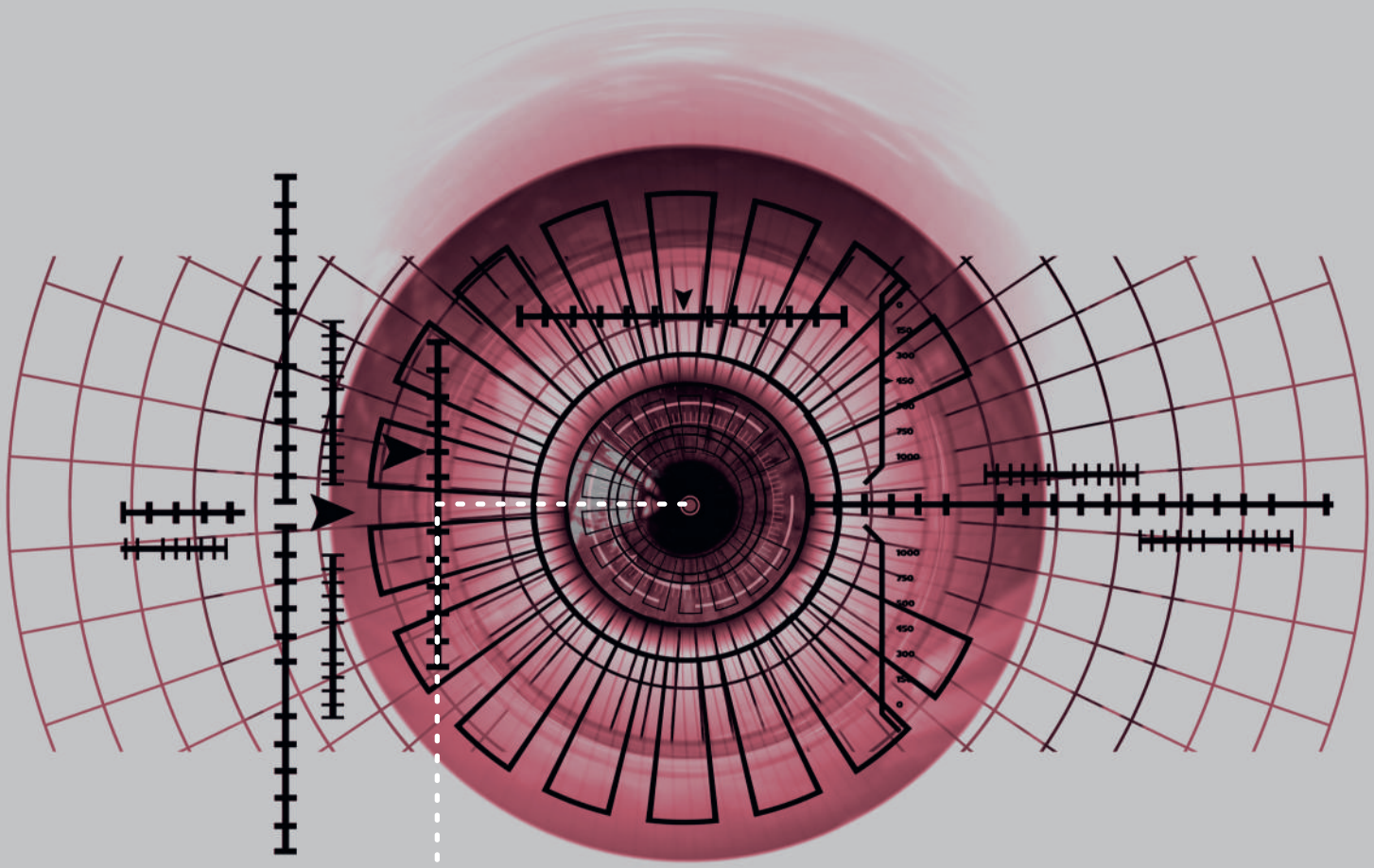


Tätigkeitsbericht 2021

KDSA Ost

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und
des Katholischen Militärbischofs

Herausgeber:

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und des Katholischen Militärbischofs

Badepark 4
39218 Schönebeck
Telefon: 03928 7179018
E-Mail: kontakt@kdsa-ost.de
www.kdsa-ost.de

Nicht der Wind, sondern das Segel bestimmt die Richtung.

Chinesisches Sprichwort

Datenschutzgesetze geben uns zwar eine rechtliche Grundlage zur Verarbeitung persönlicher Daten, tragen aber nicht zur praktischen Realisierung bei. Jeder, der mit seinen eigenen Daten und mit den Daten Anderer sorgfältig umgeht, trägt richtungsweisend für mehr Datenschutz und Datensicherheit bei.

6. Tätigkeitsbericht des Diözesandatenschutzbeauftragten

für

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

Berichtszeitraum 01.01.2021 bis 31.12.2021

Inhaltsverzeichnis

Inhaltsverzeichnis 1

Vorwort 5

1 Entwicklung des Datenschutzes 7

1.1 Entwicklung des Datenschutzes in Europa 7

1.2 Entwicklung des Datenschutzes in der Bundesrepublik 8

1.2.1 Infektionsschutzgesetz (IfSG) 8

1.2.2 Bargeld ermöglicht Freiheit 9

1.2.3 Bezahlen mit Daten 11

1.2.4 Bürger-Identifikationsnummer eingeführt: Macht uns die Steuer-ID künftig zum gläsernen Menschen? 15

1.2.5 Das Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) 18

1.2.6 Die elektronische Patientenakte (ePA): Datenschutzrechtliche Aspekte 19

1.2.7 Ohne Smartphone Mensch zweiter Klasse - aber sicher 23

1.2.8 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) 25

1.2.9 Betriebsrat als Teil des Verantwortlichen 26

1.2.10 Neues Mitbestimmungsgesetz bei Ausgestaltung mobiler Arbeit 27

1.3 Kirche 28

1.3.1 Evaluation KDG gem. § 58 Abs.2 KDG 28

1.3.2 Telegram kein zulässiger Messenger-Dienst für dienstliche Kommunikation im Bereich katholischer Einrichtungen 28

2 Datenschutz allgemein 29

2.1 Der Personalausweis auf dem Smartphone und die Einführung der Zentralisierung biometrischer Daten 29

2.2 Abfrage des Geburtsdatums im Rahmen eines Online-Bestellvorgangs 31

2.3 Erweitertes Führungszeugnis - Vorlagepflicht vor und während des Beschäftigungsverhältnisses 31

2.4 Informationspflichten oftmals nicht im Visier der Verantwortlichen 37

2.5 Wachsendes Schadenersatz-Risiko: Missbrauch von Betroffenenrechten 38

2.6 Verpflichtung zur Durchführung von Datenschutzschulungen 40

2.7 Muss eine Datenschutzerklärung auf der Website den Namen des zuständigen Datenschutzbeauftragten veröffentlichen? 41

2.8 Keine Abdingbarkeit von technischen und organisatorischen Maßnahmen 42
2.9 Original ersetzendes Scannen und Datenschutz 46
2.10 Schadenersatz und Erheblichkeitsschwelle 48
2.11 Spenderlisten und die Herausgabe der Spendernamen 49
2.12 Kinderfotos im Internet 53
2.13 Datenschutz unter Corona 54
2.13.1 Luca-App datenschutzrechtlich zweifelhaft und überflüssig 54
3 Datenschutzaufsicht 58
3.1 Datenschutzbeschwerde oder Prüfungsanregung 58
3.2 Prüfaktionen 59
3.2.1 Prüfung einer Seniorenwohneinrichtung 59
3.2.2 Datenschutzquerschnittsprüfung Pfarreien 62
4 Datenschutz im Gesundheitswesen 63
4.1 Datenschutzvorfälle 63
4.1.1 Nutzung privater Endgeräte am Arbeitsplatz 63
4.1.2 Übergriffige Klinikmitarbeiter und der Datenschutz 66
4.1.3 Verstöße gegen die Meldepflicht gem. § 33 KDG 68
4.1.4 Informationspflichten bei Datenpannen § 34 KDG 69
4.1.5 Gerichtliches Verfahren 70
4.1.6 Sonstige Vorfälle 71
5 Datenschutz in Schule und Kita 72
5.1 Ergebnisse der Prüfaktion: Nutzung privater Endgeräte – Datenverarbeitung im häuslichen Bereich 72
5.1.1 Verwendung von privaten IT-Geräten zu dienstlichen Zwecken und schriftlich Regelungen 72
5.1.2 Sicherung der IT-Geräte im privaten Bereich 74
5.1.3 Nutzung und Verfügbarkeit von E-Mailadressen durch die Lehrkräfte 74
5.2 Corona-Selbsttests an Schulen 76
5.3 Leistungsnachweise im Homeschooling – Schülervideos im Netz 77
5.4 Datenschutz im Kindergarten - Ungewollt Kinderfotos im Netz 79
5.5 Informationspflichten 81

5.5.1 Informationspflichten trotz Einwilligungserklärung am Beispiel von Fotos 81
5.6 Nachweis von Schutzimpfungen in Gemeinschaftseinrichtungen 83
6 Datenschutz im Beschäftigtenverhältnis 84
6.1 3G am Arbeitsplatz / Listen und Testate 84
6.2 Namensschilder / Persönlichkeitsrechte von Mitarbeitenden werden konsequent ignoriert! 85
7 Technischer Datenschutz 87
7.1 Windows datenschutzkonform – warum nicht 89
7.1.1 Nicht alles muss Online sein 91
7.2 Länderübergreifende Prüfaktion 92
7.3 Exchange Schwachstelle 95
7.4 Telefax (nicht) datenschutzkonform 97
7.4.1 Pauschale Aussagen nicht unbedingt förderlich für verständlichen Datenschutz 98
7.4.2 Telefaxübermittlung verschlüsselt 102
7.4.3 Verschlüsselte Kommunikation nur ein Schlagwort? 102
7.5 E-Mail-Inhalt schützen nicht immer praxistauglich 104
7.5.1 Inhaltsverschlüsselung durch verschlüsseltes PDF 106
7.6 Sensible Daten sammeln, so einfach war es noch nie 109
7.7 Doxing – Was wollen Die mit meinen Daten, ich habe doch nichts zu verbergen! 111
7.7.1 Die Masche mit der SMS zur falschen Tracking App 113
7.8 E-Mail-Tracking im Hintergrund 116
Anhang 119
Checkliste zur Selbstkontrolle 119
Muster - Informationspflicht für Fotos gemäß §§ 14, 15 KDG 120
Microsoft Versionsinformationen 124
Die Kirchliche Datenschutzaufsicht Ost 125
Abkürzungen 127

Vorwort

Auch im vergangenen Jahr war der Arbeitsalltag unserer Dienststelle bestimmt von der Corona-Pandemie.

Zahlreiche Eingaben beschäftigten sich mit der datenschutzrechtlichen Zulässigkeit von Verarbeitungen, die im Zusammenhang mit den Corona-Maßnahmen standen. Der korrekte Umgang mit Listen zur Kontaktnachverfolgung und vor allem die arbeitgeberseitige Verarbeitung von personenbezogenen Daten besonderer Kategorie standen dabei im Vordergrund.

Gerade in dieser Ausnahmesituation wurde erkennbar, wie wichtig ein wirksamer Datenschutz ist, denn dort wo personenbezogene Daten zunächst rechtmäßig erhoben worden sind, waren immer wieder Begehrlichkeiten festzustellen, diese Daten für andere Zwecke verwenden zu wollen. Hier galt es betroffene Personen zu sensibilisieren und Verantwortliche zu sanktionieren.

Aber vor allem erforderten die pandemiebedingten Einschränkungen und Kontaktbeschränkungen neue Angebote und Unterstützungsmaßnahmen durch unsere Behörde.

Gleich zu Beginn des Jahres haben wir unser Angebot „Videosprechstunden“ gestartet. Das Angebot richtet sich grundsätzlich an Jedermann. Die Idee, die dahintersteht ist es, Menschen über bestimmte datenschutzrechtliche Themen miteinander in Austausch zu bringen. Zu einem zuvor benannten und vorgestellten Thema (z.B. Beschäftigtendatenschutz) können sich Personen anmelden und ihre Fragen zu diesem Thema mit anderen Teilnehmenden diskutieren. Begleitet wird diese Diskussion von den Vertretern der Datenschutzaufsicht. Im Rahmen dieser Veranstaltungen konnten praxisrelevante Lösungen gemeinsam entwickelt werden.

Im Berichtsjahr 2021 gab es in unserer Dienststelle mehrere Prüfaktionen sowie anlassbezogene und anlasslose Datenschutzüberprüfungen vor Ort. Die Prüfaktionen wurden zum einen Teil schriftlich durch die Zusendung von Fragen bzw. Fragebögen durchgeführt, zum anderen Teil gab es auch vor-Ort-Prüfungen durch unsere Mitarbeiter.

Ebenso beteiligte sich unsere Dienststelle an einer länderübergreifenden Kontrolle der DSK zur Schrems II Entscheidung.

Die Anzahl der Anfragen und die Meldung von Datenschutzvorfällen ist im vergangenen Jahr konstant geblieben.

Die Umsetzung datenschutzrechtlicher Regelungen war in den einzelnen (Erz-) Bistümern sehr unterschiedlich gestaltet. Während betriebliche Datenschutzbeauftrage für die Bereiche der Caritas überall bestellt worden sind, ist insbesondere in einem Bistum für den verfasst kirchlichen Bereich auch nach drei Jahren der Geltung des KDG keine Lösung gefunden worden. Zwar sind der Aufsicht wegen § 51 Abs. 6 KDG für die Verhängung einer Geldbuße die Hände gebunden, jedoch sind die Verantwortlichen (in der Regel die Kirchenvorstände) darauf hingewiesen worden, dass die Einrichtungen von den betroffenen Personen auf Schadenersatz in Anspruch genommen werden können. Bei vorsätzlicher Pflichtvernachlässigung dürften für diese Ansprüche die verantwortlichen Personen in Regress genommen werden können.

1 Entwicklung des Datenschutzes

1.1 Entwicklung des Datenschutzes in Europa

Bereits mit der Einführung der DS-GVO war absehbar, dass Fragen der Auslegung der Verordnung nicht allein von den Gerichten der Mitgliedsstaaten geklärt werden können. Von den derzeit beim EuGH anhängigen Fragen können einige auch Auswirkungen auf das kirchliche Datenschutzrecht bzw. auf dessen Auslegung haben.

Nach der Rechtsprechung des Bundesgerichtshofs kommt eine Geldentschädigung wegen Persönlichkeitsrechtsverletzung nur bei einem schwerwiegenden Eingriff in Betracht, der nicht anders ausgeglichen werden kann. Fraglich ist, ob diese Rechtsprechung, die für Fälle entwickelt wurde, die nicht vom Unionsrecht beeinflusst sind, auch für einen auf Ersatz immateriellen Schadens gem. Art. 82 DS-GVO gestützten Anspruch gilt. Der EuGH ist u.a. aufgefordert, zu entscheiden, ob Art. 82 DS-GVO jede Beeinträchtigung der geschützten Rechtsposition erfasst, unabhängig von deren sonstigen Auswirkungen und deren Erheblichkeit.

Eine diesbezügliche Entscheidung wird auch Auswirkungen im Zusammenhang mit dem kirchlichen Datenschutz haben. Über Schadenersatzansprüche aus der Verletzung von Persönlichkeitsrechten entscheiden die staatlichen Zivilgerichte (§ 47 KDG). Da die DS-GVO wie auch das KDG eine Erheblichkeitsschwelle nicht festlegt, ist im Hinblick auf Erwägungsgrund 146 wohl von einem weiten Verständnis des Schadensbegriffes auszugehen. Damit erscheint es sachgerecht, betroffenen Personen einen Schadenersatzanspruch für einen immateriellen Schaden unabhängig von einer Erheblichkeitsschwelle zuzusprechen.

Eine weitere Vorlagefrage betrifft das Recht, dem zum betrieblichen Datenschutzbeauftragten bestellten Beschäftigten kündigen zu können. Nach Art. 38 Abs. 3 S. 2 DS-GVO darf der Arbeitgeber den betrieblichen Datenschutzbeauftragten nicht wegen der Erfüllung seiner Aufgaben abberufen oder benachteiligen. Nach § 6 Abs. 4 BDSG ist eine Kündigung überhaupt nur unter den Voraussetzungen des § 626 BGB möglich. Einen Bezug zur Aufgabenerfüllung enthält diese Regelung nicht. Letzteres gilt gem. § 37 Abs. 4 KDG auch für den kirchlichen Bereich.

Sollte der EuGH hier zu dem Ergebnis kommen, § 6 Abs. 4 BDSG verstoße gegen den Vollharmonisierungsgrundsatz der DS-GVO und sei deshalb unwirksam, hat dies keine direkte Auswirkung auf die kirchliche Vorschrift. Da das KDG mit der DS-GVO nur in Einklang stehen und nicht mit ihr identisch sein muss, darf einen Regelung des KDG nur nicht gegen grundsätzliche Wertentscheidungen der DS-GVO verstoßen. Hier besteht die grundsätzliche Wertung darin, betriebliche Datenschutzbeauftragte unter besonderen Schutz zu stellen, damit diese bei Ausübung ihrer Tätigkeit keine Repressalien fürchten müssen. Dem entspricht die Regelung des KDG auch dann, wenn sie über den von der DS-GVO geforderten Mindestschutz hinausgeht.

In einem weiteren, vom BAG vorgelegten Vorlagebeschluss möchte das BAG vom EuGH entschieden haben, ob das Amt des Datenschutzbeauftragten und des Betriebsratsvorsitzenden in Personalunion ausgeübt werden darf oder ob dies zu einem Interessenkonflikt nach Art. 38 Abs. 6 S. 2 DS-GVO führt.

Auch in diesem Fall dürfte eine Entscheidung keine Auswirkung auf die im KDG normierte Rechtslage haben. Anders als die DS-GVO soll nach dem KDG nur derjenige nicht zum betrieblichen Datenschutzbeauftragten benannt werden, der mit der Leitung der Datenverarbeitung oder mit der Leitung der kirchlichen Stelle betraut ist. Damit ist durch das KDG abschließend dargelegt, wer nicht zum betrieblichen Datenschutzbeauftragten benannt werden soll. Da das Gesetz für alle anderen Personen nur fordert, dass deren andere Aufgaben und Pflichten die Aufgaben des betrieblichen Datenschutzbeauftragten nicht beeinflussen dürfen, ist kein Raum für eine über das Gesetz hinausgehende Unvereinbarkeit gegeben.

1.2 Entwicklung des Datenschutzes in der Bundesrepublik

1.2.1 Infektionsschutzgesetz (IfSG)

Die seit dem 28.03.2020 geltende Epidemische Lage von nationaler Tragweite, § 5 IfSG, galt nach mehreren Verlängerungen bis zum 25.11.2021.

In diesem Zusammenhang kam es zu einer Vielzahl von Grundrechtseinschränkungen und Regelungen, die datenschutzrechtliche Fragestellungen aufwarfen.

So wurde bereits im November 2020 ein Recht bzw. eine Pflicht zum Homeoffice eingeführt. Danach galt zunächst befristet bis zum 30. Juni 2021 für Arbeitgeber die Verpflichtung, Beschäftigten, die Büroarbeit oder vergleichbare Tätigkeiten ausüben, Homeoffice anzubieten. Im Gegenzug waren die Beschäftigten verpflichtet, dieses Angebot anzunehmen. Am 24.11.2021 wurde die Verpflichtung erneut vom Gesetzgeber beschlossen und ist diesmal zunächst bis zum 19.03.2022 befristet. Die damit in Zusammenhang stehenden Verpflichtungen, die sich aus den Datenschutzgesetzen ergeben, werden dabei nicht von allen Vertragsparteien gesehen.

Mit der Einführung der 3G-Regelung am Arbeitsplatz wurde im November 2021 durch § 28b IfSG eine Regelung geschaffen, die Arbeitgeber und Beschäftigte verpflichtet, vor Betreten des Arbeitsplatzes einen Nachweis darüber zu erbringen, dass sie geimpft, genesen oder getestet sind. Diese Regelung räumt dem Arbeitgeber weder das Recht ein zu erfahren, welcher der genannten Status auf den jeweiligen Beschäftigten zutrifft, noch ergibt sich daraus eine Berechtigung Impfzeugnisse zu kopieren oder anders bei sich zu verarbeiten.

1.2.2 Bargeld ermöglicht Freiheit

Der Bundestag hat in seiner Sitzung am 25.02.2021 u. a. über den Schutz der Bargeldnutzung debattiert. Hintergrund ist das Bestreben des europäischen Gesetzgebers für Bargeldkäufe zumindest eine einheitliche Obergrenze festzulegen.

Innerhalb Europas gibt es nach wie vor sehr große Unterschiede im Zahlungsverhalten. Während es in Österreich (57 Prozent) und Deutschland (56 Prozent) nach wie vor eine klare Mehrheit für die Bargeldzahlung gibt, ist dies in Schweden, wo nur noch 15 Prozent bar zahlen,[1] ganz anders.

Die europäische Union ist in ihrem Vorhaben geleitet von der Annahme, Bargeld würde kriminellen Aktivitäten Vorschub leisten. Der ehemalige Präsident der Luxemburger Zentralbank und Mitglied im EZB-Direktorium Yves Mersch

1 https://www.tagesschau.de/wirtschaft/corona-bargeld-101.html

stellt dazu fest, eine besondere Verknüpfung zwischen Bargeld und kriminellen Aktivitäten sei statistisch nicht feststellbar.[2]

Momentan wird die diesbezügliche Diskussion auch von der aktuellen Pandemiesituation und der Frage getrieben, ob eine Infektion über Münzen und Scheine möglich ist. Nach Einschätzung des RKI spielt dieser Übertragungsweg nach aktuellem Informationsstand eine eher untergeordnete Rolle.[3] Auch dem Bundesinstitut für Risikobewertung sind mit Stand November 2020 keine Infektionen über den Übertragungsweg Bargeld bekannt geworden.[4]

Demgegenüber ist festzustellen, dass Personen, die nur bedingt Zugang zu anderen Zahlungsarten haben, die Teilnahme am täglichen Geschäftsverkehr zumindest erschwert würde.

Neben diesen praktischen Erwägungen stellt die Abschaffung von Bargeld oder die Festlegung von Obergrenzen für die Bargeldzahlung einen erheblichen Eingriff in die Persönlichkeitsrechte der Menschen dar. Es ist das Recht aller Bürger bei Einkäufen weder von staatlicher noch von privater Seite registriert zu werden. Bargeld kommt deshalb auch die wichtige Funktion zu, Menschen vor Datenmissbrauch durch private Unternehmen oder den Staat zu schützen.[5]

Yves Mersch[6] stellte bereits in einer Rede im Februar 2018 fest, Bargeld gewähre Privatsphäre und sichere damit Grundrechte wie das Recht auf informationelle Selbstbestimmung, die Handlungsfreiheit und Meinungsfreiheit ab.[7]

Der ehemalige Bundesverfassungsrichter Udo Di Fabio unterstützt diese Stellungnahme mit der Feststellung, man dürfe den Bürger nicht in ein Sys-tem zwingen, in dem er ununterbrochen Spuren hinterlässt. Eine Abschaffung des Bargelds sei deshalb ein Verstoß gegen die Pflicht des Staates, eine geeignete Infrastruktur zum Schutz von Persönlichkeitsrechten zu erhalten.[8]

2 https://www.bundesbank.de/de/aufgaben/themen/thiele-forderung-nach-kompletter-bargeldabschaffung-ist-unangemessen-665618
3 Bt.-Drs 19/25988
4 https://www.bfr.bund.de/de/kann_das_neuartige_coronavirus_ueber_lebensmittel_und_gegenstaende_uebertragen_werden_-244062.html
5 Antrag der FDP Fraktion vom 23.02.2021, Bt.-Drs.: 19/26881
6 Von 12/2012 – 12/2020 Mitglied Direktorium der EZB
7 https://www.bundesbank.de/de/aufgaben/themen/thiele-forderung-nach-kompletter-bargeldabschaffung-ist-unangemessen-665618
8 Ebd.

Zusammenfassend ist deshalb aus datenschutzrechtlichen Gründen festzustellen, dass bei Abschaffung oder weiterer Einschränkung von Bargeldzahlungen alternativ durch den Staat ein System zu etablieren ist, welches es allen Bürgern ermöglicht, anonym und überwachungsfrei Zahlungen vornehmen zu können.

1.2.3 Bezahlen mit Daten

Mit Schlagworten wie „umsonst“ oder „kostenlos“ werben viele Anbieter digitaler Produkte regelmäßig. Soziale Medien können ohne Geldzahlung genutzt werden. Im Gegenzug nimmt der Nutzer dafür Werbeeinblendungen in Kauf.

Uneigennützig motiviert sind diese Angebote selbstverständlich alle nicht. Die Anbieter stützen ihren kommerziellen Erfolg nämlich auf ein anderes, bisweilen deutlich wertvolleres Gut als Geld: die Daten der Nutzer, die sie dafür erhalten. Die Daten der Nutzer stellen für diese Unternehmen ein Millionengeschäft dar, die eine Vergütung der Angebote durch eine Geldzahlung entbehrlich macht.

Diese erhobenen Daten sind Informationen über Interessen, Lebensweise oder Psyche von Nutzern. Ihren Umsatz erwirtschaften die Anbieter durch die Weiterverwendung der Daten, zum Beispiel durch den Verkauf passgenauer Werbeplätze oder den Verkauf der Daten selbst.

Bislang war umstritten, wie der Austausch „Leistung gegen Daten“ zu behandeln ist. Im Datenschutzrecht schwelen die Diskussionen um die Zulässigkeit dieser Kopplung nicht erst seit Inkrafttreten der EU-Datenschutzgrundverordnung (DS-GVO).

Der Bundestag hat am 25.06.2021 das „**Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen**“ (Gesetz zur Neuregelung von Verbraucherverträgen über digitale Produkte) beschlossen, welches am 01.01.2022 in Kraft trat. Das Gesetz setzt die europäische Digitale Inhalte-Richtlinie (EU) Nr. 2019/770 um und stärkt die Rechte von Verbrauchern im Zusammenhang mit der Bereitstellung von digitalen Inhalten oder digitalen Dienstleistungen durch einen Unternehmer.

Mit der EU-Richtlinie soll der digitale Binnenmarkt innerhalb der EU gestärkt werden. Die nationalen digitalen Märkte sollen in einen gemeinsamen digitalen Markt zusammengeführt werden. Mit der Umsetzung wird zudem eine Stärkung der Verbraucherrechte in der EU verfolgt. Die Richtline betrifft Verträge zwischen einem Verbraucher und einem Unternehmer, die folgende Inhalte haben können:

- die Bereitstellung digitaler Inhalte und Daten in digitaler Form (z.B. Musik, Online-Videos)
- Dienstleistungen, die die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form ermöglichen (z.B. Cloud-Dienste) sowie
- Dienstleistungen, die den Austausch von Daten ermöglichen (z.B. soziale Medien wie Facebook, Instagram und TikTok oder Online-Games).

Die wichtigsten Änderungen durch das Gesetz zur Neuregelung von Verbraucherverträgen finden sich in § 312 Abs. 1a sowie § 327 Abs. 3 BGB.

312 Abs. 1a BGB

> *Die Vorschriften (...) sind auch auf Verbraucherverträge anzuwenden, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich hierzu verpflichtet. Dies gilt nicht, wenn der Unternehmer die vom Verbraucher bereitgestellten personenbezogenen Daten ausschließlich verarbeitet, um seine Leistungspflicht oder an ihn gestellte rechtliche Anforderungen zu erfüllen, und sie zu keinem anderen Zweck verarbeitet.*

327 Abs. 3 BGB

> *Die Vorschriften (...) sind auch auf Verbraucherverträge über die Bereitstellung digitaler Produkte anzuwenden, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich zu deren Bereitstellung verpflichtet, es sei denn, die Voraussetzungen des § 312 Absatz 1a Satz 2 liegen vor.*

Klargestellt wird mit diesen Regelungen, dass, wenn ein Verbraucher für den Erhalt einer Leistung personenbezogene Daten bereitstellt, dies mit

der Zahlung eines Geldbetrages gleichgestellt wird und damit auch das Verbraucherschutzrecht anwendbar ist.

Dies gilt jedoch nur dann, wenn tatsächlich ein Vertrag durch zwei übereinstimmende Willenserklärungen mit Rechtsbindungswillen zustande gekommen ist. In diesem Fall sind sowohl das aktive Bereitstellen der Daten durch den Verbraucher als auch das passive Dulden der Datenerhebung durch den Anbieter umfasst. Der Gesetzgeber will sogar die Einwilligung in das Setzen von Cookies oder ein Werbetracking auf Webseiten ausreichen lassen, wenn darüber ein Vertrag geschlossen wird. Ausgenommen sind jedoch solche Daten, die der Anbieter zur Abwicklung der Leistung benötigt, z.B. eine E-Mail-Adresse, um ein digitales Angebot zuzuschicken oder Rechnungsdaten, die der Anbieter zur Erfüllung von steuerlichen Pflichten benötigt. Wann es allerdings zu einem Vertragsschluss kommt, ist in der Praxis genau zu betrachten. Vielen Verbrauchern wird beim Surfen im Internet genau dieser Rechtsbindungswille fehlen, wenn sie im Cookie-Banner auf „alle akzeptieren“ klicken.

Die Gleichstellung sorgt für einen besseren Schutz der Verbraucher und der Durchsetzbarkeit ihrer Rechte, da der Anbieter verpflichtet ist, die Hauptleistungspflichten des Vertrags eindeutig darzulegen. Er muss offenlegen, welche Daten der Verbraucher für welche Leistung und für welchen Zweck zur Verfügung stellt. Durch die Gesetzesänderung ergeben sich jedoch auch für die Unternehmen Vorteile, da ein rechtssicheres Anbieten der Produkte und Leistungen möglich wird. Ferner wurde für den Fall, dass der Verbraucher seine datenschutzrechtliche Einwilligung widerruft und eine Fortsetzung des Vertragsverhältnisses dem Anbieter nicht zumutbar ist (§ 327q Abs. 2 BGB), für diesen ein Kündigungsrecht eingeführt.

Die Neuregelung beantwortet aber nicht die Frage der datenschutzrechtlichen Rechtsgrundlage und ob eine erteilte Einwilligung freiwillig ist oder an Art. 7 Abs. 4 DS-GVO scheitert.

Die streitige Frage, ob die Datenverarbeitung im Geschäftsmodell „Daten gegen kostenlosen Service“ auf Basis einer Einwilligung zulässig ist oder ggf. bereits zur Vertragsdurchführung erforderlich sein kann, weil der Nutzer sich vertraglich zur Bereitstellung der Daten verpflichtet, wird weiter offenbleiben. Dass der Erforderlichkeitsmaßstab auf die Erbringung der vertraglichen Leistung nicht einseitig durch den Anbieter im Rahmen sei-

nes Geschäftsmodells vorgegeben werden kann, spricht gegen die letztgenannte Annahme.
Für diese Auffassung spricht, dass sich Art. 6 Abs. 1 lit. b) DS-GVO auf Datenverarbeitungen, die erforderlich sind, um überhaupt erst die Erfüllung des Vertrages zu ermöglichen bezieht und nicht auf die Bereitstellungen der Daten als vertragliche Hauptleistungspflicht.[9] Diese Differenzierung scheint der Gesetzgeber auch in § 312 Abs. 1a S. 2 BGB getroffen zu haben, da er Daten, die der Anbieter ausschließlich zur Erbringung seiner Leistungspflicht oder an ihn gestellten rechtlichen Anforderung erhebt, gesondert erwähnt und für diesen Fall die Anwendung des Verbraucherschutzrechts ausschließt. Der Gesetzgeber differenziert damit eindeutig zwischen den „erforderlichen" personenbezogenen Daten und den „darüberhinausgehenden", z.B. für die Profilbildung zu Werbezwecken erhobenen Daten.

Eine Einwilligung in die beabsichtigte Verarbeitung personenbezogener Daten der Nutzer ist auch weiterhin erforderlich, soweit diese nicht zur Erfüllung der Leistungspflicht oder rechtlicher Anforderungen, die an den Unternehmer gestellt werden, erfolgt. Für diese Ansicht spricht auch, dass der Gesetzgeber sowohl in der Gesetzbegründung als auch durch die Statuierung eines Kündigungsrechts für den Fall des Widerrufs der datenschutzrechtlichen Einwilligung davon ausgeht, dass eine Einwilligung regelmäßig erforderlich ist.

Durch die getroffene Neuregelung wird deutlich, dass der Gesetzgeber das Geschäftsmodell Daten gegen Leistung grundsätzlich im Rahmen der Vertragsfreiheit - flankiert durch die nun geltende Anwendbarkeit der verbraucherschutzrechtlichen Vorschriften - als zulässig ansieht. Vor dem Hintergrund dürfte nunmehr viel dafürsprechen, dass erteilte Einwilligungen regelmäßig nicht wegen Art. 7 Abs. 4 DS-GVO an der fehlenden Freiwilligkeit scheitern. Ob im Einzelfall doch eine Kopplung der Preisgabe personenbezogener Daten mit der kostenlosen Zurverfügungstellung einer Leistung zum Entfallen der Freiwilligkeit einer erteilten Einwilligung nach Art. 7 Abs. 4 DS-GVO führen kann, wenn der Verbraucher auf die Leistung faktisch angewiesen ist und der Anbieter eine Monopolstellung innehat, wird die Rechtsprechung zu klären haben.

9 Schantz in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 DS-GVO Rn. 33

1.2.4 Bürger-Identifikationsnummer eingeführt: Macht uns die Steuer-ID künftig zum gläsernen Menschen?

Der Bundesrat stimmte einem Gesetz zur Einführung einer neuen Bürgeridentifikationsnummer, dem Registermodernisierungsgesetz (RegMoG), trotz verfassungsrechtlicher Bedenken zu. Im Bundesrat stimmten am 05.03.2021 zwölf von sechzehn Bundesländern für das Registermodernisierungsgesetz. Es gab vier Enthaltungen und keine Gegenstimmen. Der genaue Termin für die Umsetzung ist derzeit noch nicht festgelegt.

Steuer-ID als unveränderbares Zuordnungsmerkmal

Durch das Registermodernisierungsgesetz können Verwaltungsdaten mithilfe der festen Steuer-ID zur richtigen Person zugeordnet werden. Die Abläufe in den Verwaltungen sollen vereinfacht, beschleunigt und die Abläufe verstärkt digital umgesetzt werden können. Der Aufbau dieser digitalen Struktur ist erforderlich, um die ID-Nummer für wichtige Verwaltungsleistungen des Onlinezugangsgesetzes zu nutzen. Mit dem Onlinezugangsgesetz haben sich Bund, Länder und Kommunen selbst verpflichtet, 575 Verwaltungsleistungen online anzubieten. Durch das Registermodernisierungsgesetz soll die Steuer-ID zu einer umfassenden Bürgernummer ausgebaut werden.

Steuer-ID

Die Steueridentifikationsnummer wird bereits bei der Geburt vergeben und ist ein Leben lang gültig. Die individuelle Steuerkennung soll sicherstellen, dass steuerbezogene Daten immer derselben Person zugeordnet werden. Sie enthält 11 Ziffern und wurde 2007 eingeführt.

Gut zu wissen: Die Steuer-ID wird zusammen mit Stammdaten, die eine Identifizierung des Steuerpflichtigen ermöglichen sollen, in einer vom Bundeszentralamt für Steuern (BZSt) verwalteten Datenbank gespeichert. Zu den Stammdaten gehören unter anderem Namen, Geburtsdatum und -ort, Geschlecht und die letzte bekannte Anschrift. Außerdem ist dort die zuständige Finanzbehörde hinterlegt.

Egal ob Heirat, Namensänderung, Scheidung oder der Umzug in eine andere Stadt – die Steueridentifikationsnummer bleibt. Gespeichert wird sie

beim Bundeszentralamt für Steuern – dort unter der Bezeichnung „Persönliche Identifikationsnummer“.

“Once-Only“-Prinzip

Mit dem Registermodernisierungsgesetz kann die Bundesregierung das “Once-Only“-Prinzip verwirklichen. Bereits in Registern gespeicherte Angaben und Nachweise müssen dann nicht immer wieder aufs Neue vorgelegt werden.

Datenschutzcockpit soll für mehr Transparenz sorgen

Das Datenschutzcockpit, das schrittweise mit der Identifikationsnummer eingeführt werden soll, soll es Bürgerinnen und Bürgern von jedem Internetzugang aus ermöglichen zu überprüfen, welche ihrer Daten auf Grundlage der ID-Nummer zwischen öffentlichen Stellen ausgetauscht wurden. Das soll Transparenz herstellen und dadurch Vertrauen schaffen.

Zentrale Registermodernisierungsbehörde

Eine zentrale Registermodernisierungsbehörde wird beim Bundesverwaltungsamt eingerichtet, die das erweiterte Steuernummernsystem zu verwalten hat. Dieses Amt wird als Dreh- und Angelpunkt fungieren zwischen dem Bundeszentralamt für Steuern, wo die Steuer-IDs aufbewahrt werden, und den anderen registerführenden Behörden.

Wichtig: Der Austausch der Daten zwischen den einzelnen Behörden soll nur dann erfolgen, wenn der Betroffene einwilligt oder eine gesetzliche Grundlage besteht. Die Bürger sollen über ein “Datencockpit” die Möglichkeit haben, Einsicht in die gespeicherten und abgefragten Daten zu erhalten.

Weiterhin massive Kritik an der Bürger-ID

Das Schuldnerverzeichnis und das Insolvenzregister wurden aufgrund erheblicher Kritik im Zuge der Verabschiedung des neuen Gesetzes aus der Liste der berechtigten Stellen herausgenommen. Unbeschadet dessen sehen viele Datenschutz- und Verfassungsrechtler massive Probleme bei der Bürger-ID.

Wesentliche Kritikpunkte:

1. Die ursprüngliche festgelegte **Zweckbindung** der Steuer-ID wird durch die Überführung in die Bürgernummer ausgehebelt. Ein wesentlicher Datenschutzgrundsatz der DS-GVO ist jedoch die Zweckbindung, die eine zweckentfremdete Nutzung untersagt. Umgangen werden soll dieser Grundsatz durch die **Knüpfung an die Einwilligung** des Betroffenen. Allein die Aussicht auf vereinfachte und beschleunigte Vorgänge dürfte die Bereitschaft zur unbedachten Einwilligung jedoch erhöhen.

2. Durch die Nutzung der Bürger-ID steigt auch die Gefahr, künftig **umfassende Persönlichkeitsprofile** von einzelnen Bürgern erstellen zu können. Zu berücksichtigen ist auch, dass bereits eine einfache Datenschutzpanne bei der Abfrage für den einzelnen Bürger erhebliche Nachteile bringen kann. Nicht außeracht gelassen werden darf auch das Missbrauchspotential, denn auch der Faktor „Mensch" in den Behörden darf nicht vergessen werden. Wie unberechtigte Anfragen und Zugriffe durch Mitarbeiter verhindert werden sollen, ist nicht geklärt.

3. Gegen die Einführung umfassender Personenkennziffern positionierte sich bereits das **Bundesverfassungsgericht**[10] in der Vergangenheit regelmäßig. Nach Ansicht des Wissenschaftlichen Dienst des Bundestages[11] hat das BVerfG der Einführung der Steuer-ID damals nur deshalb nicht widersprochen, weil deren Zweckbindung auf steuerliche Belange beschränkt wurde. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Professor Ulrich Kelber hat sich gegen die Nutzung der Steuer-Identifikationsnummer als übergreifendes Ordnungsmerkmal ausgesprochen. Dazu sagte der BfDI bereits in einer Pressemitteilung vom 28. Juli 2020:

   „Die Pläne für die Registermodernisierung sind in vielen Punkten gar nicht schlecht und durchaus im Interesse der Bürgerinnen und Bürger. Doch durch die Verwendung einer einheitlichen Identifikationsnummer besteht ein erhebliches Risiko der missbräuchlichen Zusammenführung

10 Das Bundesverfassungsgericht sprach im sog. Mikrozensus-Beschluss vom 16. Juli 1969 erstmals von einem Verbot der umfassenden Registrierung und Katalogisierung der Persönlichkeit, (BVerfGE 27, 1 (6))
11 https://cdn.netzpolitik.org/wp-upload/2020/09/WD-Registermodernisierung.pdf

der Daten aus unterschiedlichen Registern. Damit werden viele Sicherheitsmaßnahmen entwertet. Ich hoffe, dass uns nicht wieder erst das Bundesverfassungsgericht vor einem zu neugierigen Staat schützen muss."

Fazit:
Trotz der Verabschiedung des Registermodernisierungsgesetzes mit kleinen Änderungen dürfte die Diskussion um die Bürger-Identifikationsnummer nicht enden. Denn es bestehen nicht nur datenschutzrechtliche Bedenken, sondern auch die Verfassungsmäßigkeit eines solchen Vorgehens wird von zahlreichen Seiten grundlegend bezweifelt. Abzuwarten ist, ob Klagen vor dem Bundesverfassungsgericht, das der informationellen Selbstbestimmung des Einzelnen in den vergangenen Jahren immer mehr Bedeutung zugemessen hat, erhoben werden.

1.2.5 Das Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG)

Das Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) ist seit Juni 2021 in Kraft. Schwerpunkt des Gesetzes ist die Modernisierung der Vernetzung im Gesundheitswesen.

Mit dem Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (PDSG) und dem Digitale-Versorgung-Gesetz (DVG) wurden im Eilverfahren entscheidende Schritte für die flächendeckende Digitalisierung in der Gesundheitsversorgung unternommen. So wurden die Telematikinfrastruktur ausgebaut und die elektronische Patientenakte (siehe nachfolgender Beitrag) als Kernelement der Patienteneinbindung weiterentwickelt. Dazu folgten Maßnahmen im Verordnungsbereich, wie das elektronische Rezept oder Digitale Gesundheitsanwendungen (DiGA) als „App auf Rezept". Das DVPMG passt die umfangreichen Regelungen, die der Gesetzgeber bereits getroffen hat, an aktuelle Entwicklungen an und ergänzt neue Ansätze für die kommenden Jahre.

Gesundheits-Apps können künftig auch in der Pflege zum Einsatz kommen. Digitale Pflegeanwendungen sollen helfen, mit speziellen Trainingsprogrammen die Gesundheit der Nutzer zu stabilisieren oder den

Austausch mit Angehörigen oder Pflegefachkräften zu erleichtern. Es wird eigens ein neues Verfahren geschaffen, um die Erstattungsfähigkeit digitaler Pflegeanwendungen zu prüfen. Auch die Pflegeberatung wird um digitale Elemente erweitert.

Einsatz digitaler Gesundheitsanwendungen

Das Gesetz erleichtert den Einsatz digitaler Gesundheitsanwendungen. So können Versicherte ihre entsprechenden Daten in der elektronischen Patientenakte speichern. Leistungen von Heilmittelerbringern und Hebammen, die im Zusammenhang mit digitalen Gesundheitsanwendungen erbracht werden, werden künftig vergütet.

Ziel ist zudem eine stärkere Nutzung der Telemedizin - zum Beispiel durch Vermittlung telemedizinischer Leistungen bei der ärztlichen Terminvergabe. Auch der kassenärztliche Bereitschaftsdienst soll künftig telemedizinische Leistungen anbieten, ebenso Heilmittelerbringer und Hebammen.

Digitale Identität

Ergänzend zur elektronischen Gesundheitskarte haben die Krankenkassen den Versicherten ab dem 01.01.2023 auf Verlangen eine sichere digitale Identität für das Gesundheitswesen barrierefrei zur Verfügung zu stellen. Ab dem 01.01.2024 dient die digitale Identität in gleicher Weise wie die elektronische Gesundheitskarte zur Authentisierung des Versicherten im Gesundheitswesen und als Versicherungsnachweis.

1.2.6 Die elektronische Patientenakte (ePA): Datenschutzrechtliche Aspekte

Seit dem 01.01.2021 sind die gesetzlichen Krankenkassen verpflichtet, ihren Versicherten die ePA zur Verfügung zu stellen. Die ePA wurde durch das Patientendatenschutzgesetz (PDSG) eingeführt. Ziel der ePA ist es, dass Versicherte relevante medizinische Informationen zur Verfügung stellen können, um dadurch die Informationslage der an der Behandlung Beteiligten zu verbessern. Die ePA wird durch die Versicherten selbst verwaltet. Sie behalten damit die „Hoheit über ihre Daten“ und entscheiden selbst über deren Errichtung, Nutzung und Löschung.

Datenschutzrechtliche Verantwortlichkeit

Gem. Art. 4 Nr. 7 DS-GVO ist Verantwortlicher die natürliche oder juristische Person ..., die ... über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet oder die vom Unionsrecht oder dem Recht der Mitgliedstaaten dazu bestimmt wird. Für die ePA hat der Gesetzgeber von dieser sog. Öffnungsklausel Gebrauch gemacht und die Verantwortlichkeit in § 307 SGB V geregelt. Diese Vorschrift regelt die Anforderungen an den Aufbau der Telematikinfrastruktur.

Verantwortlichkeit der Leistungsträger

Nach § 307 Abs. 4 SGB V ist der Leistungsträger, d.h. die jeweilige gesetzliche Krankenkasse, als Anbieter der ePA, datenschutzrechtlich verantwortlich für die Datenverarbeitung, trotz fehlender Zugriffsmöglichkeiten auf die Daten. Sie ist für alle Datenverarbeitungen im Zusammenhang mit der ePA, mit Ausnahme von Upload und Download von Dokumenten durch Leistungserbringer, d.h. Ärzte, Apotheken und Krankenhäuser oder sonstige Beteiligte, verantwortlich.

Verantwortlichkeit der Leistungserbringer

Die Leistungserbringer, d.h. Krankenhäuser und Arztpraxen, sind verantwortlich für die dezentrale Zone der IT. Das ist der Bereich, in dem die ePA über Schnittstellen mit den einzelnen Leistungserbringern, d.h. insbesondere den Praxisverwaltungssystemen (PVS) und der Krankenhausinformationssystemen (KIS) der Krankenhäuser, verbunden ist.

Zwei Formen der Datenverarbeitungen sind in diesem Kontext zu unterscheiden: Upload von Dokumenten aus den PVS/KIS in die ePA, als „Übermittlung" von Daten und der Download von Dokumenten aus der ePA in die PVS/KIS, als „Erhebung" von Daten. Die datenschutzrechtliche Verantwortung besteht im Rahmen der ePA nur für diese beiden Verarbeitungsformen und nur in der dezentralen Zone.

Verantwortlichkeit der Gematik

Nach dem Beschluss der Datenschutzkonferenz vom 12.09.2019[12] besteht für die dezentrale Zone eine gemeinsame Verantwortung gem. Art. 26 DS-GVO mit der Gesellschaft für Telematik (Gematik).

12 https://www.datenschutzkonferenz-online.de/media/dskb/20190912_beschluss_zur_gematik.pdf

Die Gematik bestimmt über die „Mittel“ der Verarbeitung, indem Sie den Leistungserbringern Vorgaben hinsichtlich der technischen Anforderungen und Konfigurationen der Konnektoren, VPN-Zugangsdienste und Kartenterminals macht. Ihr kommt darüber hinaus eine „Auffangverantwortlichkeit“ für die zentrale Infrastruktur zu, d.h. sie ist für Datenverarbeitungen in der zentralen Zone immer dann verantwortlich, wenn keine anderweitige Verantwortlichkeit greift (§ 307 Abs. 5 SGB V).

Einsatz von Auftragsverarbeitern

Denkbar ist auch der Einsatz von Auftragsverarbeitern (Art. 28 DS-GVO). Krankenkassen setzen z.B. IT-Dienstleister als Auftragsverarbeiter zum Betrieb der ePA-Systeme ein. Ebenso können Leistungserbringer IT-Dienstleister als Auftragsverarbeiter, z. B. für den Betrieb der PVS/KIS, Routern und Kartenterminals einsetzen.

Wenn die Auftragsverarbeiter „Anbieter von Betriebsleistungen“ der IT sind, wie die Anbieter von ePA-Aktensystemen und dazugehörigen Komponenten und Diensten, müssen sie zuvor durch die Gematik zugelassen werden (§§ 324, 325 SGB V).

Alle Auftragsverarbeiter müssen die Spezifikationen der Gematik im Hinblick auf die technischen Anforderungen an die Schnittstellen, Komponenten und Dienste erfüllen und Komponenten und Dienste auch regelmäßig updaten.

Rechtmäßigkeit der Datenverarbeitung

Die Zulässigkeit der Verarbeitung personenbezogener Daten bestimmt sich im Dreiecksverhältnis zwischen den Versicherten/Patient, dem Leistungsträger und dem Leistungserbringer. Zu differenzieren ist zwischen der Einrichtung und der Nutzung der ePA.

Die Datenverarbeitungen zur Einrichtung, der durch die GKV zur Verfügung gestellten ePA, erfolgt auf Basis einer Einwilligung der Versicherten. Die Einrichtung und Nutzung der ePA erfolgt nur auf Antrag der Versicherten (§ 341 Abs.1 SGB V) und ist freiwillig. Eine Pflicht zur Nutzung besteht nicht. Die Versicherten können auch jederzeit deren Löschung verlangen (§ 344 Abs. 3 SGB V). Ein Zugriff auf die ePA durch die GKV ist nur zulässig, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.

Im Verhältnis zwischen Versicherten und Leistungserbringern, z. B. der behandelnde Arzt, kann der Zugriff nur nach freiwilliger Berechtigungsvergabe durch den Versicherten erfolgen (vgl. § 353 SGB V). Der Zugriff auf die Datenverarbeitung muss im konkreten Behandlungskontext erforderlich sein (vgl. § 352 Nr. 1 SGB V). Die Einwilligung des Patienten ist demnach notwendig, jedoch allein nicht ausreichend für die Rechtmäßigkeit der Datenverarbeitung. In welchem Verhältnis die beiden Rechtsgrundlagen, Einwilligung und Erfüllung des Behandlungsvertrages zueinanderstehen ist nicht klar.

Ausbaustufen

Zum Start der ePA 2021 waren die Möglichkeiten bei den Zugriffsberechtigungen noch eingeschränkt. Der Bundesbeauftragten für den Datenschutz (BfDI) sprach gegenüber den gesetzlichen Krankenkassen bereits im November 2020 eine förmliche Warnung gem. Art. 58 Abs. 2 lit. a) DS-GVO aus, da Versicherte nur grobgranular Zugriffsrechte, nach dem „Alles oder Nichts-Prinzip“, vergeben konnten. Ein Orthopäde, dem Zugriff gewährt wurde, konnte so z. B. auch die Informationen über die Behandlung beim Psychiater in der ePA einsehen. Dies wurde aus Sicht des BfDI der Patientensouveränität nicht gerecht und stand zudem im Widerspruch mit der DS-GVO, da Datenschutzgrundsätze wie die Datenminimierung nicht wirksam umgesetzt wurden und ein derartiges Zugriffmanagement nicht dem aktuellen Stand der Technik entsprach.

Ab 2022 (ePA 2.0) soll die Zugriffsberechtigung dokumentenspezifisch erfolgen. Der Nutzer kann dann konkret festlegen, welcher Leistungserbringer welches Dokument oder welche Gruppe von Dokumenten einsehen kann. Dies erleichtert insbesondere die Zusammenarbeit verschiedener Leistungserbringer, etwa bei einer Heilmittel- oder Hilfsmittelverordnung, wenn auf einen Arztbrief, Behandlungsplan oder Befund zugegriffen werden soll. Die Möglichkeit, feingranulare Freigaben für einzelne Dokumente zu erteilen, steht allerdings nur in der App zur Verfügung.

Patienten, die die elektronische Patientenakte nicht über eine App verwenden, erhalten nur sogenannte mittelgranulare Berechtigungen. Das heißt: Nicht-App-Nutzer können den Zugriff eines Leistungserbringers auf vertrauliche Dokumentengruppen weiter einschränken. Zum Beispiel können

sie über Dokumentenkategorien festlegen, dass nur Leistungserbringer eines bestimmten Fachbereichs - wie etwa Hautarzt oder Augenarzt - Einsicht erhalten.

Eingeführt wird ein sog. stationärer Client. Die ePA kann nun nicht nur über ein Smartphone/Tablet, sondern auch über einen PC genutzt werden.

Weitere Anwendergruppen, wie Pflegeberufe, Hebammen, Physiotherapeuten, der Öffentliche Gesundheitsdienst, die Arbeitsmedizin, sowie Reha-Kliniken wurden hinzugenommen.

ePA 3.0: Dritte Ausbaustufe

Ab 2023 sollen mit der dritten Ausbaustufe viele weitere Funktionen hinzukommen. Mit der persönlichen ePA können Patienten Krankenhaus-Entlassungsbriefe, Pflegeüberleitungsbögen, Laborwerte und noch vieles mehr verwalten. Daten von genutzten digitalen Gesundheitsanwendungen (DIGAs) -sogenannten Apps auf Rezept- können dann auch in der ePA gespeichert werden.

Mit der ePA 3.0 soll es möglich werden, direkt mit Ärzten oder Ärztinnen in Kontakt zu treten – ein integrierter Messenger macht dies möglich.

Daten können dann auch pseudonymisiert für Forschungszwecke freigegeben werden, damit diese Daten zukünftig für die Gesundheitsversorgung genutzt werden können.

1.2.7 Ohne Smartphone Mensch zweiter Klasse - aber sicher

Immer mehr Anwendungen und Aufgabenstellungen des täglichen Lebens werden auf Smartphones verlagert. Insbesondere in den Medien wird dieser Umstand häufig als „Vorteil“ und „Sicherheitsgewinn“ dargestellt. Schnell stellt sich die Frage, wer eigentlich die Gewinner sein sollen, die Endanwender oder die Wirtschaft.

Faktisch verpflichten Banken, Sparkassen, Behörden, Krankenkassen und andere Einrichtungen der Daseinsvorsorge die Bürgerinnen und Bürger zum Besitz eines Smartphones. Menschen, die im Umgang mit modernen Geräten oder dem Internet nicht geübt sind, werden ebenso wie diejeni-

gen, die ein Handy nur besitzen, um damit mobil telefonieren zu können, von vielen Anwendungen ausgegrenzt. Durch den Zwang, immer mehr Anwendungen auf dem Smartphone zu installieren, werden darüber hinaus Menschen sozial ausgegrenzt, die sich solche Geräte und die damit einher gehenden Kosten für das Internet nicht leisten können.

Weiterhin werden Smartphones dadurch zu Speicherorten für wichtige, teils sensible personenbezogene Daten. Früher wäre niemand auf die Idee gekommen, seine Bankunterlagen, Ausweisdokumente etc. ins Schwimmbad mitzunehmen. Jetzt ist alles auf dem Smartphone, welches u.a. auf Grund der auch möglichen Bezahlfunktionen ständig mitgeführt wird. Je mehr Alltagsanwendungen auf dem Gerät eingerichtet werden, desto mehr „persönliches Leben" wird ständig mitgetragen.

Kommt ein Smartphone abhanden oder wird gestohlen, besteht für Fremde der Zugriff auf große Teile des Lebens, inklusive Banking-Apps und Zugriff auf soziale Kontakte und Medien.

Früher gebräuchliche, sichere Mehrfaktor-Authentifizierungen werden abgeschafft und auf das Smartphone verlagert. Ein Beispiel dafür ist das HBCI Verfahren der Banken. Bei diesem Verfahren benötigte man eine Chipkarte mit einem Sicherheitschip, ein Lesegerät und zusätzlich die PIN zur Chipkarte. Bei einer mehrfach falschen Eingabe der PIN wurde der Chip gesperrt, teilweise auch zerstört. Diese Verfahren haben viele Banken zum Ende 2021 abgestellt und durch Verfahren auf dem Smartphone ersetzt. Ein sicheres System wurde zugunsten vermeintlicher Bequemlichkeit aufgegeben.

Mit dem Argument „mit der App wird's sicherer" kann man wohl nicht punkten. Sicherheitsexperten und Polizei warnen zunehmend vor einem Anstieg der Angriffe auf mobile Geräte. Cyber-Kriminellen wird es durch die **zentralisierte Ablage des persönlichen Lebens** leicht gemacht (das wurde auch bei der Luca-App kritisiert). Sie müssen sich nur noch Zugang zu einem Gerät verschaffen und hätten ohne weiteren Aufwand zusätzliche Kontakte und Chatverläufe inklusive.

Ein Beweggrund für den Einsatz von Apps zur Abwicklung ihrer Geschäfte und Dienstleistungen wird für Behörden und Unternehmen oftmals die Tat-

sache der geringeren Kosten solcher Systeme sein. Die einseitige Kostenersparnis bzw. Gewinnmaximierung kann jedoch nicht zu Lasten der Sicherheit von zwangsverpflichteten Anwendern gehen. Der Gesetzgeber ist deshalb aufgefordert, hier eine Verpflichtung zur Schadenersatzübernahme für solche Unternehmen und Einrichtungen zu etablieren, die Nutznießer einer verpflichtenden Anwendung solcher Apps sind.

1.2.8 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Zum 01.12.2021 trat das neue Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft.

Mit Hilfe dieses Gesetzes soll eine Anpassung der Datenschutzbestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) an die DS-GVO erreicht werden. Gleichzeitig wurde damit die ePrivacy-Richtlinie umgesetzt.[13] Außerdem soll die Gesetzesänderung für Rechtsklarheit im Hinblick auf das bisherige Nebeneinander von DS-GVO, TMG und TKG sorgen.

Zum Fernmeldegeheimnis verpflichtet sind u. a. Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten (§ 3 Abs. 2 S. 1 Nr. 2). Eine Geschäftsmäßigkeit liegt vor, wenn ein entsprechendes Angebot für Dritte vorliegt. Auf eine Gewinnerzielungsabsicht kommt es dabei nicht an. Bislang wurde von der herrschenden Meinung ein Arbeitgeber als geschäftsmäßiger Anbieter eingestuft, wenn er die private Nutzung der betrieblichen Kommunikationsmittel erlaubte und diese seinen Beschäftigten für private Zwecke zur Verfügung stellt. An dieser Rechtslage ändert das neue Gesetz nichts.

Die Regelungen zur Zulässigkeit des Cookie-Einsatzes in § 25 TTDSG orientieren sich unmittelbar an den Vorgaben von Art. 5 Abs. 3 ePrivacy-Richtlinie. Aufgrund der Rechtsprechung des BGH[14] ergibt sich auch insoweit keine Änderung der Rechtslage.

13 RiLi 2002/58/EG; RiLi 2009/136/EG
14 BGH, 28.05.2020 – I ZR 7/16

1.2.9 Betriebsrat als Teil des Verantwortlichen

Am 01.06.2021 ist das „Gesetz zur Förderung der Betriebsratswahlen und der Betriebsratsarbeit in einer digitalen Arbeitswelt" (Betriebsrätemodernisierungsgesetz) ist in Kraft getreten.

Unter anderem wird durch dieses Gesetz ein § 79a BetrVG in das Betriebsverfassungsgesetz (BetrVG) eingefügt.

> *„Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Arbeitgeber und Betriebsrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften.".*[15]

Der Gesetzgeber kam damit einer Aufforderung der Konferenz der Datenschutzaufsichten des Bundes und der Länder (DSK)[16] nach, diese bis dahin von Literatur, Rechtsprechung[17] und unter den Aufsichtsbehörden[18] unterschiedlich beantwortete Frage, zu klären.

Die Ergänzung des BetrVG um § 79a hat keine direkte Auswirkung auf das kirchliche Datenschutzgesetz. Dennoch ist es für die bislang auch für das kirchliche Datenschutzrecht umstrittene Frage, ob die Mitarbeitervertretung „Verantwortlicher"[19] ist, eine Auslegungshilfe. Im Hinblick auf die datenschutzrechtlichen Rechte und Pflichten gibt es keine inhaltlichen Unterschiede zwischen Betriebsräten und Mitarbeitervertretungen. Auch ohne eine entsprechende gesetzliche Regelung, sind die Mitarbeitervertretungen nicht als eigene Verantwortliche zu betrachten. Die Verantwortlichkeit auch für diesen Teil der Einrichtung ist deshalb beim Arbeitgeber zu sehen.

---

15 Eine parallele Regelung ist in § 69 Entwurf eines Gesetzes zur Novellierung des Bundespersonalvertretungsgesetzes vorgesehen, BT.-Drs. 19/26820
16 Protokoll der DSK, Protokoll der 99. Sitzung vom 12.05.2020
17 Betriebsrat ist Teil des Verantwortlichen: LAG Hessen, Beschl. v. 10.12.2018 – 16 TaBV 130/18; LAG Niedersachsen, Beschl. V. 22.10.2018 – 12 TaBV 23/18; Gola, DS-GVO 2. Aufl., Art. 4 Rn. 56; Kranig/Wybitull ZD 2019, 1; Baumgärtner Honsch ZD 2019, Betriebsrat ist eigener Verantwortlicher: ohne Begründung: LAG Sachsen-Anhalt, Beschl. v. 18.12.2018 – 4 TaBV 19/17; LAG Mecklenburg-Vorpommern, Beschl. v. 15.5.2019 – 3 TaBV 10/18; Schaffland/Holthausen, in Schaffland/Wiltfang ,Art. 37, Rn. 90; Wybitul/von Gierke, BB 2017, S. 184
18 Betriebsrat eigener Verantwortlicher: LfDI Baden-Württemberg, TB 2018, S. 38; Betriebsrat Teil des Verantwortlichen Arbeitgebers LfDI Niedersachsen, TB 2020, S. 36
19 Andelewski/Bach/Fröb, ZMV 2020, S. 10; anders Ullrich, ZAT 2019, S. 140

1.2.10 Neues Mitbestimmungsgesetz bei Ausgestaltung mobiler Arbeit

Ebenfalls mit dem Betriebsrätemodernisierungsgesetz wurde dem § 87 Abs. 1 BetrVG in Punkt 14 ein weiteres Mitbestimmungsrecht des Betriebsrates etabliert. Ein solches besteht danach bei

> *„Ausgestaltung von mobiler Arbeit, die mittels Informations- und Kommunikationstechnik erbracht wird."*

Ein eigenes Mitbestimmungsrecht besteht damit nur im Hinblick auf die Ausgestaltung, also das „wie" von mobiler Arbeit. Die Entscheidung darüber „ob" mobile Arbeit eingeführt wird, verbleibt weiterhin in der Entscheidungsbefugnis des Arbeitgebers. Zur inhaltlichen Ausgestaltung der mobilen Arbeit gehören zum Beispiel Regelungen über den zeitlichen Umfang mobiler Arbeit, über Beginn und Ende der täglichen Arbeitszeit in Bezug auf mobile Arbeit oder über den Ort, von welchem aus mobil gearbeitet werden kann und darf. Es können Regelungen zu konkreten Anwesenheitspflichten in der Betriebsstätte des Arbeitgebers, zur Erreichbarkeit, zum Umgang mit Arbeitsmitteln der mobilen Arbeit und über einzuhaltende Sicherheitsaspekte getroffen werden. Auch bisher konnten die Betriebsräte über die Regelung des § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht ausüben, soweit mit Einführung mobiler Arbeit auch eine Überwachung von Verhalten oder Leistung von Arbeitnehmern möglich war. Durch die Ergänzung um den neuen Punkt können Persönlichkeitsrechte der Arbeitnehmer noch weiter geschützt werden. So z.B. wenn für Videokonferenzen zwingend das Einschalten der Kamera gefordert wird oder Arbeitgeber über Geoinformationen der Aufenthaltsort angezeigt wird. Nicht zuletzt bietet es der Interessenvertretung eine weitere Möglichkeit, auf Einhaltung der gesetzlichen Vorgaben zu bestehen und vom Arbeitgeber die Überlassung von dienstlichen Geräten zur Ausübung der mobilen Arbeit zu fordern.

Die Regelung hat keine direkte Auswirkung auf die Vorschriften der MAVO. Gleichwohl würde auch dort eine diesbezügliche Erweiterung der Mitbestimmungsrechte aus datenschutzrechtlicher Sicht eine Bereicherung darstellen.

1.3 Kirche

1.3.1 Evaluation KDG gem. § 58 Abs.2 KDG

In der benannten Vorschrift ist vorgesehen, das KDG innerhalb von drei Jahren ab Inkrafttreten zu überprüfen. Tatsächlich ist Anfang 2020 auch eine Arbeitsgruppe vom VDD eingerichtet worden, die sich dieses Themas annehmen soll. Ergebnisse dieser Arbeitsgruppe liegen bislang noch nicht vor. Nach dem derzeitigen Projektplan ist nicht vor Sommer 2023 mit einem überarbeiteten Entwurf des KDG zu rechnen.

1.3.2 Telegram kein zulässiger Messenger-Dienst für dienstliche Kommunikation im Bereich katholischer Einrichtungen

Die Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche hat in ihrer Sitzung vom 15.09.2021 ihren Beschluss zur Beurteilung von Messenger-Diensten vom 26.07.2018 aktualisiert. Die dort aufgeführten Kriterien, die ein Messenger-Dienst erfüllen muss, werden vom Dienst Telegram nicht erfüllt. Die Verwendung dieses Dienstes für eine dienstliche Kommunikation verstößt deshalb gegen das KDG und ist unzulässig!

Es ist nicht sicher nachvollziehbar, in welchem Land sich die Serverstandorte befinden. Nach eigenen Angaben von Telegram befinden sich deren Server überall in der Welt. Der Server für Europa befindet sich angeblich in London.

Ein sicherer Datentransport ist nicht gewährleistet. Eine Ende-zu-Ende-Verschlüsselung findet regelmäßig nicht statt. Laut heise-online[20] werden die meisten Chats auf Telegram nur sicher verschlüsselt, während sie zwischen den Geräten und den Servern von Telegram übertagen werden. Während die Chats auf den Servern ruhen, kann Telegram jedoch die Chat-Daten lesen. Bei anderen Messenger-Diensten (selbst bei WhatsApp) existieren echte Ende-zu-Ende-Verschlüsselungen, bei denen nur die Empfänger auf

20 https://www.heise.de/tipps-tricks/Wie-sicher-ist-Telegram-5048425.html

die Nachrichten zugreifen können, da die Chats nur auf deren eigenen Smartphones abgelegt sind und nicht auf irgendwelchen Servern.

Etwas anderes gilt für geheime Chats, die bei Telegram für jeden Chat separat eingestellt werden müssen. Jedoch dürfte dies den meisten Telegram-Nutzern nicht bekannt sein. Auch ist diese Möglichkeit in dem System gut versteckt.[21] Außerdem liefert die App laut einem Test von „heise-online" alles was getippt wird an den Telegram-Server und zwar bereits bevor die Nachricht abschickt wird.

Darüber hinaus greift die App auf Metadaten und das Telefonbuch zu. Dadurch wird es möglich, Bewegungsprofile zu erstellen und zu speichern, um zu sehen, mit welchen Geräten Nutzer wann und wo online waren. Nutzer haben deshalb keine Kontrolle über die auf ihrem Gerät gespeicherten personenbezogenen Daten Dritter.

Schließlich ist in den letzten Monaten deutlich geworden, dass Telegram seinen Geschäftssitz nach Dubai verlegt hat und damit für deutsche Aufsichtsbehörden oder für eine Strafverfolgung nicht erreichbar ist.

2 Datenschutz allgemein

2.1 Der Personalausweis auf dem Smartphone und die Einführung der Zentralisierung biometrischer Daten

Seit August 2021 gibt es keinen Personalausweis mehr ohne Fingerabdruck. Bereits am 05. November 2020 wurde das „Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen" mit den Stimmen der Großen Koalition im Bundestag beschlossen. Das Gesetz passt das Personalausweisgesetz an die Anforderungen der EU-Verordnung 2019/1157 vom 20. Juni 2019 an.

Was für Reisepässe bereits seit 2007 gilt, ist nun auch für Personalausweise Realität – die Fingerabdruckpflicht.

21 https://www.heise.de/hintergrund/Telegram-Chat-der-sichere-Datenschutz-Albtraum-eine-Analyse-und-ein-Kommentar-4965774.html; https://www.rnd.de/digital/telegram-datenschutz-ist-katastrophal-UWYTXHQ5QSW-G4WDB6X6J4RGS6A.html

Biometrische Fotos sind in Deutschland zum Standard geworden, weil es der Gesetzgeber so wollte. Das Versprechen, diese biometrischen Daten auf dem Chip in den Ausweisdokumenten und nur dezentral zu speichern, wurde nicht gehalten. Am 25.06.2021 wurde trotz Kritik das „Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät", welches am 20.05.2021 vom Bundestag beschlossen worden ist, vom Bundesrat bestätigt. Das Gesetz trat am 1. September 2021 in Kraft.

Ziel des eID-Gesetzes ist es, neben den bisherigen Möglichkeiten des elektronischen Identitätsnachweises unter Verwendung des Personalausweises, der eID-Karte oder des elektronischen Aufenthaltstitels, die Durchführung des elektronischen Identitätsnachweises allein mit einem mobilen Endgerät zu ermöglichen und durch diese Weiterentwicklung die Nutzungszahlen des elektronischen Identitätsnachweises zu erhöhen. Unabhängig von der Möglichkeit des mobilen Identitätsnachweises wird den Bundesländern mit diesem Gesetz ermöglicht, zentrale Biometriedatenbanken einzurichten.

Der Ausbau einer biometrischen Überwachungsinfrastruktur, vor dem schon mit Beginn der Einführung der biometrischen Merkmale in Ausweisdokumenten gewarnt wurde, hat damit eine konkrete Form angenommen.

Die am Gesetzesvorhaben geäußerte Kritik fand kein Gehör, weil die Biometrie längst in den Alltag „eingedrungen" ist. Dass die für einen Pass oder Ausweis auf den Ämtern abzugebenden Fotos biometrisch sind, wurde vielfach als Selbstverständlichkeit betrachtet.

Biometrische Gesichtserkennung wurde erstmals im Rahmen der Ermittlungen zu den G20-Protesten in Deutschland eingesetzt, obwohl die Rechtmäßigkeit umstritten war. Die nun ermöglichte Zentralisierung der Biometriedaten leistet solchem Vorgehen in der Zukunft noch Vorschub und normalisiert die Nutzung von „Körperdaten" und den Einsatz von biometrischen Erkennungstechnologien.

Für welche Zwecke die eigenen biometrischen Daten künftig abgerufen, gespeichert und ob und welche Abgleiche mit welcher Datenbank vorgenommen werden, kann niemand mehr selbst kontrollieren, da das eigene Gesicht und nun auch die Fingerabdrücke für ein Ausweisdokument verpflichtend vermessen und abgespeichert werden.

2.2 Abfrage des Geburtsdatums im Rahmen eines Online-Bestellvorgangs

Das Verwaltungsgericht Hannover hat sich mit der Frage befasst, welche Daten eine Versandapotheke im Rahmen des Bestellvorgangs erheben darf.[22] Die Landesbeauftragte für den Datenschutz in Niedersachsen war der Meinung, die Versandapotheke erhebe zu viele Daten im Bestellvorgang und untersagte ihr im Januar 2019, unabhängig vom bestellten Medikament das Geburtsdatum abzufragen. Auch die Angabe des Geschlechts sei, jedenfalls bei nicht geschlechtsspezifisch zu dosierenden Medikamenten, nach ihrer Auffassung nicht erforderlich.

Die Betreiberin der Versandapotheke berief sich auf ihre Beratungspflicht, die sich aus der Apothekenbetriebsordnung ergibt. Diese umfasse auch die geschlechtsspezifische und altersgerechte Beratung. Ferner müsse sie wissen, ob die Besteller volljährig seien. Sie klagte gegen den Bescheid der Datenschutzbehörde, die Klage wurde nach mündlicher Verhandlung vom VG Hannover abgewiesen.

Vor dem Verhandlungstermin hat die Versandapotheke auf eine geschlechtsspezifische Anrede verzichtet, so dass über diesen Punkt nicht verhandelt wurde. Die Verarbeitung des Geburtsdatums beim Erwerb rezeptfreier Produkte ist nach Ansicht des Gerichts für solche Produkte unzulässig, die keine altersgerechte Beratung erfordern. Dies gilt u.a. für Drogerieartikel. Um die Geschäftsfähigkeit der Kunden zu prüfen, reicht es nach Ansicht des Gerichts aus, abzufragen, ob die bestellende Person volljährig ist oder nicht. Dies folgt aus dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) DS-GVO.

2.3 Erweitertes Führungszeugnis - Vorlagepflicht vor und während des Beschäftigungsverhältnisses

Immer mal wieder wird gefragt, wann der Arbeitgeber die Vorlage eines (erweiterten) Führungszeugnisses gem. §§ 30 a, 32 V BZRG verlangen darf. Da dies generell nicht erlaubt ist, darf der Arbeitgeber nur solche personen-

22 VG Hannover, Urteil vom 09.11.2021, Az.: 10 A 502/19

bezogenen Daten erheben, verarbeiten und nutzen, die notwendig sind. Nachfolgend wird dargelegt, in welchen Fällen die Vorlage verlangt werden darf.

Erweitertes Führungszeugnis

Gem. § 30 a I BZRG wird einer Person auf Antrag ein erweitertes Führungszeugnis erteilt. Die Erteilung erfolgt, wenn dies in gesetzlichen Bestimmungen unter Bezugnahme auf § 30 a Bundeszentralregistergesetzes (BZRG) vorgesehen ist (Nr. 1) oder wenn das Führungszeugnis für eine berufliche oder ehrenamtliche Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger (Nr. 2 a) oder für eine Tätigkeit, die in vergleichbarer Weise geeignet ist, Kontakt zu Minderjährigen aufzunehmen, benötigt wird (Nr. 2 b).

Einfache Führungszeugnisse enthalten bestimmte Eintragungen nicht. Im erweiterten Führungszeugnis sind gem. § 32 V BZRG neben den Eintragungen des einfachen Führungszeugnisses zusätzlich bestimmte Straftaten (§§ 171, 180 a, 181 a, 183 bis 184 g, 184 i, 184 j, 201 a III StGB, den §§ 225, 232 bis 233 a, 234, 235 StGB oder § 236 StGB) enthalten.

Diese Vorschrift dient dem Schutz von Kindern und Jugendlichen und soll gewährleisten, dass Arbeitgeber auch über sexualstrafrechtliche Verurteilungen im unterschwelligen Strafbereich, die nicht in das einfache Führungszeugnis aufgenommen werden, Kenntnis erhalten.

Ein erweitertes Führungszeugnis muss bei der zuständigen Meldebehörde beantragt werden. Dabei muss eine schriftliche Aufforderung der Stelle, z. B. des Arbeitgebers, vorgelegt werden, die das erweiterte Führungszeugnis verlangt. Der Arbeitgeber muss bestätigen, dass die Voraussetzungen des § 30 a I BZRG vorliegen.

Vorlagepflicht

Die Pflicht zur Vorlage eines erweiterten Führungszeugnisses kann sich aus verschiedenen Gründen ergeben.

Gesetzliche Vorlagepflicht

a) Bundesrecht

aa) Einrichtungen der Kinder und Jugendhilfe

§ 72 a Abs. 1 SGB VIII normiert die Pflicht zur Vorlage eines erweiterten Führungszeugnisses. Danach dürfen Träger der öffentlichen Jugendhilfe für die hauptberufliche Wahrnehmung der Aufgaben in der Kinder- und Jugendhilfe keine einschlägig vorbestraften Personen beschäftigen oder vermitteln. Träger dürfen bei der Einstellung oder Vermittlung und in regelmäßigen Abständen während des Beschäftigungsverhältnisses von den betroffenen Personen die Vorlage eines Führungszeugnisses verlangen.

Gem. § 72 a Abs. 2 SGB VIII sollen die Träger der öffentlichen Jugendhilfe durch Vereinbarungen mit den Trägern der freien Jugendhilfe sicherstellen, dass auch diese keine einschlägig vorbestraften Personen beschäftigen, wenn sie im Bereich der Kinder- und Jugendhilfe i. S. d. § 2 SGB VIII tätig werden. Zu den Trägern der freien Jugendhilfe gehören z. B. Jugendverbände, Jugendgruppen und Initiativen der Jugend, Selbsthilfe- und Initiativgruppen, Wohlfahrtsverbände, wenn und soweit sie Jugendhilfe leisten, sowie Kirchen und Religionsgemeinschaften des öffentlichen Rechts.

Aus Abs. 5 ergibt sich, dass bei Neben- und Ehrenamtlichen nur Einsicht in das erweiterte Führungszeugnis genommen und lediglich der Umstand der Einsichtnahme, das Datum dieser und ob eine Voreintragung besteht, dokumentiert werden dürfen.

Eine derartig ausdrückliche Regelung für Mitarbeitende ist im Gesetz nicht enthalten. Deshalb richtet sich das Verfahren bei dieser Gruppe nach den allgemeinen Regelungen des § 53 KDG. Danach dürfen nur solche personenbezogenen Daten verarbeitet werden, die für die Durchführung des Beschäftigungsverhältnisses erforderlich sind. Erforderlich ist nur die Dokumentation der Tatsache, dass ein erweitertes Führungszeugnis vorgelegen hat, welches keine Eintragungen zu den in § 72a SGB VIII genannten Sexualstraftaten enthalten hat.

Gem. § 45 III Nr. 2 SGB VIII hängt die Erteilung einer Erlaubnis für den Betrieb einer Jugendeinrichtung, in der Kinder oder Jugendliche ganztägig oder stundenweise betreut werden, u. a. davon ab, ob durch die Vorlage erweiterter Führungszeugnisse nach § 30 V und § 30 a I BZRG die Eignung des Personals nachgewiesen wurde.

bb) Aufnahmeeinrichtungen (Asylbegehrender)

Gem.§ 44 Abs. 3 AsylG sollen sich Träger von Aufnahmeeinrichtungen von Personen, die in diesen Einrichtungen mit der Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger oder mit Tätigkeiten, die in vergleichbarer Weise geeignet sind, Kontakt zu Minderjährigen aufzunehmen, betraut sind, zur Prüfung, ob sie für die aufgeführten Tätigkeiten geeignet sind, vor deren Einstellung oder Aufnahme einer dauerhaften ehrenamtlichen Tätigkeit und in regelmäßigen Abständen ein Führungszeugnis nach § 30 Abs. 5 und § 30a Abs. 1 BZRG vorlegen lassen.

cc) Einrichtungen gem. Bundesteilhabegesetz (BTHG)

§ 75 Abs. 2 SGB VIII

In § 75 Abs. 2 SGB VIII, der für den Bereich der Sozialhilfe Anwendung findet, ist geregelt, dass sich Träger der Einrichtungen, ebenfalls ein erweitertes Führungszeugnis gem. § 30 BZRG vorlegen lassen müssen. In diesem Bereich wird nicht zwischen Ehren-, Neben, und Hauptamtlichen differenziert. Es darf nur die Tatsache, dass Einsicht genommen worden ist, das Datum des Zeugnisses und die Information, ob einschlägige Eintragungen vorhanden sind oder nicht vermerkt werden.

§ 124 Abs. 2 S. 3 SGB IX

In § 124 Abs. 2 S. 3 SGB IX, welcher eine Regelung für den Bereich der Eingliederungshilfe für Menschen mit Behinderung enthält, ist ebenfalls vorgesehen, dass die dort beschäftigten (ehrenamtlichen) Personen das erweiterte Führungszeugnis vorlegen. Zur Dokumentation und Aufbewahrung gilt das bereits Gesagte.

Grundsätzlich gilt der § 75 Abs. 2 SGB XII sowohl bei der Erbringung der Eingliederungshilfe für Menschen mit Behinderungen als auch bei Leistungen für (pflegebedürftige) Menschen außerhalb des SGB XI. Gemäß § 75 Abs. 5 SGB XII gilt § 75 Abs. 3 SGB XII nicht für zugelassene Pflegeeinrichtungen nach § 72 SGB XI. Die Befreiung von der Pflicht zur Vorlage erweiterter Führungszeugnisse gilt auch noch für zugelassene Einrichtungen ohne vereinbarte Vergütung (§ 91 SGB XI).

Für diese Bereiche bestehen gesonderte landesrechtliche Regelungen. In Sachsen-Anhalt müssen gem. § 3 Abs. 3 WTG-PersVO (Wohn- und Teilha-

begesetz-Personalverordnung) Beschäftigte in stationären Einrichtungen für ältere und pflegebedürftige Menschen, stationären Hospizen, stationären Einrichtungen und betreuten Wohngruppen für Menschen mit Behinderungen vor der Einstellung oder bei begründeten Zweifeln an der persönlichen Eignung ein erweitertes Führungszeugnis nach § 30 Abs. 5, § 30a Abs. 1 Nr. 1 des BZRG vorlegen, das nicht älter als drei Monate ist.

Welche Mitarbeiter müssen ein erweitertes Führungszeugnis vorlegen?

Nach § 75 Abs. 2 S. 4 SGB XII und § 124 Abs. 2 S. 4 SGB IX müssen sich die Leistungserbringer ein erweitertes Führungszeugnis von Fach- und anderem Betreuungspersonal vorlegen lassen, welches in Wahrnehmung ihrer Aufgaben Kontakt mit Menschen mit Behinderung hat und entweder eingestellt oder dauerhaft ehrenamtlich tätig ist.

Kein Fach- und Betreuungspersonal sind daher z.B. Hausmeister, Verwaltungskräfte, Geschäftsführer einer Einrichtung oder ein Fahrer, die keinen Kontakt zu den schutzwürdigen Personengruppen haben. Bei Praktikanten ist maßgeblich, ob sie eigenständig Betreuungsaufgaben wahrnehmen, so dass ein Vertrauens- und Abhängigkeitsverhältnis zum Klienten entstehen kann.

Freie Mitarbeiter müssen ebenfalls ein erweitertes Führungszeugnis vorlegen, da der Begriff der Beschäftigung in § 75 Abs. 1 S.1 SGB XII und § 124 Abs. 1 S.1 SGB IX mit Blick auf den Schutzzweck der Regelungen zur Vorlage des erweiterten Führungszeugnisses weit auszulegen ist und jedes Vertragsverhältnis zwischen Einrichtung und Mitarbeiter ausreicht. Gleiches gilt für ehrenamtlich Tätige. In der Praxis wird maßgeblich sein, ob die Tätigkeit so beständig ist, dass die Klienten ein besonderes Vertrauens- und Abhängigkeitsverhältnis aufbauen können.

b) Landesrecht

Eine Vorlagepflicht kann sich ferner aufgrund landesrechtlicher Regelungen ergeben. Einige Bundesländer haben für den Schulbereich Regelungen getroffen. So sind Lehramtsreferendare in Mecklenburg-Vorpommern gem. § 3 II Nr. 11 LehVDVO M-V verpflichtet, ihre Eignung durch die Vorlage eines erweiterten Führungszeugnisses nachzuweisen, wenn sie den Vorbe-

reitungsdienst beginnen möchten. In Nordrhein-Westfalen müssen Lehramtsstudierende gem. § 12 Abs. 4 LABG NRW ein erweitertes Führungszeugnis vorlegen, wenn sie ein Praxissemester an öffentlichen Schulen absolvieren möchten. In Niedersachsen gilt aufgrund eines Erlasses vom 01.09.2020 (SVB 11/2020 S. 544) die Regelung, dass bei der Einstellung von lehrendem und nicht lehrendem Personal im schulischen Bereich von den Bewerberinnen und Bewerbern das „Erweiterte Führungszeugnis zur Vorlage bei Behörden" nach §§ 30, 30a, 31 des BZRG zu verlangen ist.

Schutz der personenbezogenen Daten

In § 72 a V SGB VIII ist für die Träger der öffentlichen Jugendhilfe geregelt, dass nur solche Daten aus dem erweiterten Führungszeugnis der in § 72 a III, IV SGB VIII genannten Personengruppen erhoben werden dürfen, welche eine einschlägige Verurteilung betreffen. Eine Speicherung und Nutzung dieser Daten ist nur möglich, soweit dies zum Ausschluss der betreffenden Person von der Tätigkeit, die Anlass der Vorlageverpflichtung war, erforderlich ist. Wird die in Aussicht genommene Tätigkeit nicht aufgenommen oder aufgrund der Einsichtnahme beendet, sind die Daten zu löschen. Im Übrigen sind die Daten spätestens drei Monate nach der Beendigung einer solchen Tätigkeit zu löschen. Ferner sind die Daten vor dem Zugriff Unberechtigter zu schützen. Eine inhaltsgleiche Regelung findet sich in § 75 SGB XII. Der Personenkreis, welcher Zugriff auf das erweiterte Führungszeugnis eines Arbeitnehmers oder Stellenbewerbers erhält, sollte so weit wie möglich beschränkt werden.

Praxistipp: Arbeitgeber sollten sich intern Aufzeichnungen über die erfolgte Vorlage des Führungszeugnisses machen und dieses sodann an den Arbeitnehmer bzw. Stellenbewerber zurückgeben. Der Arbeitgeber überprüft das vorgelegte Führungszeugnis und bestätigt in der Personalakte, dass die Vorlagepflicht erfüllt wurde und ob das Führungszeugnis relevante Einträge enthält. Überträgt der Arbeitgeber die vorgenannten Aufgaben, so sind die mit den Vorgängen betrauten Personen gesondert zur Verschwiegenheit zu verpflichten.

Verwertung von Zufallsfunden

Der Arbeitgeber darf grundsätzlich nur diejenigen Verurteilungen verwerten, welche für die konkrete Tätigkeit relevant sind. Auch im bestehenden

Arbeitsverhältnis dürfen arbeitsrechtliche Konsequenzen nur auf relevante Verurteilungen zurückgeführt werden. Die Verweigerung der Vorlage eines erweiterten Führungszeugnisses berechtigt nicht zum Ausspruch einer Abmahnung, wenn die vertragliche Tätigkeit nicht auf einen Kontakt zu Minderjährigen ausgelegt ist und sich daher keine besondere Gefahrensituation ergeben kann.[23]

Unrechtmäßiges Vorlageverlangen

Wird von einem Arbeitgeber im Rahmen eines Bewerbungsverfahrens unrechtmäßig ein erweitertes Führungszeugnis verlangt, kann dies ggf. Schadenersatzansprüche auslösen. Dabei kommt auch der Ersatz immateriellen Schadens in Betracht, wenn der Arbeitnehmer in seinem Persönlichkeitsrecht verletzt wird[24]. Ebenso können sich derartige Schadenersatzansprüche ergeben, wenn der Arbeitgeber im laufenden Beschäftigungsverhältnis zu Unrecht ein Führungszeugnis verlangt und das Persönlichkeitsrecht des Arbeitnehmers verletzt wird.

Praxistipp: Angesichts der Gefahr von Schadenersatzansprüchen sollten Arbeitgeber nur dann ein erweitertes Führungszeugnis verlangen, wenn dies erforderlich ist. In Zweifelsfällen sollte auf ein Vorlageverlangen verzichtet werden.

2.4 Informationspflichten oftmals nicht im Visier der Verantwortlichen

Bei Überprüfungen stellen wir des Öfteren fest, dass bei einer erweiterten oder im Laufe der Zeit zusätzlichen Datenerfassung die Informationsplichten unbeachtet bleiben.

Nicht nur bei der Anfertigung von Fotos von Beschäftigten für die Veröffentlichung auf einer Webseite eines Unternehmens oder einer Einrichtung sind die Informationspflichten aus § 15 KDG zu beachten (vgl. auch Beitrag unter 5.5. im TB), sondern auch immer dann, wenn personenbezogene Daten erhoben werden. Diese Vorschrift verlangt, dass spätestens zum Zeitpunkt der Datenerhebung diese Person entsprechend informiert wird. Ihr muss also in präziser, transparenter, verständlicher und leicht zugänglicher

23 LAG Hamm, Urteil v. 25.4.2014 – 10 Sa 1718/13
24 Linck, in Schaub ArbR-HdB, 18. Aufl.,2019, § 26 Rn. 10

Form sowie in einer klaren und einfachen Sprache eine Datenschutzerklärung zur Verfügung gestellt werden, die alle Mindestinformationen aus § 15 KDG (Art. 13 DS-GVO) beinhaltet.

Die Informationspflichten sind z. B. bei der durch das Infektionsschutzgesetz vorgeschriebenen Erfassung von Gesundheitsdaten (genesen, geimpft, getestet) im Zusammenhang mit der Datenverarbeitung zum Zwecke der Auskunftserteilung gegenüber zuständigen Behörden, z. B. dem Gesundheitsamt, zu beachten. Auch bei Anmeldeverfahren in Bildungs- und Betreuungseinrichtungen sind die Informationspflichten zu beachten. Bei der Überlassung eines Dienstfahrzeuges muss der Arbeitgeber als Fahrzeughalter sicherstellen, dass der Mitarbeiter über die nötige Fahrerlaubnis verfügt. Diese Kontrolle muss regelmäßig stattfinden. Sie ergibt sich aus § 21 Abs. 1 Nr.2 StVG (Straßenverkehrsgesetz), wonach strafrechtliche Folgen drohen können, wenn der Fahrzeughalter zulässt, dass jemand das Fahrzeug ohne Fahrerlaubnis führt. Daher müssen die Informationspflichten auch in diesem Kontext Beachtung finden.

Merke! Immer wenn personenbezogene Daten erhoben werden, muss die Informationspflicht erfüllt werden. Entweder bei Erhebung direkt beim Betroffenen selbst oder aber über einen Dritten. Die entsprechenden Vorschriften sind in § 14 ff KDG bzw. Art. 12 ff. DS-GVO zu finden. Ausnahmen gibt es nur wenige (§ 15 Abs. 5 KDG), von denen man auch eher zurückhaltend Gebrauch machen sollte. Ein Muster -Informationspflicht für Fotos- befindet sich im Anhang.

2.5 Wachsendes Schadenersatz-Risiko: Missbrauch von Betroffenenrechten

In jüngerer Vergangenheit gab es in den Medien vermehrt Meldungen über den systematischen Missbrauch von Betroffenenrechten, insbesondere das Auskunftsrecht nach Art. 15 DS-GVO. Ziel des Missbrauchs ist die Bewirkung außergerichtlicher Schadenersatzzahlungen.

Welche Fallkonstellationen könnten eintreten?

- Eine Person meldet sich über das **Kontaktformular** der Website einer Einrichtung, gibt ihre Telefonnummer an und bittet um Rückruf. Der dann getätigte Rückruf wird nicht entgegengenommen.

Die Person meldet sich nach einigen Wochen wieder und verlangt Auskunft, welche Daten das Unternehmen gespeichert hat, sowie die Löschung der Daten.

- Eine Person abonniert den **Newsletter** auf der Website des Unternehmens. Anschließend kontaktiert die Person das Unternehmen und verlangt Auskunft über die von ihr gespeicherten Daten sowie deren Löschung.

Wird diesem Begehren nicht termingerecht bzw. nicht richtig entsprochen, meldet sich ein Rechtsanwalt, der im Auftrag seines Mandanten immateriellen Schadenersatz in vierstelliger Höhe (meist 1.500 bis 2.500 €) und Ersatz der angeblich entstandenen Rechtsanwaltskosten (meist 500 bis 600 €) verlangt. Bei Nichtzahlung wird mit Gerichtsverfahren und damit angeblich zwangsläufig weit höheren Kosten sowie einer Beschwerde bei der zuständigen Datenschutzaufsicht gedroht.

Diese Fehler sollten vermieden werden:

- Die betreffenden personenbezogenen Daten aufgrund der (nicht eindeutigen) Anfrage vorschnell löschen und dem Anfragenden mitteilen, dass keine personenbezogenen Daten verarbeitet worden sind.
- Mitteilen, dass keine personenbezogenen Daten des Anfragenden verarbeitet werden, obwohl nachweislich die Telefonnummer und/oder die E-Mail-Adresse des Betroffenen vorliegen.
- Überhaupt nicht reagieren.

Unsere Empfehlung

1. Auskunfts- und Löschungsanfragen sollten nicht ignoriert werden.

2. Korrekte und fristgerechte Bearbeitung sollte sichergestellt werden (Frist: 1 Monat).

3. Wenn ein Anwaltsschreiben mit einer Schadenersatzforderung eingeht, sollte zeitnah reagiert und der Anspruch sachlich begründet bestritten werden.

4. Der Datenschutzbeauftragten sollte in jedem Fall involviert werden.

Weitere Ausführungen zum Umgang mit Auskunftsersuchen sind in unserem Tätigkeitsbericht 2020 auf S. 33 ff zu finden.

2.6 Verpflichtung zur Durchführung von Datenschutzschulungen

Eine ausdrückliche gesetzliche Regelung zur Durchführung von Schulungen für Mitarbeitende ist in den Datenschutzgesetzen nicht vorgesehen. Die Durchführung von Schulungen ist also keine Pflicht im rechtlichen Sinne.

Dennoch kann sie eine Obliegenheit sein, also ein Handeln, das nicht erzwungen werden kann, aber zur Vermeidung von Rechtsnachteilen im Interesse des Verantwortlichen geboten ist. So besteht nach § 7 Abs. 2 KDG (Art. 5 Abs. 2 DS-GVO) für den Verantwortlichen eine Rechenschaftspflicht, in der er nachweisen können muss, dass die Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Die Verarbeitung findet regelmäßig durch die Mitarbeiter statt. Diese müssen also über die Grundsätze informiert sein. Weiterhin ist der Verantwortliche gem. § 26 KDG (Art. 32 DS-GVO) verpflichtet, organisatorische Maßnahmen zu treffen, um ein dem Risiko bei der Verarbeitung personenbezogener Daten angemessenen Schutz zu gewährleisten und einen Nachweis darüber führen zu können. Im Rahmen dieser Maßnahmen wird der Arbeitgeber, der Verantwortliche, nicht umhinkommen, seine Mitarbeiter Vorgehens- und Verhaltensweisen im Zusammenhang mit der Verarbeitung personenbezogener Daten zu erläutern. Schließlich legt § 38 lit. c) KDG als Aufgabe für betriebliche Datenschutzbeauftragte fest, die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften des KDG sowie anderer Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen (Art. 39 Abs. 1 lit a) DS-GVO).

Der Verantwortliche ist also durch die genannten Vorschriften gehalten, seine Mitarbeiter zu unterrichten, zu informieren oder zu beraten. Die Geister scheiden sich häufig an dem Begriff „Schulung“, weil darunter eine Versammlung aller oder großer Teile der Belegschaft verstanden wird, der hohen organisatorischen Aufwand mit sich bringt. Versteht man Schu-

lung als eine wissensvermittelnde Tätigkeit, kann dies auch praxisgerechter gestaltet werden. Präsenzschulungen werden regelmäßig nur in größeren Abständen veranstaltet werden können. In der Zwischenzeit können sich aber Gesetze, Vorschriften oder auch die Unternehmenspraxis verändert haben. Hier ist es sinnvoll, kurzfristig reagieren zu können. „Geeignete Maßnahmen" i. S. d. § 38 KDG sind deshalb z. B. auch Newsletter oder Datenschutzblogs.

Der Verantwortliche ist also nicht zur Durchführung von Präsenzveranstaltungen in regelmäßigen Abständen verpflichtet, sondern dazu, seine Mitarbeitenden über datenschutzrechtliche Regelungen und Verpflichtungen auf dem Laufenden zu halten. Kommt es zur Meldung eines Datenschutzverstoßes, wird die Aufsicht prüfen, ob der Verantwortliche diese Verpflichtung umgesetzt hat.

2.7 Muss eine Datenschutzerklärung auf der Website den Namen des zuständigen Datenschutzbeauftragten veröffentlichen?

Zunächst legt § 36 Abs. 1 KDG fest, dass für kirchliche Stellen gem. § 3 Abs. 1 lit. a) KDG immer ein Datenschutzbeauftragter zu bestellen ist.

Für Kirchliche Stellen gem. § 3 Abs. 1 lit. b) und c) sind betriebliche Datenschutzbeauftragte nur dann zu bestellen, wenn eine der Bedingungen gem. § 36 Abs. 2 lit. a) bis c) KDG erfüllt sind.

Entgegen den staatlichen Regelungen, die eine bestimmte Form der Benennung nicht mehr vorsehen, ist in § 36 Abs. 1 und 2 KDG weiterhin eine schriftliche Benennung gefordert.

§ 36 Abs. 4 KDG verpflichtet Verantwortliche oder den Auftragsverarbeiter die **Kontaktdaten** des betrieblichen Datenschutzbeauftragten zu veröffentlichen. Es besteht in den Kommentierungen zur Parallelvorschrift des staatlichen Rechts (Art. 37 DS-GVO) Einigkeit darin, dass die **Kontaktdaten** nicht den Namen der/des betrieblichen Datenschutzbeauftragten umfassen müssen.[25] Weniger Einigkeit besteht bei der Frage des Umfangs

25 Bäcker in Kühling/Buchner DS-GVO Art. 13 Rn. 22; Knyrim in Ehmann/Sedlmayr DS-GVO Art. 13 Rn. 36; Drewes in Simitis Datenschutzrecht DS-GVO Art. 13 Rn. 68

der Kontaktdaten. Nach hier vertretener Ansicht reicht die Nennung einer funktionalen E-Mail-Adresse als Kontaktdatum des Datenschutzbeauftragten aus.[26]

Gleiches gilt für die Erfüllung der Informationspflicht bei unmittelbarer Datenerhebung gem. § 15 Abs. 1 lit. b) KDG. Die Formulierung „gegebenenfalls" seien die Kontaktdaten des betrieblichen Datenschutzbeauftragten mitzuteilen, eröffnet jedoch keine Wahlmöglichkeit oder ein Ermessen. Vielmehr ist der Fall immer dann gegeben, wenn ein betrieblicher Datenschutzbeauftragter benannt wurde. Dies gilt unabhängig davon, ob er aufgrund des Gesetzes oder freiwillig benannt wurde.

Auf der Website oder in Datenschutzinformationen muss der Name des betrieblichen Datenschutzbeauftragten deshalb nicht benannt werden.

Anders verhält es sich dagegen bei den Angaben im Verzeichnis der Verarbeitungstätigkeiten gem. § 31 Abs. 1 lit a) KDG. Diese Vorschrift sieht die Namensnennung des betrieblichen Datenschutzbeauftragten ausdrücklich vor. Entgegen dem Gesetzeswortlaut ist die Benennung wohl auch dann als erforderlich anzusehen, wenn ein betrieblicher Datenschutzbeauftragter zwar nicht zu benennen ist, gleichwohl aber benannt wurde.

Auch in der Meldung einer Verletzung des Schutzes personenbezogener Daten an die Datenschutzaufsicht gem. § 33 KDG sind gem. § 33 Abs. 3 lit. b) KDG der Name und die Kontaktdaten des betrieblichen Datenschutzbeauftragten mitzuteilen.

Im Verzeichnis der Verarbeitungstätigkeiten und bei der Mitteilung einer Datenschutzverletzung an die Datenschutzaufsicht ist der/die betriebliche Datenschutzbeauftragte namentlich zu benennen.

2.8 Keine Abdingbarkeit von technischen und organisatorischen Maßnahmen

Art. 32 DS-GVO (§ 26 KDG) verpflichtet den Verantwortlichen dazu, technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko an-

26 Ebenso Knyrim in Ehmann/Sedlmayr DS-GVO Art. 13 Rn. 36; weitergehend Paal/Hennemann in Paal/Pauly DS-GVO Art. 13 Rn. 15, die eine ladungsfähige Anschrift fordern.

gemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu gewährleisten.

Abdingbarkeit

Bereits unter der Geltung der früheren Rechtslage, § 9 BDSG a. F., § 6 KDO, wurde in Praxis und Lehre darüber diskutiert, ob diese Regelung zur Disposition von Betroffenen steht, mit der Konsequenz, dass diese den Verantwortlichen von dieser Verpflichtung befreien können.

Diese Frage wird u. a. bei der Versendung von E-Mails virulent. Können Betroffene rechtswirksam in die unverschlüsselte Versendung von personenbezogenen Daten und ggf. auch von solchen besonderer Kategorie einwilligen?

Neu aufgekommen ist diese Frage, nachdem ein Vermerk der Hamburger Datenschutzaufsicht[27] bekannt geworden ist. Darin wird die Ansicht vertreten, der Verantwortliche könne grundsätzlich ein niedrigeres Schutzniveau wählen, wenn Betroffene darin einwilligen.

Die gegenteilige Ansicht wurde in einem Beschluss der Österreichischen Datenschutzbehörde[28] vom 16.11.2018 vertreten. Eine Einwilligung im Sinne des Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DS-GVO sei schon deshalb nicht statthaft, weil die Einwilligung an dieser Stelle nicht dazu diene, eine Rechtsgrundlage für die Datenverarbeitung zu schaffen, sondern um von – gegebenenfalls erforderlichen – Datensicherheitsmaßnahmen zum Nachteil von Betroffenen abweichen zu können.

Einigkeit besteht zwischen beiden Behörden soweit sie vom Verantwortlichen die Gewährleistung eines angemessenen Schutzniveaus fordern. Der Verantwortliche muss also entsprechende technische und organisatorische Maßnahmen bei sich etabliert haben und vorhalten. Die Einwilligung Betroffener kann nach beiden Ansichten nicht dazu führen, Verantwortliche von der Erfüllung einer europäischen Verordnung zu dispensieren. Art. 32 Abs. 1 DS-GVO lässt dem Verantwortlichen keine Wahlmöglichkeit hinsichtlich der grundsätzlichen Gewährleistungspflicht.[29]

27 https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf
28 DSB-D213.692/0001-DSB/2018 vom 16.11.2018
29 Jandt, in Kühling/Buchner, DS-GVO BDSG, 3. Auflage 2020, Rn. 40

Es bleibt dann die Frage, ob Betroffene auf die Anwendung der vom Verantwortlichen grundsätzlich bereitgestellten Sicherungsmaßnahmen durch eine Einwilligung verzichten können. Diese Frage brauchte die Österreichische Datenschutzbehörde nicht zu klären, da die Voraussetzungen dafür in dem zu entscheidenden Fall nicht gegeben waren. In ihrem Vermerk spricht sich die Hamburgische Datenschutzbehörde für die Möglichkeit einer Abdingbarkeit von technisch-organisatorischen Maßnahmen aus, wenn Betroffene unter der o. g. Voraussetzung eine entsprechende Einwilligung erteilt haben. Wenn Betroffene mit einer Einwilligung darüber entscheiden können, „ob" ihre personenbezogenen Daten verarbeitet werden können, müssen sie erst recht entscheiden können, „wie" diese verarbeitet werden.

Diese Schlussfolgerung ist keineswegs zwingend. Die Möglichkeit der Einwilligung gem. Art. 6 Abs. 1 lit. a) DS-GVO (§ 8 KDG) steht systematisch im Zusammenhang mit der Frage der Zulässigkeit der Datenverarbeitung, nicht aber mit den spezifischen Pflichten bei der Umsetzung.[30]Die Einwilligung erlaubt nur die ansonsten verbotene Verarbeitung personenbezogener Daten. Dies muss aber in datenschutzkonformer Weise geschehen. Die rechtfertigende Wirkung, die Art. 6 Abs. 1 lit. a) DS-GVO (§ 8 KDG) der Einwilligung zugesteht, bezieht sich systematisch nur auf das „Ob" der Verarbeitung, nicht aber auch vollumfänglich auf das „Wie".[31]Würde man die Einwilligung soweit für zulässig erachten, wie dies im Vermerk der Hamburger Datenschutzbehörde zum Ausdruck kommt, handelte es sich nicht mehr um eine Einwilligung, sondern um einen Verzicht auf Datenschutz. Noch in seinem Tätigkeitsbericht 2018 hat der Hamburgische Datenschutzbeauftragte zur alten Rechtslage einen Verschlüsselungsverzicht nur dann für zulässig angesehen, wenn die „Umstände der Verarbeitung" einen solchen rechtfertigen.[32] Als Beispiel für solche Umstände wurden dort medizinische Notfälle und wechselnder Auslandsaufenthalt benannt. Aus solchen rechtfertigenden Umständen kann aber keine generelle Aussage abgeleitet werden. Insoweit leidet der neue Vermerk darunter, dass die Frage der Zulässigkeit einer so weitreichenden Einwilligung ausschließlich aus Sicht Betroffener in den Blick genommen wird. Aus Sicht von Verantwortlichen ermöglicht diese Rechtsauffassung, Betroffene gleich zu Beginn eines Ver-

30 Jandt, in Kühling/Buchner, DS-GVO BDSG, 3. Auflage 2020, Rn. 40
31 Paal, in Pall Pauly, DS-GVO, 3. Auflage 2021, Rn. 4a
32 HmbBfDI, TB 2018, S.121

tragsverhältnisses eine entsprechende Einwilligungserklärung unterzeichnen zu lassen, um sich auf diese Weise die Möglichkeit einer vereinfachten Kommunikation zu sichern. Dabei ist es kein Hindernis, dass der Verantwortliche eine Verschlüsselungstechnik vorhalten muss, die er aber praktisch nicht nutzt.

Für die Gewährleistung eines einheitlichen Datenschutzniveaus innerhalb der Europäischen Union und um eine naheliegende Umgehung datenschutzrechtlicher Vorschriften zu vermeiden, ist die Möglichkeit der Abdingbarkeit von technisch-organisatorischen Maßnahmen durch eine Einwilligung Betroffener abzulehnen.

Etwas anderes kann nach hier vertretener Ansicht nur dann gelten, wenn Betroffene im Einzelfall vom Verantwortlichen über die Risiken einer Einwilligung in den Verzicht technisch-organisatorischer Maßnahmen aufgeklärt worden sind und der Betroffene nachweislich auf eigenes Verlangen entgegen dieser Belehrung auf die ungeschützte Übersendung besteht.

Eine generelle Einwilligungserklärung bleibt zur Sicherstellung der Persönlichkeitsrechte unwirksam.[33] Demgegenüber gewährt eine aufgeklärte, informierte und freiwillige Einwilligung auf Veranlassung Betroffener deren Datensouveränität.

Art der Verschlüsselung

Darüber hinaus ist zu berücksichtigen, welche Art der Verschlüsselung zu wählen ist. Bei der Transportverschlüsselung (TLS) wird die Übertragung der E-Mail zwischen den beteiligten E-Mail-Servern gesichert durch Verschlüsslung übertragen.[34] Generell wird die Verwendung einer Transportverschlüsselung datenschutzrechtlich ausreichend sein, sofern keine Anhaltspunkte für besonders sensible Daten bestehen oder sonstige Umstände hinzutreten[35]. Die Kommunikation mittels obligatorisch transportverschlüsselter E-Mails ist auch im geschäftlichen Verkehr durchaus als sozialadäquat und wohl derzeit noch als Stand der Technik einzustufen[36].

33 DSK, Beschluss vom 24.11.2021, TOP 7
34 Ausführliche Darstellung: KDSA Ost, TB 2020, Seite 89 ff.
35 VG Mainz, Urteil vom 17.12.2020 - 1 K 778/19.MZ
36 Gasteyer/Säljemar, NJW 2020, 1768 [1771

Eine Ende-zu-Ende-Verschlüsselung zeichnet sich demgegenüber dadurch aus, dass eine Entschlüsselung des Inhalts nur den Kommunikationspartnern (Absender und Empfänger) möglich ist, also nur derjenige den Inhalt der Nachricht zur Kenntnis nehmen kann, der auch den passenden Entschlüsselungsmechanismus hat.

Bei personenbezogenen Daten, die unter Art. 9 oder Art. 10 DS-GVO (§ 4 Nr. 2, § 12 KDG) fallen, sind in jedem Fall „besondere Schutzmaßnahmen" zu ergreifen, da insoweit schon aufgrund der allgemeinen datenschutzrechtlichen Wertung stets von einem hohen Risiko ausgegangen werden muss[37]. Eine angebrachte „besondere Schutzmaßnahme" wäre z.B. die zu übermittelnden sensiblen Daten in einer passwortgeschützte ZIP Datei als E-Mail-Anlage zu versenden. Eine mit Passwort geschützte PDF-Datei ist eine weitere Möglichkeit. Den damit verbundenen Implementierungsaufwand kann man in Bezug auf die Vertraulichkeit vernachlässigen. Bei einer fehlerhaften Zustellung einer Nachricht mit sensiblen Informationen an falsche Empfänger, z.B. durch einen Tippfehler bei Eingabe der E-Mail-Adresse, würde TLS nicht mehr den erforderlichen Schutz bringen. Sobald die Nachricht beim Empfänger in seinem Postfach eingegangen ist, liegt diese im Klartext vor. Ein solcher Fehlversand wäre deshalb als Datenschutzverstoß zu werten, da die erforderliche Sorgfalt bei der Versendung personenbezogener Daten besonderer Kategorie außeracht gelassen wäre.

Sind die sensiblen Informationen in einer verschlüsselten Anlage enthalten, wo das „Geheimnis" (Passwort) um die Anlage zu entschlüsseln nur den berechtigten Empfängern bekannt ist, können alle anderen Empfänger (Dritte) nicht auf den Inhalt der Anlagen zugreifen. Sie würden nur Kenntnis von dem unverschlüsselten Inhalt in der E-Mail-Nachricht erlangen. Die sensiblen Informationen in der Anlage bleiben geschützt.

2.9 Original ersetzendes Scannen und Datenschutz

Die Unterhaltung von Archiven ist eine ebenso anspruchsvolle wie aufwändige Verpflichtung. Werden darin Papierakten aufbewahrt, nehmen diese

37 VG Mainz, Urteil vom 17.12.2020 - 1 K 778/19.MZ

viel Platz in Anspruch und erzeugen damit Kosten. Viele Einrichtungen gehen deshalb dazu über, die Akten einzuscannen und danach die Originale zu vernichten. Dieser Vorgang, der als „Ersetzendes Scannen“ bezeichnet wird, wirft die Frage auf, ob er datenschutzrechtlichen Vorgaben widerspricht. Konkret: Stellt es einen Verstoß dar, dass dem Verantwortlichen die Originale nicht mehr zur Verfügung stehen?

§ 26 Abs. 1 lit b) KDG (Art. 32 Abs. 1 lit. b) DS-GVO) verpflichtet den Verantwortlichen, technisch organisatorische Maßnahmen zu etablieren, um die Verfügbarkeit der Systeme im Zusammenhang mit der Verarbeitung sicherzustellen und in lit c) die Verfügbarkeit der personenbezogenen Daten nach einem Zwischenfall wiederherstellen zu können. Beide Regelungen verpflichten dazu, personenbezogene Daten zu erhalten bzw. zugänglich zu halten. Eine Aufbewahrungspflicht des Originals wird damit nicht gefordert. Eine entsprechende Regelung ist auch an anderer Stelle im Gesetz nicht zu finden.

Die personenbezogenen Daten müssen erhalten werden. In welcher Form dies geschieht ist nicht vorgeschrieben. Für den Gesundheitsbereich ist die Führung einer digitalen Patientenakte durch § 630 f BGB ausdrücklich zugelassen.

Werden Originale gescannt und dabei die Richtlinien[38] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eingehalten, entsteht ein digitales Dokument, welches die datenschutzrechtlichen Vorgaben erfüllt. Darüber hinaus ist das so erzeugte Dokument auch geeignet im zivilen Recht zur Beweisführung zu dienen. Mit den Worten des OLG München: „Die These …, dass nur die ärztliche Originaldokumentation beweiskräftig ist, findet weder in Gesetz und Recht noch in der Rechtsprechung eine Stütze[39]“.

Fazit: Das Vernichten des Originals nach einem, den Vorschriften des BSI entsprechenden, Einscannen stellt keinen Datenschutzverstoß dar, auch wenn die Löschungsfristen noch nicht abgelaufen sind.

38 BSI TR-03138 RESISCAN
39 OLG München, Beschluss vom 28. Mai 2013, Az.: 1 U 844/13.

2.10 Schadenersatz und Erheblichkeitsschwelle

Im Gegensatz zur Kirchlichen Datenschutzordnung (KDO) sind nach dem Kirchliche Datenschutzgesetz (KDG) seit seinem Inkrafttreten 2018 ausdrücklich Nichtvermögensschäden, also immaterielle Schäden, auszugleichen. Darunter fallen z. B. Diskriminierung, Identitätsdiebstahl oder -betrug, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugte Aufhebung der Pseudonymisierung oder andere gesellschaftliche Nachteile[40]. Wann ein ausgleichsfähiger immaterieller Schaden vorliegt, wird derzeit von den Gerichten unterschiedlich bewertet. Nach einer weiten Auslegung können Betroffene für jede Verletzung datenschutzrechtlicher Vorschriften durch Verarbeitung ihrer personenbezogenen Daten auch ein angemessenes Schmerzensgeld verlangen. Insbesondere bei der Zugänglichmachung von Daten einer betroffenen Person für Dritte ohne ihr Einverständnis wird ein Schadenersatzanspruch auch einen immateriellen Schaden abzudecken haben, der diese öffentliche „Bloßstellung" kompensiert[41]. Der immaterielle Schaden läge nach dieser Ansicht allein in der unrechtmäßigen Verarbeitung[42]. In diesem Sinne haben einige Gerichte den Betroffenen Schadenersatz zugesprochen[43].

Andere Gerichte tendieren eher zu einer einschränkenden Auslegung[44]. Danach soll nicht bereits jede individuell empfundene Unannehmlichkeit oder jeder Bagatellverstoß einen Schadenersatzanspruch begründen[45]. Eine Verpflichtung zum Ausgleich eines immateriellen Schadens müsste vielmehr eine gewisse Erheblichkeitsschwelle überschreiten.

Auch das Amtsgericht Goslar[46] sah eine solche Erheblichkeitsschwelle für die Stattgabe einer Schmerzensgeldklage als erforderlich an. Gegen diese Entscheidung hat sich aber der Kläger mit einer Beschwerde vor dem Bundesverfassungsgericht (BVerfG) gewandt. Dieses gab dem Kläger in seiner Einschätzung Recht, das Amtsgericht hätte die umstrittene Rechtsfrage nicht selbst entscheiden dürfen.

40 Erwägungsgrund 75 zur DS-GVO
41 Nemitz, in Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 82 Rn. 13
42 Wybitul, NJW 2019, 3265 (3266)
43 LG Darmstadt, Urteil vom 26.05.2020 - 13 O 244/19 Rn. 76; ArbG Düsseldorf, Urteil vom. 05.03.2020 - 9 Ca 6557/18 (nicht rechtskräftig Nachinstanz LAG Düsseldorf, Az.: 14 Sa 294/20)
44 OLG Dresden, Beschluss vom 11.06.2019 – 4 U 760/19; LG Karlsruhe, Urteil vom 02.08.2019 – 8 O 26/19
45 OLG Dresden a.a.O.
46 AG Goslar, Urteil vom 27.09.2019 - 28 C 7/19

Nach Art. 82 Abs. 1 DS-GVO (entspricht § 50 Abs. 1 KDG) hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen.

Dieser Geldentschädigungsanspruch ist in der Rechtsprechung des Gerichtshofs der Europäischen Union nicht erschöpfend geklärt. Deshalb hätte das Amtsgericht ein Vorabentscheidungsersuchen an den Europäischen Gerichtshof (EuGH) stellen müssen. Damit hat das BVerfG die hochstrittige Rechtsfrage zwar nicht geklärt, es jedoch den Gerichten schwerer gemacht, einfach mit dem Argument der Unerheblichkeit über die Schadenersatzforderung hinwegzugehen. Bis zu einer Entscheidung des EuGHs werden Monate vergehen. In dieser Zeit werden die Gerichte auf Schmerzensgeld wegen eines Datenschutzverstoßes gerichtete Klagen entweder bis zur Entscheidung des EuGHs aussetzen oder Entscheidungen fällen, die mit Rechtsmitteln angegriffen werden können.

In jedem Fall ist es für Verantwortliche ein zusätzlicher Grund, auf die Einhaltung datenschutzrechtlicher Vorschriften zu achten. Dies gilt insbesondere für kirchliche Stellen, die öffentlich-rechtlich verfasst sind und gegen die wegen § 51 Abs. 6 KDG keine Geldbußen verhängt werden können. Das schließt nämlich nicht aus, dass diese Stellen von Betroffenen auf Schadenersatz in Anspruch genommen werden können.

Nach einer Entscheidung des Landesarbeitsgerichts Nürnberg[47] entscheiden über Schadenersatzansprüche wegen einer Datenschutzverletzung nicht die kirchlichen Datenschutzgerichte, sondern die staatlichen Zivilgerichte.

2.11 Spenderlisten und die Herausgabe der Spendernamen

Nicht nur Traueranzeigen enthalten oftmals die Bitte, auf Blumen- oder Kranzspenden zu verzichten und stattdessen einer sozialen Einrichtung zu spenden, sondern auch anlässlich von Jubiläen wird zum Teil darum gebeten, auf Geschenke zu verzichten und stattdessen an eine soziale Einrichtung zu spenden. Gerade im Bereich der Hospiz- und Palliativarbeit sind

47 LAG Nürnberg, Beschluss v. 29.05.2020 – 8 Ta 36/20

solche Spendenaufrufe die Regel und entsprechen dem letzten Willen des Verstorbenen oder dem Wunsch der Hinterbliebenen.

Welche Rolle spielt hierbei der Datenschutz?

Name und Spendensumme sind unstreitig personenbezogene Daten im Sinne des § 4 Nr. 1 KDG (Art. 4 Nr. 1 DS-GVO). Die Weitergabe dieser Daten stellt eine datenschutzrechtliche Verarbeitung im Sinne von § 4 Nr. 3 KDG (Art. 4 Nr. 2 DS-GVO) dar und bedarf für deren Übermittlung an die Hinterbliebenen bzw. Veranlasser der Spende einer Rechtsgrundlage. In Frage kommen als Rechtsgrundlage eine vertragliche Beziehung, eine rechtliche Verpflichtung, ein berechtigtes Interesse der Angehörigen des Spendenveranlassers oder die Einwilligung des Spenders.

Seien es die Caritas-Einrichtungen, die Diakonie oder sonstige gemeinnützige Organisationen und Vereine, sie alle kennen die Situation, dass sich nach einem erfolgreichen Spendenaufruf im Rahmen einer Traueranzeige oder eines anderen Anlasses, die Hinterbliebenen bzw. die Spendenveranlasser in Form eines persönlichen Anschreibens bei den Spendern bedanken möchten. Dafür benötigen sie jedoch die Namen der Spender. Diese können sie nur bekommen, indem sie sich an die soziale Einrichtung wenden, da die Namen dort aus den Überweisungen ersichtlich sind. Doch wie sieht die datenschutzrechtliche Einordung aus und darf die Liste mit den Spenderdaten überhaupt übermittelt werden?

Vertrag oder rechtliche Verpflichtung als Ermächtigungsgrundlage?

Da zwischen den Spendern und den Angehörigen keine vertragliche Beziehung besteht, scheidet § 6 Abs. 1 lit. c) KDG (Art. 6 Abs. 1 S. 1 lit. b) DS-GVO) als Ermächtigungsgrundlage für die Weitergabe der Spenderdaten aus. Eine zivilrechtliche Vertragsbeziehung besteht allenfalls durch die Überweisung zwischen Spender und Empfänger der Spende.

Auch besteht keine rechtliche Verpflichtung, die die Herausgabe der Spendernamen rechtfertigen könnte. Sofern ein Spender seine Kontaktdaten angibt, erfolgt dies regelmäßig zum Zwecke der Ausstellung einer Spendenbescheinigung. Hieraus kann aber nicht abgeleitet werden, dass der Spender die Daten zum Zwecke der Weitergabe an die Hinterbliebenen für

eine Danksagung übermittelte. § 6 Abs. 1 lit. c) KDG scheidet als Ermächtigungsgrundlage mithin aus.

Berechtigtes Interesse?

Auch die Weitergabe der Spenderdaten aufgrund § 6 Abs. lit. g) KDG (Art. 6 Abs. 1 S.1 lit. f) DS-GVO) wird schwer konstruierbar sein. Zwar haben die Hinterbliebenen bzw. die Spendenveranlasser den Wunsch sich bei den Spendern zu bedanken, jedoch ist das Interesse der Angehörigen mit den Interessen der Spender abzuwägen. Pauschal von einem überwiegenden Interesse der Angehörigen oder des Spendenveranlassers auszugehen, wäre falsch und würde nicht berücksichtigen, dass manche Spender ungenannt bleiben wollen und nicht damit rechnen müssen, dass ihre Daten weitergegeben werden. Es liegen daher gute Gründe vor, von einem Interesse des Spenders an der Wahrung seiner Anonymität auszugehen. Damit scheidet auch ein berechtigtes Interesse als Rechtsgrundlage aus

Einwilligung?

Letztlich bleibt als Ermächtigungsgrundlage noch die Einwilligung gem. § 6 Abs. 1 lit. b) KDG (Art. 6 Abs. 1 S. 1 lit. a) DS-GVO). Eine Einwilligung hat jedoch informiert zu erfolgen, d.h. der Einwilligende muss zum Zeitpunkt der Einwilligung wissen, welche Konsequenzen seine Einwilligung hat. Die Einwilligung muss zudem gem. § 8 Abs. 2 KDG schriftlich erfolgen. Die Einwilligung der Spender als Rechtsgrundlage wird daher in der Praxis wohl regelmäßig scheitern. In der Regel findet der Spendenaufruf über eine Traueranzeige in einer oder mehreren regionalen Tageszeitungen oder in der Einladung eines Jubilars statt. Ein Einwilligungstext mit allen erforderlichen Informationen am Ende einer Traueranzeige wäre wohl sehr befremdlich und würde den Rahmen sprengen. Darüber hinaus muss die Einwilligung grundsätzlich aktiv und in dokumentierter Weise erfolgen, was vorliegend kaum möglich erscheint. Daher scheidet auch die Einwilligung als Rechtsgrundlage aus.

Was nun?

Mit konsequenter Anwendung des KDG dürfen die Spenderdaten nicht weitergegeben werden, d. h. die Angehörigen bzw. die Spendenveranlasser haben folglich keinen Anspruch auf die Herausgabe der Spendernamen.

Unproblematisch ist die Mitteilung der gespendeten Gesamtsumme. Diese Information können die Hinterbliebenen/ Spendenveranlasser dann in einer allgemein formulierten Danksagung zum Beispiel in einer weiteren Anzeige verwenden.

Sofern die Angehörigen/Spendenveranlasser auf die Kenntnis der einzelnen Spender und der Beträge bestehen, bleibt ihnen nur der Weg, dass sie die Spenden selbst einsammeln und die gespendete Summe im Anschluss an die Einrichtung weiterleiten. So sind sie selbst Verantwortliche und die Spenderdaten werden direkt bei ihnen erhoben. Diese datenschutzrechtliche sichere Lösung hat jedoch zur Folge, dass Spender keine Spendenbescheinigung erhalten, da die Angehörigen oder Jubilare eine solche nicht ausstellen können. Auch die bedachte Einrichtung kann den einzelnen Spendern keine Spendenbescheinigung ausstellen.

Dies könnte möglicherweise zur Folge haben, dass Spenden teilweise ausbleiben oder geringer ausfallen als ursprünglich gewollt. Ebenfalls bei dieser Lösung unberücksichtigt bleibt der Fall, dass sich die von der Spende berücksichtigte Einrichtung bei den Spendern bedanken möchte und hierfür ebenfalls gerne die Spenderdaten hätten. Das Problem würde also nur verlagert.

Viele Einrichtungen und Organisationen geben auf ihren Web-Seiten an, dass im Nachgang einer Spendenaktion die Übersendung einer Spendenliste erfolgt, wobei einige angeben, dass auch die jeweilige Höhe der Spende mitgeteilt wird. Datenschutzrechtlich ist das, wie dargelegt, unzulässig. Mitgeteilt werden darf nur die Gesamtsumme der Spenden.

Unsere Empfehlung: Transparenz schaffen!

Steht ein weiterer Spendenaufruf an und soll die Spende direkt an die Einrichtung überwiesen werden, sollten die Veranlasser der Spende über die rechtlichen Gegebenheiten informiert werden. So kann zumindest verhindert werden, dass sich diese im Nachgang über die Versagung der Herausgabe ärgern. Die Spender sollten vorab, z. B. über die Information auf der Webseite der jeweiligen Einrichtung zur Spende, darüber informiert werden, dass sie sich mit der Bitte um Erteilung einer Spendenquittung direkt an die bedachte Einrichtung wenden können.

2.12 Kinderfotos im Internet

Die KDSA Ost hat wiederholt auf die Probleme aufmerksam gemacht, die mit der Veröffentlichung von Kinderfotos verbunden sind. Eine neue Entscheidung des OLG Düsseldorf[48] veranlasste uns erneut auf dieses Thema einzugehen.

In dem Fall des OLG Düsseldorf ging es um die Einwilligung in die Veröffentlichung eines Kinderfotos. Die Eltern des Kindes leben getrennt. Steht den Eltern die gemeinsame Sorge für das Kind zu, hat der Elternteil, bei dem sich das Kind gewöhnlich aufhält, gem. § 1687 Abs. 1 BGB die Befugnis zur alleinigen Entscheidung in Angelegenheiten des täglichen Lebens.

In Angelegenheiten von erheblicher Bedeutung müssen dagegen beide Elternteile im gegenseitigen Einvernehmen zustimmen bzw. ihre Einwilligung erteilen.

Das OLG Düsseldorf hat noch einmal, wie bereits zuvor das OLG Oldenburg[49], entschieden, dass es sich bei der Veröffentlichung von Fotos eines Kindes im Internet, um eine Angelegenheit von erheblicher Bedeutung handelt.

Das öffentliche Teilen der Bilder bei Facebook und bei Instagram oder ihre Einstellung auf einer Webseite hat schwer abzuändernde Auswirkungen auf die Entwicklung des Kindes.[50] Insbesondere bei Veröffentlichung von Fotos im Internet ist dieses Recht in erhöhtem Maße gefährdet, da der Personenkreis, dem die Fotos zugänglich gemacht werden, theoretisch unbegrenzt ist, eine verlässliche Löschung von Fotos nicht möglich und eine etwaige Weiterverbreitung kaum kontrollierbar ist.[51] Einmal veröffentlichte Kinderfotos der Abgebildeten werden potenziell für ihr gesamtes Leben einem unbeschränkten Personenkreis zur Einsichtnahme zur Verfügung stehen. Diese Tatsache greift also weit über das Kindesalter hinaus massiv in die Persönlichkeit und die Privatsphäre der abgebildeten Personen ein.

48 OLG Düsseldorf, Beschluss v. 20.7.2021 – 1 UF 74/21
49 OLG Oldenburg, Beschluss v. 24.05.2018 - 13 W 10/18
50 OLG Düsseldorf, Beschluss v. 20.7.2021 – 1 UF 74/21
51 OLG Oldenburg, Beschluss v. 24.05.2018 - 13 W 10/18

Das Gericht schließt daraus, dass bei getrenntlebenden Elternteilen, denen das gemeinschaftliche Sorgerecht zusteht, beide Elternteile einer Veröffentlichung von Kinderfotos im Internet zustimmen müssen.

Einrichtungen, die diese Rechtswirklichkeit missachten, laufen Gefahr, Fotos unrechtmäßig zu verarbeiten. Sie müssen in diesem Fall mit einer Sanktion durch die Datenschutzaufsicht rechnen, ebenso aber mit entsprechenden Schadenersatzforderungen.

Die eindringlichen Hinweise des Gerichts im Hinblick auf die Auswirkungen einer Fotoveröffentlichung im Internet und die damit verbundenen Gefahren sollte aber auch alle anderen Sorgeberechtigten davon abhalten, Fotos ihrer Kinder in sozialen Medien zu veröffentlichen. Es kann nicht oft genug darauf hingewiesen werden, dass mit einer Veröffentlichung eines Fotos im Internet jede Kontrolle über dessen weitere Verwendung aufgegeben wird.

2.13 Datenschutz unter Corona

2.13.1 Luca-App datenschutzrechtlich zweifelhaft und überflüssig

Die Luca-App stand bereits nach der Veröffentlichung in der öffentlichen Kritik. Zum einen aufgrund von Sicherheits- und Datenschutzbedenken und zum anderen wegen der zentralen Speicherung persönlicher Daten. Ungeachtet der Kritik schlossen einige Behörden und die meisten Bundesländer Vertragsbeziehungen mit dem Anbieter, um der Flut an Nachverfolgungen zu begegnen.

Bei der von der Bundesregierung in Auftrag gegebenen Entwicklung der Corona-Warn-App (CWA) stand die Sicherheit und der Datenschutz im Vordergrund. Unter Kritikern wurde aufgrund der hohen Anforderungen an den Datenschutz der Nutzeffekt in Frage gestellt.

An den weiteren Entwicklungen der CWA, u.a. auch im Vergleich zu anderen Produkten, wurde immer deutlicher, dass es die richtige Entscheidung war, den Datenschutz und die Sicherheit bereits in der Entwicklungsphase

zu berücksichtigen. Nach und nach konnten trotz der hohen Sicherheitsanforderungen viele weitere Funktionen, wie z. B. Check-In-Funktion, Tagebuch, Zertifikatserweiterungen u.a. mit Kompatibilität zu anderen Produkten, integriert werden. Bei der Installation der App werden keine persönlichen Daten erhoben.

Bei der Nutzung der Luca-App werden hingegen u.a. persönliche Daten, wie Name, E-Mail-Adresse und Telefonnummer, zur Registrierung benötigt. Im Gegensatz zur CWA, bei der sich die persönlichen Daten nur auf dem eigenen Gerät befinden, werden bei der Luca-App die Daten aller Nutzer in einem zentralen Kontaktnachverfolgungssystem gespeichert und verarbeitet. Für Sicherheits- und Datenschutzexperten bedeutet so eine zentrale Datenspeicherung, zum Teil mit sensiblen Gesundheitsinformationen, ein erhöhtes Risiko der Datenverarbeitung. Die Datenschutzkonferenz der Länder (DSK) hatte eingeschätzt, dass eine unbefugte Einsicht in so einen sensiblen Datenbestand zu einer schweren Beeinträchtigung für die Einzelnen und das Gemeinwesen führen kann.

Ursprünglich war über die CWA nur eine Risikowarnung des Nutzers der App nach einem Kontakt möglich. Die Kontaktnachverfolgung oblag dem Gesundheitsamt. Bei der Luca-App konnte eine positiv auf SARS-CoV-2 getestete Person ihre Historie (Kontaktdatenbuch) dem Gesundheitsamt mittels einer Transaktionsnummer (TAN) freigeben. Dadurch sendet die Luca-App des positiv Getesteten alle Veranstaltungsorte der letzten 14 Tage (laut der Programm-Historie) an das Luca-System. Das Gesundheitsamt fordert dann über das Luca-System die entsprechenden Veranstalter auf, die Kontaktdaten aller Gäste, die zur selben Zeit wie der Meldende am jeweiligen Veranstaltungsort waren, ans Gesundheitsamt zu übertragen. Damit erhält das Gesundheitsamt die Kontaktdaten aller „betroffenen" Gäste. Über die Luca-App kann das Gesundheitsamt alle „Betroffenen" informieren.

Mit der Erweiterung der CWA um die Check-In-Funktion wurde hingegen ein anderer Ansatz verfolgt. Die Angaben über den Restaurant- oder Konzertbesuch werden in der CWA im eigenen Kontakttagebuch auf dem Endgerät gespeichert - also nur auf dem eigenen Smartphone. Im Fall der Fälle werden Personen über die CWA informiert, so wie es

bislang bei einer Risiko-Begegnung der Fall war. Behörden und Gesundheitsämter sind somit außen vor. Die Nutzer sollen die Empfehlung des Robert Koch Institutes beachten. Diese lautet:

> *„Die Nutzer*in erhält die Aufforderung, wenn möglich, sich nach Hause zu begeben und Begegnungen zu reduzieren sowie Verhaltenshinweise bei auftretenden Symptomen zu beachten. Die Nutzer*in wird aufgefordert, weitere Schritte mit dem Hausarzt, dem kassenärztlichen Bereitschaftsdienst bzw. dem örtlichen Gesundheitsamt abzustimmen."*

Gewarnte Personen können demnach selbst entscheiden, wem sie sich anvertrauen und ggf. wo und von wem sie einen Test durchführen lassen. Dieses Verfahren wahrt die Persönlichkeitsrechte Betroffener. Die CWA setzt auf Eigenverantwortung.

Gesundheitsämtern die personenbezogenen Daten all derer zu übermitteln, die sich zum selben Zeitpunkt wie ein Infizierter z.B. in einem Restaurant oder einem anderen Standort aufgehalten haben (wie bei der Luca-App), ist nur dann sinnvoll, wenn Behörden oder Ämter Betroffenen gegenüber konkrete Anweisungen aussprechen können/müssen. Gesundheitsämtern stehen aber keine Befugnisse zu, allein aufgrund der Meldung durch die Luca-App Schutzmaßnahmen, wie z.B. „Absonderungen" oder einen Zwangstest anzuordnen, da dafür regelmäßig ein Verwaltungsakt (Quarantäneanordnung) erforderlich ist. Da die Luca-App lediglich die Richtigkeit der Telefonnummer verifiziert, dürfte sich das als schwierig erweisen.

Behörden und Ämter wurden mit dem Luca-App-System nicht unbedingt so unterstützt, wie es angedacht war. Manuelle geführte Listen und elektronischen Kontaktnachverfolgung trafen aufeinander und führten teilweise zur Überforderung bei der Abarbeitung der Kontakte. Erschwerend hinzu kam die Problematik mit den teilweise fiktiven Telefonnummern, denn auch mit der Luca-App können sich, wie bei Verwendung manuell geführter Listen, Besucher hinter einem Pseudonym verstecken. Genau das sollte die Anwendung eigentlich verhindern und damit die Kontaktverfolgung einfacher und zuverlässiger machen. Was nicht erfolgt ist.

Der aufgezeigte zeitliche Verzug bei der Luca-App wird bei der CWA umgangen, da Kontaktpersonen direkt durch die App informiert werden können, sowohl bei der ursprünglichen Risikowarnung und auch nach der Erweiterung über die Check-In-Funktion. Auch mit der Erweiterung zum Einchecken z.B. mit einem QR-Code der Luca-App bleiben in der CWA weiterhin alle persönlichen Daten sicher auf dem eigenen System. Eine Weitergabe der Daten an ein Kontaktnachverfolgungssystem wie bei der Luca-App war niemals vorgesehen.

Zusammenfassung

Die Luca-App sowie vergleichbare Systeme hatten ihre Berechtigung, solange sich das Bundesministerium für Gesundheit dagegen sperrte, die CWA mit Funktionen zur Kontaktnachverfolgung ausstatten zu lassen. Mit den Erweiterungen der CWA wurden die anderen Systeme überflüssig. Die CWA ist datenschutzrechtlich unangefochten und mit über 42 Mio. Usern das führende System. Daneben Apps zu etablieren, die aufgrund ihrer zentralen Datenspeicherung und verschiedener Schnittstellen schwere Beeinträchtigungen für die Einzelnen und das Gemeinwesen nicht ausschließen können, ist auch für die Pandemiebekämpfung nicht zweckmäßig. Auch wenn man den Nutzern der CWA unterstellt, sie würden die ihnen angezeigten Warnungen ignorieren oder sich nicht entsprechend den Empfehlungen verhalten, erreichte die Luca-App mit der Einbindung der Gesundheitsämter kein besseres Ergebnis.

Der Zweck, die Gesundheitsämter zu entlasten, ist nicht erfüllt worden. Für die Nutzer besteht ein deutlich höheres Datenschutzrisiko. Daher haben sich viele Bundesländer mittlerweile gegen eine Vertragsverlängerung mit Luca entschieden.

Ein Fall aus Mainz, bei dem Polizeibeamte die Daten von Gaststättenbesucher zur Zeugenbefragung angefragt hatten, sorgte für Aufsehen und macht mehr als deutlich welchen Stellenwert der Datenschutz hat.

Die Luca-App hat ausgedient, auch weil eine Kontaktnachverfolgung nicht mehr vorgeschrieben ist. Die Daten hat der Betreiber jedoch gespeichert und offensichtlich nicht vor, diese zu löschen. Luca hat nach eigenen Angaben weitreichende Pläne.

Die App soll breiter aufgestellt werden. Die Funktionen sollen dabei erheblich erweitert werden. Luca überlegt, den Impfnachweis und den Personalausweis in der App zu verbinden, das soll die Kontrollen einfacher machen. Noch weiter gehen Pläne, eine eigene Bezahlfunktion in Gaststätten, die Luca nutzen, einzubauen.

Diese Pläne zeigen das Risiko einer solchen zentralen Datenspeicherung. Ein lukrativer Datenbestand weckt Begehrlichkeiten.

3 Datenschutzaufsicht

3.1 Datenschutzbeschwerde oder Prüfungsanregung

Über unser Beschwerdeformular erreichen uns gelegentlich Mitteilungen, in denen Verstöße gegen das KDG aufgezeigt werden, die aber nicht erkennen lassen, inwieweit die Rechte und Freiheiten der/des Mitteilenden verletzt worden sind. Bereits in unserem 5. Tätigkeitsbericht[52] hatten wir erläutert, welche inhaltlichen Anforderungen an eine Beschwerde zu stellen sind.

Nach § 48 Abs. 1 KDG hat jede betroffene Person das Recht auf Beschwerde bei der Datenschutzaufsicht, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen Vorschriften des KDG oder gegen andere Datenschutzvorschriften verstößt. Wir sind auch für solche Hinweise, die keine eigene Betroffenheit erkennen lassen, dankbar und nehmen diese als Prüfungsanregungen auf. Es erfolgt jedoch in diesen Fällen keine weitere Bescheidung oder Information an Mitteilende.

Datenschutzbeschwerden können auch anonym eingereicht werden. Auch in diesen Fällen behandeln wir die Hinweise als Prüfanregungen. Abschlussbescheide oder Mitteilungen über das Prüfergebnis erfolgen in diesen Fällen nicht gegenüber Mitteilenden.

Bei der Einreichung der Beschwerde muss kein Dienstweg eingehalten werden (§ 48 Abs. 1 S. 2 KDG). Auch darf niemand gemaßregelt oder be-

52 KDSA Ost, TB 2020, Punkt 2.3

nachteiligt werden, weil er sich an die Datenschutzaufsicht gewendet hat (§ 48 Abs. 3 KDG). Dennoch wenden sich einige betroffene Personen an die Datenschutzaufsicht mit der Bitte ihren Namen nicht dem Verantwortlichen mitzuteilen. Dieser Bitte werden wir zunächst nachkommen. Betroffene Personen müssen aber wissen, dass eine vollständige Anonymität nicht zugesichert werden kann. Der Beschwerdegegner könnte im Rahmen eines Beanstandungs-, Bußgeld- oder Gerichtsverfahrens Akteneinsicht verlangen und so ggf. Kenntnis über die Identität von Beschwerdeführern erlangen. In einem möglichen Bußgeldverfahren könnte es zudem erforderlich werden, Beschwerdeführer als Zeugen zu laden.

Aus Gründen der Vertraulichkeit und Rechtssicherheit versenden wir die Ergebnisse einer Beschwerdeprüfung, abschließende Bescheide und abschließende Mitteilungen ausschließlich auf dem Postweg. Beschwerdeführer, die ihre Postadresse nicht mitteilen, können solche Bescheide deshalb nicht erhalten.

3.2 Prüfaktionen

Von unserer Dienststelle wurden anlasslose Vor-Ort-Prüfungen in verschiedenen Einrichtungen durchgeführt. Diese angemeldeten Besuche dienen zum einen der Überprüfung von Datenschutzstandards, zum anderen aber auch der Beratung der Verantwortlichen im Zusammenhang mit der Verarbeitung personenbezogener Daten. Da die Veranstaltungen nicht auf die Meldung von Datenschutzvorfällen gründeten, konnte gleichsam „proaktiv“ geprüft werden, ob die Datenschutzregelungen in den Einrichtungen geeignet wären, einen Datenschutzverstoß zu vermeiden.

3.2.1 Prüfung einer Seniorenwohneinrichtung

Im September 2021 haben wir eine Seniorenwohneinrichtung vor Ort geprüft. Die Prüfung war angemeldet und fand im Beisein des Datenschutzbeauftragten der Einrichtung statt. Geprüft wurden die datenschutzrechtlichen Abläufe im Zusammenhang mit dem Betrieb des Seniorenheimes, insbesondere die Verwaltung und Aufbewahrung der Bewohnerakten, der Pflegedokumentation und der Personalakten. Gegenstand der Prüfung war

auch das Anmelde- und Aufnahmeverfahren und die damit verbundene Erhebung personenbezogener Daten. In diesem Zusammenhang wurde darauf hingewiesen, dass nur die für die Erfüllung des Betreuungsvertrages notwendige Daten erhoben werden dürfen.

Personalakten

Die Prüfung hat ergeben, dass Personalakten in der Einrichtung aufbewahrt werden. Eine Kopie der Personalakte befindet sich bei der Trägergesellschaft, da dies für die Entgeltabrechnung erforderlich sei. Wir haben dargelegt, dass eine solche doppelte Personalaktenführung nicht den Grundsätzen der Datenverarbeitung entspricht. Angegeben worden ist, dass beabsichtigt sei, Anfang 2022 ein DMS-System einzuführen und die Personalakten zu digitalisieren, so dass eine doppelte Erfassung /Aktenführung überflüssig wird.

Wir haben angekündigt, die Umsetzung am Ende des 1. Quartals 2022 zu prüfen.

Bewohnerakten/Pflegedokumentation

Festgestellt worden ist, dass neben der digitalen Pflegeakte eine sogenannte „kleine Pflegeakte“ in Papierform geführt wird. Nach den Angaben des Verantwortlichen sei dies für den Notfall (Ausfall der Systeme, kurzfristige Krankenhauseinweisungen) erforderlich. Die Akte enthält neben der Kopie der Krankenversicherungskarte, die Medikation sowie eventuell weitere notwendige medizinische Unterlagen. Die Akten befanden sich in Ordnern, welche im Zimmer der Pflegedienstleitung in einem Regal, welches nicht verschlossen werden kann, standen.

Aufgefallen ist uns, dass Akten offen auf den vorhandenen Schreibtischen lagen. Zugang zu den Räumen haben neben den dort beschäftigten Mitarbeitenden auch Reinigungskräfte, die sich teilweise allein in den Räumen aufhalten.

> *Den Verantwortlichen wurde die Auflage erteilt, dass Unterlagen mit personenbezogenen Daten in Schränken aufzubewahren sind, die abgeschlossen werden können, wenn sich Mitarbeitende nicht in dem Raum befinden. Es wurde ausdrücklich daraufhin hingewiesen,*

dass Akten mit personenbezogenen Daten weder auf dem Schreibtisch liegen, noch in einem unverschlossenen Regal aufbewahrt werden dürfen, wenn der Zutritt durch Dritte nicht ausgeschlossen ist.

Es wird neben der kleinen Pflegeakte eine Bewohnerakte geführt, die neben dem Pflege- und Heimvertrag eine Kopie des Ausweises, ggf. den Ausweis im Original (bei Bewohnern mit Demenz) enthält. Die Bewohnerakte befindet sich wie auch die Personalakte der Mitarbeitenden im Büro der Einrichtungsleitung in einem abschließbaren Schrank. Zugriff hat nur die Einrichtungsleiterin. Versichert wurde uns, dass der Einblick in die Pflegeakte nur gewährt wird, sofern eine Einwilligung des Bewohners vorliegt.

Verwaltungs- und Abrechnungsabläufe/TOM

Im Rahmen der erörterten Verwaltungs- und Abrechnungsabläufe wurde darauf hingewiesen, dass personenbezogene Daten per Mail nur verschlüsselt verschickt werden dürfen und die Passwortübersendung gesondert auf anderem Weg erfolgen soll. Eine Sicherheitsrichtlinie zur Versendung von personenbezogenen Daten lag vor.

Auch die allgemeinen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten, wie z. B. Zutritts-, Zugangs- und Zugriffsbeschränkungen, wurden geprüft. Ebenso das Vorhandensein von Einwilligungserklärungen, wie z. B. für das Anfertigen von Fotos (für Bewohner und Mitarbeiter). Es wurde darauf hingewiesen, dass es grundsätzlich möglich ist eine generelle Fotoerlaubnis einzuholen, es dann jedoch entsprechende Wahlmöglichkeiten für unterschiedliche Zwecke der Veröffentlichung geben soll (keine Generaleinwilligung!). Die Einwilligung sollte den Hinweis enthalten, dass bei Veröffentlichung im Internet (Druckmedien, Webseite) Fotos weltweit von beliebigen Personen abgerufen oder weiterverwendet werden können. Vereinbart wurde, dass das Muster der vorhandenen Einwilligungserklärung entsprechend angepasst wird. Eine jährliche Anpassung der Einverständniserklärung wurde empfohlen.

Schlussendlich war die IT-Sicherheit Gegenstand der Prüfung. Kontrolliert worden ist, ob die Arbeitsplätze/Zugänge zur Pflegedokumentation passwortgeschützt sind und ob alle Bildschirme sich automatisch ausschalten, wenn das Gerät nicht genutzt wird. Wo die Geräte stehen und ob die

Räume abschließbar sind wurde geprüft. Ebenso der Standort der Server. Beanstandungen waren nicht erforderlich.

Archiv

Zur Aufbewahrung nicht mehr benötigter Patientenunterlagen müssen ausreichend bemessene und entsprechend ausgestattete Archivräume vorgehalten werden. Festgestellt worden ist, dass das vorhandene Archiv nicht den brandschutztechnischen Anforderungen genügte. Auch gegen Wasserschäden bestand kein hinreichender Schutz, da die Akten auf dem Dachboden in Pappkartons gelagert waren. Der abgetrennte Bereich konnte zwar verschlossen werden, aber die weiteren Maßnahmen zur Datensicherheit (Brandschutz, Maßnahmen gegen Wasserschäden), waren nicht umgesetzt.

Feuerlöscher oder andere Löschmittel waren nicht vorhanden.

Die KDSA hat der Einrichtungsleitung erläutert, dass das Archiv nicht den Anforderungen einer sicheren Datenverarbeitung entspricht. Wir haben darauf hingewiesen, dass die Akten in brand- und wassersicheren Stahlschränken aufzubewahren sind. Der Einrichtung wurde aufgegeben zeitnah das Archiv datensicher herzurichten.

Ergebnis: Über anzupassende Abläufe konnte ein Konsens gefunden werden. Entsprechende Vereinbarungen wurden getroffen. Die Umsetzung wird nach Zeitablauf kontrolliert.

3.2.2 Datenschutzquerschnittsprüfung Pfarreien

Im Rahmen einer Prüfaktion zur Einhaltung des Datenschutzes in Katholischen Kirchengemeinden/ Pfarreien wurden im 4. Quartal 2021 Fragebögen an ausgewählte Pfarreien im Zuständigkeitsgebiet der Kirchlichen Datenschutzaufsicht Ost versandt. Der Fragebogen kann unter der Webseite eingesehen und heruntergeladen[53] werden.

Ziel dieser Prüfaktion war die Einhaltung der Vorschriften des KDG und KDG-DVO bei der Datenverarbeitung im Bereich der Gemeindearbeit.

Abgefragt wurden die allgemeinen Rahmenbedingungen, u.a. ob die Pfarreien einen Datenschutzbeauftragten bestellt haben, ein Datenschutzkon-

53 https://www.kdsa-ost.de/pruefaktion

zept/Datenschutzdokumentation vorliegt, die Mitarbeiter auf die Einhaltung des Datenschutzes verpflichtet wurden/werden, ob ein Verzeichnis der Verarbeitungstätigkeiten gem. § 31 KDG vorhanden ist sowie ob ein Prozess geregelt ist, wie mit Datenschutzbeschwerden umzugehen ist. Ferner wurde abgefragt, ob die Informationspflichten und Betroffenenrechte bekannt sind. Auch die Einhaltung der technischen und organisatorischen Maßnahmen, wie z. B. die Einhaltung von Löschfristen, ist Gegenstand der Prüfung. Abgefragt wurde, ob private Endgeräte für betriebliche/dienstliche Zwecke verwendet werden und ob es, wenn dies der Fall ist, Regelungen zur Nutzung gibt.

Zum Zeitpunkt der Erstellung des Tätigkeitsberichtes hatten noch nicht alle Pfarreien, den Fragebogen zurückgesandt. Die Prüfaktion ist noch nicht abgeschlossen. Wir werden im Tätigkeitsbericht für das Jahr 2022 über das Ergebnis berichten.

Datenschutzüberprüfungen - Checkliste

Auch in Zukunft wird es Prüfaktionen und Vor-Ort-Kontrollen durch unsere Dienststelle geben. Eine Checkliste im Anhang gibt Einrichtungen die Möglichkeit einer Selbstkontrolle wie gut sie in puncto Datenschutz aufgestellt sind.

4 Datenschutz im Gesundheitswesen

4.1 Datenschutzvorfälle

4.1.1 Nutzung privater Endgeräte am Arbeitsplatz

Unserer Aufsicht wurden Vorfälle im Zusammenhang mit der Nutzung von privaten Endgeräten am Arbeitsplatz gemeldet.

Abfotografieren und Versenden eines Dienstplanes per WhatsApp

Unserer Aufsicht wurde von einem Datenschutzbeauftragten eines Krankenhauses gemeldet, dass eine Mitarbeiterin mit ihrem privaten Smartphone ein Foto von einem Dienstplan erstellt und anschließend -wohl un-

beabsichtigt- dieses Foto in einer WhatsApp-Gruppe mit 240 Teilnehmern veröffentlicht hat. Aus dem Dienstplan gingen die Dienstzeiten der Mitarbeitenden hervor.

Der Verantwortliche der Klinik hat ausgeführt, dass die Dienstpläne auf den Stationen per Dienstplanprogramm erstellt werden und die Mitarbeiter ihre Dienstpläne auf den jeweiligen Stationen einsehen können. Weiterhin wurde angeben, dass ein Ausdruck im Stationszimmer ausgehängt wird.

Dienstpläne enthalten generell personenbezogenen Daten. Gem. § 4 Nr. 1 KDG sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Dienstplan enthält Personendaten, wie den Vor- und Nachnamen der Mitarbeiter und die Arbeitszeiten. Zudem enthielt der Dienstplan nach den Angaben der Verantwortlichen der Klinik auch Abwesenheitsgründe, wie z. B. Urlaub oder Krankheit. Die Information, dass jemand erkrankt ist, gehört gem. § 4 Nr. 2 KDG zu den personenbezogenen Daten besonderer Kategorie. Das Erstellen und Aushängen der Dienstpläne stellen Verarbeitungen im Sinne des § 4 Abs. 3 KDG durch Erfassen und Offenlegen dar.

Eine rechtmäßige Verarbeitung personenbezogener Daten ist gem. § 6 Abs. 1 KGD nur zulässig, wenn eine der dort genannten Bedingung erfüllt ist. Gem. § 11 Abs. 1 KDG ist die Verarbeitung personenbezogener Daten der besonderen Kategorie unzulässig. Eine Ausnahme besteht nur für den Fall, dass eine der in Abs. 2 dieser Vorschrift genannten Bedingungen zutrifft.

Das Aushängen von Dienstplänen ist zur Vertragserfüllung nicht erforderlich, § 6 Abs. 1 lit c) bzw. § 11 Abs. 2 lit b). KDG. Eine Zulässigkeit ergibt sich auch nicht aus § 53 Abs. 1 KDG. Nach dieser Vorschrift dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Mitarbeitende konnten, wie vom Verantwortlichen dargelegt worden ist, selbst ihren eigenen Dienstplan auf ihren Stationen über ihren Arbeitsplatz im Dienstplanprogramm einsehen. Ein aushängender Dienst-

plan ist, nach unserer Ansicht, daher für die Erfüllung der Verpflichtungen aus dem Arbeitsvertrag nicht erforderlich.

Ein öffentlicher Dienstplan-Aushang wäre nach unserer Auffassung nur zulässig, wenn alle Mitarbeiter, deren Daten auf dem Plan erscheinen, der Veröffentlichung zustimmen (§ 6 Abs. 1 lit b KDG). Das gilt auch, wenn sich, wie in der betroffenen Einrichtung, der Aushang in einem Raum auf der jeweiligen Station befindet, zu dem nur die Mitarbeiter der Station Zutritt haben. Ohne die Zustimmung der Mitarbeitenden ist die Weitergabe von personenbezogenen Daten an Dritte nicht rechtmäßig. Verwehrt ein Mitarbeitender die Zustimmung zur Dienstplanveröffentlichung, dürfen dessen Daten nicht weitergeben werden, d. h. der Dienstplan darf keine ihn betreffenden Angaben erhalten.

Auch im Fall der Einwilligung der Mitarbeiter in den Aushang der Dienstpläne gilt: Dienstpläne dürfen keine konkreten Informationen, warum ein Mitarbeiter abwesend ist (Urlaub, Krankheit usw.) enthalten. Der Hinweis, dass die Person nicht anwesend ist, genügt.

Das Aushängen des Dienstplanes im Stationszimmer der Klinik stellte somit einen Datenschutzverstoß dar.

Das Abfotografieren und Versenden des Dienstplanes per WhatsApp stellt eine Verarbeitung i. S. d. § 4 Abs. 3 KDG dar. Die Verantwortlichen der Klinik haben diesen Datenschutzverstoß eingeräumt. Das Verhalten der Mitarbeiterin war dem Verantwortlichen jedoch nicht zuzurechnen, da uns glaubhaft versichert worden ist, dass allen Mitarbeitern bekannt war, dass Dienstpläne nicht vervielfältigt oder abfotografiert werden dürfen. Die Mitarbeiterin hatte gegen diese in der Klinik geltende Anweisung verstoßen. Hierbei handelt es sich um einen sog. Mitarbeiterexzess.

Der Verantwortliche hat uns zugesichert, dass Dienstpläne künftig keine Angaben zu Abwesenheitsgründen enthalten und auch kein Aushang erfolgt.

Unbeschadet dessen hat die Aufsicht förmlich beanstandet, dass Mitarbeiter einer Station die Dienstpläne aller Mitarbeiter dieser Station einsehen konnten und die Pläne konkrete Angaben zu Abwesenheitsgründen (Urlaub/Krankheit) enthielten. Gem. § 47 Abs. 5 lit. a) KDG wurde der Klinik die

Auflage erteilt, das Aushängen der Dienstpläne zu unterlassen, es sei denn die Mitarbeiter, deren Daten offengelegt werden, haben dem ausdrücklich zugestimmt. Angaben zu konkreten Abwesenheitsgründe, wie z. B. Urlaub oder krank, darf der Dienstplan nicht enthalten.

TikTok

Unserer Dienststelle wurde gemeldet, dass eine Mitarbeiterin einer Pflegeeinrichtung mit ihrem privaten Handy während ihrer Arbeitszeit ein Video erstellt hat, um es auf der Plattform „TikTok" einzustellen. Die Mitarbeiterin hatte eine Bewohnerin gefilmt, die sich mit einem Gehwagen in der Einrichtung bewegte. Eine Einwilligung der Bewohnerin lag nicht vor. Das Video wurde auf der Plattform veröffentlicht und nach Aufforderung durch die Einrichtungsleitung wieder gelöscht.

Im Rahmen der Anhörung des Verantwortlichen wurde uns mitgeteilt, dass in der Einrichtung eine Anweisung existiert, nach der private Handys während der Arbeitszeit nicht genutzt werden dürfen. Gegen diese Anweisung hat die Mitarbeiterin verstoßen. Es handelt sich ebenfalls um einen Mitarbeiterexzess. Exzesse von Beschäftigten, die bei verständiger Würdigung nicht der dienstlichen Tätigkeit zugeordnet werden können, sind datenschutzrechtlich nicht den Einrichtungen als Verantwortliche zu zurechnen.

Aufgrund dieses Vorfalls haben wir angeregt, die Mitarbeiter anzuweisen, ihre privaten Geräte während ihrer Dienstzeit nicht unmittelbar bei sich zu tragen und eine ständige Erreichbarkeit in Notfällen über eine Tel-Nr. der Einrichtung zu gewährleisten, da dies aus unserer Sicht ausreichend ist. Seitens der Verantwortlichen wurde eingewandt, dass die praktische Umsetzung (Kontrolle der Dienstkleidung) schwierig sei. Verständigt haben wir uns mit den Verantwortlichen im Ergebnis darauf, dass alle Mitarbeitenden darauf zu verpflichten sind, dass die privaten Endgeräte im dienstlichen Kontext nicht genutzt werden dürfen.

4.1.2 Übergriffige Klinikmitarbeiter und der Datenschutz

Bereits in unserem Bericht 2020[54] haben wir auf die Wichtigkeit eines Need-to-know-Prinzip (Rollenkonzept) hingewiesen. Gerade im Gesund-

54 KDSA Ost, TB 2020, Punkt 4.1

heitsbereich ist es notwendig, dass der Verantwortliche gem. § 26 KDG dafür Sorge trägt, dass ein angemessenes Schutzniveau für Patientendaten gewährleistet ist.

Auch wenn Rollen- und Berechtigungskonzepte bestehen und eingesetzt werden, kann, wie uns gemeldete Fälle zeigen, nicht verhindert werden, dass Unberechtigte Zugriff auf Daten von anderen Mitarbeitern nehmen. Nachfolgend sollen einige Fälle geschildert werden:

Neugierige Kollegen

So wurde uns in mehreren Fällen gemeldet, dass Mitarbeiter von Kliniken auf Patientenakten von anderen Mitarbeitern der Klinik zugegriffen haben, die sich auf einer anderen Station dieser Klinik behandeln lassen haben bzw. Kenntnis von Behandlungsinhalten hatten, wobei eingeräumte Zugriffsrechte missbraucht worden sind. Die so erlangten Erkenntnisse wurden mit anderen Mitarbeitenden geteilt. Die Behandlungsgründe machten in der Klinik die Runde -mit Sicherheit keine angenehme Situation für die Betroffenen. In diesen Fällen wurden Daten unrechtmäßig verarbeitet. Gem. § 6 Abs. 1 KDG dürfen personenbezogene Daten nur verarbeitet werden, wenn eine der dort genannten Erlaubnistatbestände vorliegt. Grundsätzlich ist eine Datenverarbeitung verboten, es sei denn, sie ist ausdrücklich gesetzlich erlaubt oder die Betroffenen stimmen zu. Das heißt die Betroffenen hätten einwilligen müssen, dass die nicht in die Behandlung einbezogenen Kollegen Einsicht in die Patientenakte nehmen, was nicht der Fall war.

Verliebt am Arbeitsplatz

Gemeldet wurde uns auch folgender Vorfall aus einem Klinikum: Ein Mitarbeiter der IT-Abteilung hat den Umstand, dass er Zugang zu Personaldaten hatte, missbraucht, um die private Telefonnummer einer Auszubildenden in Erfahrung zu bringen, um mit dieser über einen Messangerdienst Kontakt aufzunehmen. Nach einigen ausgetauschten Nachrichten war der Auszubildenden klar, welcher Mitarbeiter zu ihr Kontakt aufgenommen hatte. Da sie sich über diese Vorgehensweise beim Datenschutzbeauftragten der Klinik beschwerte, hielt sich ihr Interesse offensichtlich in Grenzen.

Auch in diesem Fall wurden Daten unrechtmäßig verarbeitet. Die Auszubildende war mit der privaten Nutzung ihrer, in der Personalakte gespeicherten Telefonnummer, durch diesen Mitarbeiter nicht einverstanden.

Da in allen gemeldeten Fällen Rollen- und Berechtigungskonzepte bestehen und eingesetzt wurden, konnte der Verantwortliche nicht in Anspruch genommen werden. Es handelte sich in allen Fällen um einen sog. Mitarbeiterexzess. Die Mitarbeiter hatten in allen Fällen die ihnen eingeräumten Berechtigungen missbraucht. In diesen Fällen wurden die Verantwortlichen angehalten ihre Mitarbeiter anlassbezogen erneut und regelmäßig auf die Einhaltung des Datenschutzes zu schulen. Eine Sanktionierung gegenüber der den Datenschutzverstoß begehenden Personen ist gem. § 3 KDG nicht möglich, da das KDG nur für kirchliche Stellen Anwendung findet.

4.1.3 Verstöße gegen die Meldepflicht gem. § 33 KDG

Im Berichtszeitraum kam es zu Verstößen gegen die Meldepflicht gem. § 33 KDG. Festgestellte Datenschutzverstöße wurden nicht unverzüglich der Datenschutzaufsicht gemeldet. In einem Fall wurde der Verantwortlichen eine förmliche Beanstandung ausgesprochen.

Im beanstandeten Fall war eine am 26.03.2021 bekannt gewordene Datenschutzverletzung (Offenlegen einer AU-Bescheinigung) der Aufsicht erst am 30.03.2021 gemeldet worden. Die Verantwortliche hat dies damit begründet, dass weiterer Klärungsbedarf bestanden hätte. Zudem berief sie sich darauf, dass zwischen dem Tag des Bekanntwerdens und der Meldung ein Wochenende lag und eine Fristüberschreitung nicht vorliegt, da dies gem. Art. 3 Abs. 5 Fristen-VO zu berücksichtigen sei. Gem. dieser Vorschrift muss jede Frist von Zwei oder mehr Tagen mindestens zwei Arbeitstage umfassen. Dieser Argumentation sind wir aus folgenden Gründen nicht gefolgt:

Ein festgestellter Datenschutzverstoß muss der Datenschutzaufsicht von dem Verantwortlichen **unverzüglich** (ohne schuldhaftes Zögern) gemeldet werden, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt (§ 33 Abs. 1 KDG). Anknüpfungspunkt für die Rechtzeitigkeit der Meldung ist die Kenntnis des Verantwortlichen von der

Verletzung des Schutzes personenbezogener Daten. Eine positive Kenntnis vom Vorliegen eines Verstoßes muss noch nicht gegeben sein. Es müssen auch noch nicht alle Details der Verletzungshandlung oder der Folgen aufgeklärt sein. Es reicht, wenn eine hinreichende Kenntnis einer Schutzverletzung vorliegt.[55]

Hinzu kommt, dass wenn die Meldung nicht innerhalb von 72 Stunden nach Bekanntwerden der Verletzung erfolgt, der Meldung eine Begründung der Verzögerung beizufügen ist (§ 33 Abs. 1 S. 2 KDG).

Die Verantwortliche hat sich zudem auf Art. 3 Abs. 5 Fristen-VO berufen. Diese Vorschrift findet jedoch keine Anwendung, da gem. Art. 1 dieser Verordnung, diese, soweit nichts anderes bestimmt ist, nur für die Rechtsakte, die der Rat und die Kommission auf Grund des Vertrages zur Gründung der Europäischen Wirtschaftsgemeinschaft oder des Vertrages zur Gründung der Europäischen Atomgemeinschaft erlassen haben bzw. erlassen werden, gilt. Dies war vorliegend nicht der Fall. Die verspätete Meldung stellte einen Datenschutzverstoß dar, der zu sanktionieren war. Der Bescheid ist bestandskräftig.

Im Übrigen gilt im kirchlichen Bereich § 7 Abs. 4 KDS-VwVfG, wonach für den Fall, dass eine Frist nach Stunden bestimmt ist, Sonntage, gesetzliche Feiertage oder Sonnabende mitgerechnet werden.

4.1.4 Informationspflichten bei Datenpannen § 34 KDG

Im Zusammenhang mit Datenschutzverletzungen ist immer auch § 34 KDG zu beachten. Eine Verletzung muss nicht nur der Datenschutzaufsicht gemeldet werden, sondern gem. § 34 KDG ist der Verantwortliche auch verpflichtet, bei Datenschutzverletzungen, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge haben, die betroffene Person unverzüglich über die Verletzung zu benachrichtigen. Auch in diesem Berichtszeitraum gab es Meldungen zum Fehlversendungen von Diagnoseberichten, Laborbefunden, Rechnungen durch medizinisches Personal, etwa weil eine falsche Faxnummer verwendet wurde oder falsche Unterlagen herausgeben worden sind. Da es sich

55 Pau, in HK-Kirchliches DatenschutzR, 2021, § 33 Rn. 11

bei Gesundheitsdaten um besonders schützenswerte Daten handelt, haben die Verantwortlichen zumeist in der Meldung an uns mitgeteilt, dass die jeweils Betroffenen vorsorglich und unabhängig von einer Rechtspflicht informiert worden sind und dass sie Maßnahmen zur künftigen Vermeidung solcher Fehler getroffen haben. Dies hat uns gezeigt, dass den Verantwortlichen diese Verpflichtung bekannt ist.

4.1.5 Gerichtliches Verfahren

Im Tätigkeitsbericht 2020[56] haben wir über folgenden Fall berichtet: Ein Arztbrief wurde an den Ehemann einer Patientin herausgegeben, obwohl diese bei der Aufnahme angeben hat, dass ihrem Ehemann keine Auskünfte zu erteilen sind. Begünstigt wurde dieser Datenschutzverstoß auch aufgrund der Tatsache, dass das von dem Klinikum verwendeten Krankenhausinformationssystem hinsichtlich der Eintragung von Auskunftserteilungswünschen der Patienten eine Opt-Out-Regelung vorsah. In der verwendeten Maske war vorgesehen, dass eingetragen werden konnte, welchen Personen keine Auskünfte erteilt werden dürfen, sog. Sperrvermerke. Die Eintragung eines Sperrvermerks für Ehepartner oder nahe Angehörige sah die Maske und auch die Datenschutzleitlinie jedoch nicht vor. Die Klinik vertrat die Auffassung, dass Ehepartnern und nahen Angehörigen generell Auskunft erteilt werden kann, wenn der Patient einer Auskunftserteilung nicht widersprochen hat. Wir hatten zudem gerügt, dass die Meldung der Datenschutzverletzung nicht innerhalb der Frist gem. § 33 KGD erfolgt ist. Die Meldung erfolgte 12 Tage später, obwohl sich die Petentin bereits vorher bei der Chefarztsekretärin beschwert hatte, die die Beschwerde nicht weitergeleitet hatte. Der Verantwortliche war der Auffassung, dass Wissen der Chefarztsekretärin sei ihm nicht zu zurechnen.

Dieser Vorfall wurde von uns förmlich beanstandet und eine Geldbuße in Höhe von 2.100,00 € festgesetzt. Die Klinik hat gegen diesen Bescheid Rechtsmittel eingelegt und beantragt, den Bescheid aufzuheben. Das Gericht hat den Antrag[57] als unbegründet zurückgewiesen. Das Gericht hat sich unserer Auffassung angeschlossen und in der Verfahrensweise ei-

56 KDSA Ost, TB 2020, Punkt 4.3
57 IDSG, Beschluss vom 12.07.2021 - AZ: IDSG 21/2020, https://www.dbk.de/fileadmin/user_upload/Beschluss-IDSG-21-2020_vom_16.07.2021_anonym.Fas_geschw%C3%A4rzt.pdf.

nen Verstoß gegen § 26 KDG gesehen. Auch bezüglich der Frage, ob die Kenntnis der Chefarztsekretärin von der Beschwerde dem Verantwortlichen zuzurechnen sei, hat sich das Gericht unserer Auffassung angeschlossen und ausgeführt, dass der Verantwortliche für die Pflichtverletzung im Chefarztsekretariat gemäß dem Funktionsträgerprinzip hafte. Die Kenntnis der Chefarztsekretärin von der Datenschutzverletzung muss sich der Verantwortliche zurechnen lassen. Die Meldung war daher verspätet. Das Gericht hat mithin einen Verstoß gegen § 33 KDG bejaht.

Anzumerken ist, dass das Gericht die verhängte Geldbuße als sehr moderat angesehen hat. Die Entscheidung kann unter dem AZ IDSG 21/2020 beim IDSG abgerufen werden.

4.1.6 Sonstige Vorfälle

Auch in diesem Berichtszeitraum wurde uns in mehreren Fällen gemeldet, dass Patientenunterlagen, wie Arztbriefe, Entlassberichte, Rechnungen oder Zuzahlungsrechnungen an unbeteiligte Dritte versandt worden sind. Die Offenlegung erfolgte durch fehlerhaften Fax-Versand (falsche Faxnummer), Herausgabe von Patientenunterlagen an andere Patienten, Verbinden von nicht zusammengehörigen Unterlagen, wodurch ebenfalls eine Offenlegung von Gesundheitsdaten an Unberechtigte erfolgte. Unsere Prüfungen haben in allen gemeldeten Fällen ergeben, dass in den Einrichtungen entsprechende Datenschutzunterlagen vorhanden waren und die Verantwortlichen ihren Verpflichtungen gem. § 26 KDG einhielten. Den Verantwortlichen wurde aufgegeben, ihre Mitarbeiter regelmäßig auf die Einhaltung der vorhandenen Regelungen, insbesondere auf die Regelungen zur Herausgabe von Unterlagen, die Gesundheitsdatenenthalten, zu schulen und auf den Datenschutz zu sensibilisieren. In einem Fall erfolgte dies über einen förmlichen Beanstandungsbescheid, der rechtskräftig ist. Die Mitarbeiter wurden, wie beauflagt, fristgerecht geschult.

5 Datenschutz in Schule und Kita

5.1 Ergebnisse der Prüfaktion: Nutzung privater Endgeräte – Datenverarbeitung im häuslichen Bereich

Im letzten Tätigkeitsbericht hat sich unsere Dienststelle zur Datenverarbeitung durch Lehrer im häuslichen Bereich geäußert. Wir haben Hinweise und Tipps gegeben, wie die Arbeitsplätze aus Sicht des Datenschutzes gestaltet sein müssen und welche Datenschutzregelungen bei der Datenverarbeitung maßgebend sind[58].

Im Rahmen einer sich anschließenden Prüfaktion in diesem Bereich wurden im Berichtsjahr 2021 Fragebögen an 12 Schulen im Zuständigkeitsgebiet der Kirchlichen Datenschutzaufsicht Ost geschickt.

Ziel dieser Prüfaktion war die Einhaltung der Vorschriften des KDG und der KDG-DVO bei der Nutzung von privaten Endgeräten zu dienstlichen Zwecken bei Lehrkräften sowie der Datenverarbeitung durch Lehrkräfte im häuslichen Bereich.

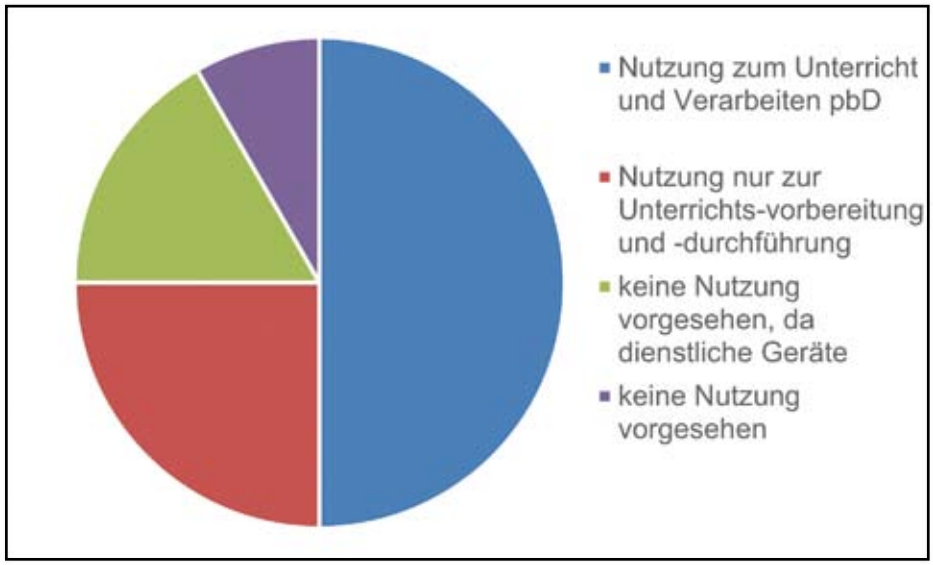
5.1.1 Verwendung von privaten IT-Geräten zu dienstlichen Zwecken und schriftliche Regelungen

Im Schuljahr 2020/2021 haben von den 12 geprüften Schulen 9 Schulen private Endgeräte dienstlich genutzt.
Von diesen 9 Schulen war an 3 Schulen die Nutzung ausschließlich zur Unterrichtsvorbereitung und -durchführung gestattet. Alle dienstlichen Daten (inkl. personenbezogene Daten) durften in diesem Zusammenhang auf privaten Geräten nur temporär zwischengespeichert werden und mussten umgehend in die zur Verfügung stehende zentrale Datenablage (wie z.B. der Schulcloud) oder dem dienstlichen USB-Stick übertragen werden, so dass alle temporär gespeicherten Daten sofort vom privaten IT-System/Gerät gelöscht werden konnten. Dies war in einer entsprechenden Richtlinie

58 KDSA Ost, TB 2020, Punkt 5.2

zur Nutzung von USB-Datenträgern festgelegt, die von jedem Nutzer zu unterzeichnen ist.

An den übrigen 6 Schulen, an denen die Verwendung privater Endgeräte gestattet war, durfte die Nutzung privater Geräte nur auf Antrag bei der Schulleitung erfolgen. Dazu gab es an diesen Schulen eine Vereinbarung zur Datenverarbeitung auf privaten Endgeräten, welche detaillierte Angaben zum Umfang der Datenverarbeitung enthält. Die Antragsteller wurden auf die Einhaltung der in § 20 KDG-DVO enthaltenen Regelungen sowie umzusetzende technische- und organisatorische Maßnahmen verpflichtet.



In 3 von 12 geprüften Schulen wurden im Prüfungszeitraum keine privaten IT-Geräte verwendet.

In einer Einrichtung war die Verarbeitung personenbezogener Schülerdaten im häuslichen Bereich auf IT-Geräten nicht vorgesehen, da im Lehrerzimmer dienstliche Geräte zur Verfügung gestellt wurden. Dementsprechend gab es keine schriftliche Regelung zur Verwendung privater Geräte.

An 2 Schulen wurden bereits 2019 dienstliche Endgeräte zur Verfügung gestellt, da die Nutzung privater IT-Systeme/Geräte zu dienstlichen Zwecken problematisch gesehen wurde. Die Datenverarbeitung erfolgt in diesen Einrichtungen auf betrieblichen/dienstlichen Endgeräten. Für die dienstlichen Geräte gibt es eine Nutzungsvereinbarung, die Maßnahmen zur IT-Sicherheit und Hinweise zum Datenschutz enthält.

5.1.2 Sicherung der IT-Geräte im privaten Bereich

In den schriftlichen Vereinbarungen und Richtlinien, die uns im Rahmen dieser Prüfaktion übermittelt worden sind, gab es zahlreiche gute Regelungen und Hinweise, wie mit dienstlichen Daten insbesondere Schülerdaten umzugehen ist. Sobald personenbezogene Daten verarbeitet werden, müssen IT-Systeme und Geräte vor unerlaubten und nicht autorisierten Zugriff geschützt werden (s. u.a. KDG-DVO). Insbesondere schon deshalb, weil zum Teil IT-Geräte der Lehrkräfte in deren privaten Umfeld zur Unterrichtsvorbereitung und -durchführung genutzt werden. In einem familiären privaten Umfeld halten sich in der Regel Familienangehörige auf, die als Dritte zu betrachten sind.

Für die Sicherung von IT-Geräten kommen bei Lehrkräften u.a. folgende Sorgfaltspflichten bzw. Maßnahmen zum Einsatz:

- USB-Stick mit Kennwortschutz
- Datenträger mit personenbezogenen Daten nicht unbeaufsichtigt lassen
- Schutz durch Passwörter und Verschlüsselung
- 2-Faktor Authentifizierung (beim Zugriff auf Schulclouds)
- Regelmäßige Datensicherung (Auslesen der USB Sticks und Speicherung auf dem Server)
- Clean-Desk (aufgeräumter Schreibtisch)
- verschlossene Schränke und falls möglich verschließbare Räume für alle dienstlichen bzw. betrieblichen Daten, Papierunterlagen, etc.
- Mobile Device Management und Fernzugriff für dienstliche Geräte

5.1.3 Nutzung und Verfügbarkeit von E-Mailadressen durch die Lehrkräfte

Im Rahmen dieser Prüfaktion wurde auch die dienstliche Kommunikation der Lehrer per E-Mail der zu überprüfenden Schulen abgefragt. An allen geprüften Schulen wurden dienstliche E-Mailadressen vom Schulträger

oder der Schule zur Verfügung gestellt. Eine Nutzung dieser E-Mailadressen für private Zwecke ist nicht erlaubt und wurde dementsprechend in den Nutzungsbedingungen untersagt.

Die dienstlichen E-Mailadressen werden u.a. zur Kommunikation mit Schülern und Erziehungsberechtigten genutzt. Einige Schulen haben den Schülern E-Mailadressen zur Verfügung gestellt. Bei anderen Schulen lief die Kommunikation mit den Lehrkräften über Chats in den Lernplattformen.

Beide Varianten haben den Vorteil, dass sich Schüler für die schulische Kommunikation keine eigenen privaten E-Mailadressen zulegen müssen und die Kommunikation zentralisiert über die Schule bzw. deren Infrastruktur organisiert wird.

Der überwiegende Teil der Befragten gab an, dass die verwendeten IT-Dienstleister und Rechenzentren in Deutschland angesiedelt sind.

Fazit

Insgesamt hatte unsere Dienststelle nur wenig zu beanstanden. Es wurden den Schulen bzw. Schulträgern Hinweise gegeben, wo noch Verbesserungspotential besteht. Ebenso wurde die Empfehlung ausgesprochen Mitarbeitende und Schüler regelmäßig zu sensibilisieren.

Private Endgeräte werden bzw. wurden teilweise genutzt, aber nur unter der Voraussetzung, dass die Regelungen gemäß § 20 KDG-DVO eingehalten werden müssen. Alle Lehrkräfte wurden dahingehend belehrt, wie im häuslichen Umfeld mit allen dienstlichen Daten und vor allem mit Schülerdaten, umzugehen ist. Zudem wurden ihnen zur Einhaltung der Datensicherheit und des Datenschutzes technische und organisatorische Maßnahmen mitgeteilt.

Innerhalb der Antworten war auffällig geworden, dass Einrichtungen nahezu identischen Antworten gegeben hatten, die denselben betrieblichen Datenschutzbeauftragten beauftragt haben. Das verwundert, da sich die Schulstufen der geprüften Schulen und die sich daraus ergebenen Altersstrukturen der Schüler sehr unterscheiden. Die Unterrichtsvorbereitung der Lehrkräfte und die Kommunikationsmöglichkeiten werden sich möglicherweise vom Primärbereich bis zum Sekundarbereich II unterscheiden. So wird es beispielsweise im Primärbereich nicht üblich sein mit Schülern über

E-Mail oder Chats zu kommunizieren. Auch die Verarbeitung personenbezogener Daten von Schülern des Primärbereiches muss nicht zwingend digital zu Hause stattfinden. Hier kann es ausreichend sein, wenn dafür Endgeräte im Lehrerzimmer genutzt werden, wie es u.a. von einer Schule vorgesehen war.

Sobald jedoch die Möglichkeit besteht personenbezogene Daten auch zu Hause zu verarbeiten, wird dies gern in Anspruch genommen, ohne dabei die Erforderlichkeit zu hinterfragen.

Positiv hervorzuheben ist, dass sich alle Schulen Gedanken über den Schutz ihrer persönlichen Daten (Datenschutz) machen. Fast alle Schulen machen davon Gebrauch, digitale Endgeräte für das Lehrpersonal zur Verfügung zu stellen.

Die Datenschutzaufsicht wird sich vorbehalten im Nachgang dieser formalen Prüfaktion ausgewählte Schulen auch vor Ort zu überprüfen.

5.2 Corona-Selbsttests an Schulen

Im Berichtsjahr hat sich neben dem Tragen von Masken auch die Durchführung von Corona-Selbsttests als eine Maßnahme zur Eindämmung der Pandemie etabliert.

Jedoch warf die Durchführung dieser Selbsttests in der Schule vor allem in der Elternschaft die Frage auf, ob die Verarbeitung von besonders schützenswerten Gesundheitsdaten bei diesem Prozedere überhaupt erlaubt ist?

Richtig ist, dass bei der Durchführung von Corona-Selbsttests an Schulen besondere Kategorien personenbezogener Daten (Gesundheitsdaten) nach § 4 Nr. 2, 17 KDG (Art. 4 Nr. 15 DS-GVO) verarbeitet werden. Um Gesundheitsdaten rechtmäßig zu verarbeiten, muss entweder eine Einwilligungserklärung der betroffenen Person vorliegen oder eine Rechtsgrundlage dies erlauben. Die meisten Bundesländer haben durch ihre Corona-Schutzverordnungen entsprechende Rechtsvorschriften erlassen, so dass die Durchführung von Selbsttests entsprechend § 11 Abs. 2 lit. i) KDG (Art. 9 Abs. 2 lit. i) DS-GVO) erlaubt ist.

Auch die Verhältnismäßigkeit gegenüber dem Recht auf informationelle Selbstbestimmung ist gegeben, denn der Schutz der Gesundheit jeder

einzelnen Person und die des gesamten Systems wiegen in einer Pandemie höher, als das Recht des Einzelnen. Die Durchführung von Selbsttests an Schulen ist ein geeignetes Mittel, die akute Ansteckungsgefahr zu minimieren, indem positiv Getestete vom Schulbetrieb ausgeschlossen werden. Zudem steht kein milderes Mittel zur Verfügung, um den Schulbetrieb bei einer Pandemie aufrecht zu erhalten.

Trotzdem ist wie bei allen anderen Verarbeitungsprozessen von personenbezogenen Daten eine besondere Sorgfaltspflicht und die Information der Betroffenen über diese Datenerhebung wichtig. Verantwortlich für die Verarbeitung dieser Gesundheitsdaten ist die Schule. Diese muss den Schülern und Erziehungsberechtigten Informationen zur Verarbeitung der personenbezogenen Daten im Zusammenhang mit der Selbsttestung gemäß § 15 KDG (Art. 13 DS-GVO) bereitstellen. Aufgrund der Gegebenheiten an einer Schule ist nicht auszuschließen, dass auch andere Schüler Kenntnis über die Testergebnisse erhalten können, da spätestens bei einem positiven Ergebnis Betroffene sofort isoliert werden müssen. Daher sollte die Schule möglichst sehr sensibel im Umgang mit positiv Getesteten sein.

Die Testergebnisse sind entsprechend ihrer Erforderlichkeit nach spätestens 14 Tagen datenschutzgerecht zu vernichten. Eine Dokumentation in den Schüler- bzw. Personalakten ist nicht erforderlich und daher nicht erlaubt. Ausschließlich dem zuständigen Gesundheitsamt dürfen im Fall eines positiven Tests die Kontaktdaten der betroffenen Person zur Verfügung gestellt werden. Darüber hinaus kann es erforderlich sein, Daten von Kontaktpersonen zu übermitteln.

5.3 Leistungsnachweise im Homeschooling – Schülervideos im Netz

Bedingt durch mehrere Lockdowns zur Eindämmung der Corona-Pandemie haben viele Schulen im Berichtsjahr den zuvor eingeführten Distanzunterricht fortführen müssen.

Trotz dieser Umstände waren die Lehrer angehalten regelmäßig Lernzielkontrollen und Leistungsnachweise bei den Schülern durchzuführen. Da die Regelwerke (Schulgesetze, Erlasse etc.) neben schriftlichen und gestalterischen auch mündliche -für den Sportunterricht auch körperliche-

Leistungsnachweise vorschreiben, forderten einige Lehrkräfte diese Nachweise zum Beispiel per Video von Schülern ab. In einem Video werden personenbezogene Daten i. S. v. § 4 Nr. 1 KDG, teilweise auch besondere Kategorien personenbezogener Daten i.S. v. § 4 Nr. 2 KDG, verarbeitet, da Videos Aufnahmen der privaten Wohnung, die als Mittelpunkt privater Lebensgestaltung grundrechtlich geschützt ist, enthalten können[59]. Sollen beispielsweise Schüler ein Video von sich selbst aufnehmen, dass sie beim Halten eines Vortrages oder beim Ausführen einer Sportübung zeigt, und dieses Video anschließend dem Lehrer zur Bewertung zur Verfügung stellen, gibt es einiges zu beachten:

Das Video darf nur über eine gesicherte Verbindung, idealerweise der Lernplattform, die gemäß den allgemeinen Datenschutzgrundsätzen und Empfehlungen betrieben wird, der Lehrkraft zur Verfügung gestellt werden. Das Video hat nur die Lehrkraft und nicht die gesamte Klasse zu erreichen. Entsprechende Voreinstellungen müssen auf der Lernplattform etabliert sein. Es ist nicht erlaubt -z.B. aus Kapazitätsgründen der Lernplattform- die Schüler aufzufordern, einen YouTube Kanal oder ihre private E-Mailadresse für die Übermittlung des Videos zu nutzen. Das Betreiben eines YouTube-Kanals ist üblicherweise an ein Google Konto geknüpft, welches die meisten Schüler nicht besitzen können, da Google die Volljährigkeit zur Benutzung eines solchen Kontos voraussetzt. Die Schüler können unter Umständen animiert werden, diese Daten zu fälschen. Besonders unter datenschutzrechtlichen Aspekten ist jedoch von YouTube abzusehen, da dieses Netzwerk zum Google-Konzern gehört. So hält YouTube keine eigene Datenschutzerklärung vor, sondern verweist direkt auf die Datenschutzerklärung von Google. Diese wiederum entspricht nicht Datenschutzniveau der DS-GVO bzw. dem KDG.

Praxistipps

Die Lehrkraft hat das Video ausschließlich zur Leistungsbeurteilung zu nutzen und muss dieses nach Bewertung der Leistung löschen.

Die Schüler sind dahingehend zu sensibilisieren, dass auch sie das Video nach der Bewertung löschen und keinem Dritten oder sozialen Netzwerken zur Verfügung stellen.

59 KDSA Ost, TB 2020, Punkt 5.1.5

Das häusliche Umfeld, welches mit aufgezeichnet wird, ist durch die Lehrkraft außeracht zu lassen und darf in keiner Weise in die Bewertung mit einfließen. Idealerweise werden auch hier die Schüler sensibilisiert, möglichst wenig aus dem privaten Bereich mitaufzunehmen.

Weiterhin setzt diese Art der Leistungswertung natürlich auch voraus, dass die Schüler und die Erziehungsberechtigten der Übermittlung von Ton und Bild zugestimmt haben. Diese Einverständniserklärung kann auch durch das schlüssige Handeln erfolgen, indem das Video aufgenommen und zur Bewertung zur Verfügung gestellt wird.

Wird die Einwilligung zum Video nicht gegeben, so darf das für den Schüler nicht nachteilig sein und es muss eine alternative Lösung angeboten werden.

5.4 Datenschutz im Kindergarten - Ungewollt Kinderfotos im Netz

Im Vorfeld einer Datenschutzkontrolle, die in einer Kindertagesstätte stattgefunden hat, analysierte unsere Dienststelle die Webseite dieser Einrichtung und überprüfte eine Konzeption, die im Internet über einen Sharehoster frei zur Verfügung stand.

Im weiteren Verlauf der Analyse fand unsere Dienststelle Kinderfotos mit Angabe zum Namen und Alter im Contentinhalt der Webseite. Die Bilder waren für normale Nutzer nicht mehr zu sehen, da sich diese „nur" im älteren Inhalt der Webseite befanden. Trotzdem war es ohne großen technischen Aufwand machbar, diese Bilder zusammen mit den Angaben zum Namen und Alter der Kinder aufzurufen. Die Kindertagesstätte wurde darauf hingewiesen, dass das Löschen einer Verknüpfung zu einem Bild nicht ausreicht, sondern dieses Bild auch aus dem Content (Inhalt) gelöscht werden muss.

Auch die Konzeption dieser Einrichtung, die auf der Webseite eines bekannten Sharehosters zu finden war, wurde unter die Lupe genommen. Sharehoster sind Dienste, auf denen digitale Dokumente verschiedener Dateiformate veröffentlicht werden können. Diese Dokumente oder auch

Bilder sind dann für andere Nutzer im Internet über gängige Suchmaschinen zu finden oder können als Link abgerufen werden.

So waren in dieser Konzeption zahlreiche Kinderfotos enthalten. Besonders ein Bild war kompromittierend, da Kinder eindeutig identifizierbar und nur leicht bekleidet abgebildet waren. Im Vorortttermin wurde von der Datenschutzaufsicht angeordnet, diese Konzeption umgehend aus dem Internet zu entfernen. Dies stellte sich jedoch als eine größere technische Herausforderung dar, da weder der Träger noch Mitarbeiter der Kindertagesstätte diese Konzeption veröffentlicht hatten, sondern vermutlich eine Praktikantin.

Wir nahmen diesen Vorfall noch einmal zum Anlass, auf die Verpflichtung aus § 5 KDG hinzuweisen. Danach sind die mit der Verarbeitung personenbezogener Daten betrauten Personen bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis und die Einhaltung der einschlägigen Datenschutzregelungen schriftlich zu verpflichten! Die unbefugte Erstellung einer „Homepage“ wie auch bereits das unbefugte Einstellen von Bildern ins Internet, der kein Auftrag des Verantwortlichen zugrunde liegt, stellen eine unerlaubte Verarbeitung personenbezogener Daten dar.

In diesem Zusammenhang müssen ebenso die urheberrechtlichen Fragen Berücksichtigung finden, denn viele Anbieter überprüfen die Inhalte nicht, so dass unter Umständen Schadenersatzanforderungen auf die Verantwortlichen (hier: Ersteller der Bilder) zukommen können.

Sharehoster oder Clouds können je nach Anwendung trotzdem eine gute und sichere Lösung sein, Dokumente anderen zugänglich zu machen. Hier sollten aber, wie auch bei anderen Diensten, die mit Hilfe des Internets zur Verfügung stehen, die Nutzungsbedingungen, Datenschutzbestimmungen und Speicherorte der Daten transparent sein sowie die datenschutzrechtlichen Bestimmungen eingehalten werden. Viele Anbieter ermöglichen passwortgeschützte Lösungen, so dass Dokumente nur einer begrenzten Menge Nutzern zur Verfügung gestellt werden.

In dem geschilderten Fall standen alle rechtlichen Angaben wie Nutzungsbedingungen und Datenschutzbestimmungen nur in Englisch zur Verfügung. Ein Impressum war auf der Seite des Dienstanbieters nicht ver-

fügbar, weshalb ein Verantwortlicher nicht zu ermitteln war. Erschwerend kam auch hinzu, dass es keine Kontakte mehr zu der Praktikantin gab, die dieses Dokument auf der Plattform hochgeladen hatte.

Der Träger dieser Einrichtung hat im Weiteren den Sharehoster mit Hilfe einer auf der Webseite angegebenen Mailadresse kontaktiert, mit der Bitte dieses Dokument umgehend zu löschen. Das Dokument wurde in diesem Fall von dem Sharehoster-Dienst gelöscht.

5.5 Informationspflichten

5.5.1 Informationspflichten trotz Einwilligungserklärung am Beispiel von Fotos

Eine Einwilligungserklärung für Fotoaufnahmen, sog. Fotoerlaubnis, einzuholen hat sich mittlerweile in fast allen Einrichtungen etabliert. Auch unsere Dienststelle hatte sich bereits in der Vergangenheit mehrfach mit dem Thema Foto und Fotoerlaubnis auseinandergesetzt.

Neben der einzuholenden Einwilligungserklärung muss der Verantwortliche aber auch dafür sorgen, dass dem Betroffenen die Informationen gemäß §§ 15, 16 KDG übermittelt werden. Informationspflichten werden auch dann ausgelöst, wenn die rechtliche Grundlage eine Einwilligungserklärung ist.

Dieses trifft besonders auf Bildungs- und Betreuungseinrichtungen zu, da dort häufig Bildnisse für unterschiedlichste Zwecke angefertigt werden. Die Erklärung gem. §§ 15, 16 KDG zur Datenerhebung (Informationspflichten) an die Betroffenen entfällt auch dann nicht, wenn die angefertigten Bilder nicht veröffentlicht oder nur in der Einrichtung verwendet werden. Allein das bloße Erstellen eines Fotos stellt eine Verarbeitung personenbezogener Daten i.S. von § 4 Nr. 3 KDG dar. Auch § 15 Abs. 1 KDG stellt klar, dass sobald personenbezogene Daten bei der betroffenen Person erhoben werden, diese darüber zu informieren ist.

Selbst wenn es eine Rechtsgrundlage für die Erstellung von Fotos gibt, muss die betroffene Person über diese Verarbeitung ihrer personenbezogenen Daten informiert werden.

Somit kommen Bildungs- und Betreuungseinrichtungen um die Erfüllung der Informationspflichten durch Aushändigung entsprechender Hinweisblätter an die Betroffenen, i. d. R. die Erziehungsberechtigten, nicht herum. Die einzige Ausnahme bleibt, dass grundsätzlich keine Bilder von den Kindern angefertigt werden.

Welche Informationen gemäß § 15 KDG sind in Bezug auf die Fotos besonders hervorzuheben bzw. unterscheiden sich von den allgemeinen Auskünften wie Angabe des Verantwortlichen oder des betrieblichen Datenschutzbeauftragten?

In den Hinweisblättern zur Datenerhebung muss beschrieben werden, zu welchen Zweck die Bildnisse angefertigt werden. Sind eine Rechtsgrundlage oder eine gesetzliche Verpflichtung der Zweck für das Verarbeiten von Fotos, so sind auch diese konkret zu benennen. Das Führen einer Entwicklungsdokumentation dürfte als Zweck -Erfüllung der Einrichtung zugewiesenen gesetzlichen Aufgaben- jedoch ausscheiden, da zwar die Verpflichtung der Einrichtung besteht eine Entwicklungsdokumentation zu führen, jedoch Fotos nur ein Mittel von vielen sind, diese zu dokumentieren. Auch berechtigte Interessen gemäß § 6 Abs. 1 lit. g) KDG für das Anfertigen und Verarbeiten von Fotos werden in Bildungs- und Betreuungseinrichtungen schwer zu begründen sein.

Das Hinweisblatt zu den Informationspflichten muss Angaben zur Speicherdauer bzw. zu Löschfristen der erstellten Fotos enthalten. Die Einrichtungen sollten an dieser Stelle abwägen, wie lange sie erstellte Bildnisse wirklich verarbeiten bzw. vorhalten. Zudem sind hier die unterschiedlichen Speichermedien sowie auch der Grundsatz der Zweckbindung zu berücksichtigen. Wenn der Zweck erfüllt ist, für den das Bild erstellt wurde, so ist dieses zu löschen[60].

Wenn Einrichtungen Bilder über Fotodienstleister entwickeln lassen, müssen Angaben wie Speicherdauer, Speicherort (Rechenzentrum), Weitergabe an Dritte etc. vom Dienstleister erfragt und in den Hinweis zur Informationspflicht wiedergegeben werden. Eine kursorische Überprüfung der Datenschutzbestimmungen einiger Fotodienstleister hat ergeben, dass zwar

60 Dr. Federrath/Hautumm-Grünberg, in: Datenschutz bei Bild-, Ton- und Videoaufnahmen, 2. Aufl. 2020, BlnBDI & Senatsverwaltung Berlin

die Speicherdauer der Bilddateien angegeben wird, nicht aber der Speicherort.

Zu den Informationspflichten gehören auch Angaben zur Weitergabe bzw. Empfänger der Fotos, dies können z.B. Presse, Förderverein oder auch andere Eltern sein. Wenn diese Angaben bereits in der Fotoeinwilligungserklärung enthalten sind, muss keine zusätzliche Information erfolgen (ein Muster befindet sich im Anhang).

5.6 Nachweis von Schutzimpfungen in Gemeinschaftseinrichtungen

Aufgrund des im Jahr 2020 eingeführten Masernschutzgesetzes, wonach alle nach 1970 geborenen Beschäftigten sowie Kinder in Einrichtungen einen Schutz gegen Masern aufweisen müssen, sind die Erziehungsberechtigten verpflichtet dieses entsprechend nachzuweisen.

So ist unserer Dienststelle wiederholt aufgefallen, dass die Kindergärten und Schulen diese Nachweise durch Vorlage oder auch Kopie des Impfausweises des aufzunehmenden Kindes verlangen.

Dieses Vorgehen entspricht jedoch nicht dem allgemeinen Grundsatz der Datensparsamkeit. Zum einen sind in einem Impfausweis weit mehr Immunitätsnachweise enthalten, als für die Aufnahme des Kindes erforderlich sind. Zum anderen wird eine Immunität auch nach einer Infektion mit einem Erreger ausgelöst, welcher dann eben nicht im Impfausweis dokumentiert ist.

Weiterhin führt die Vorlage einer Kopie auch oft zum grundlosen Aufbewahren dieser in der Kinder- oder Schülerakte. Das Aufbewahren in Akten stellt eine Verarbeitung im Sinn von § 4 Nr. 3 KDG dar. Die Verarbeitung besonderer Kategorein personenbezogener Daten, wozu Impfausweise oder Immunitätsnachweise zählen, ist nach § 11 KDG grundsätzlich untersagt und nur in besonderen Ausnahmefällen erlaubt.

Daher empfehlen wir grundsätzlich, sich eine Immunität gegenüber einer Infektionskrankheit, z.B. Masern mit Hilfe eines ärztlichen Attests bescheinigen zulassen. Es ist ausreichend, wenn der ausstellende Arzt bestätigt,

dass die Immunität vorliegt. Ob diese durch Schutzimpfung oder Infektion erreicht wurde, ist dabei unerheblich. Natürlich dürfen Erziehungsberechtigte auch weiterhin den Impfausweis vorlegen. Dieser sollte jedoch nicht kopiert werden. Eine Einsichtnahme bzw. Vorlage und Dokumentation reicht in beiden Fällen aus.

6 Datenschutz im Beschäftigtenverhältnis

6.1 3G am Arbeitsplatz / Listen und Testate

Im Berichtszeitraum wurde das Infektionsschutzgesetz mehrfach geändert. Am 24.11.2021 traten neue und weitreichende – Regelungen zur Bekämpfung der Coronapandemie in Kraft. Darüber hinaus hat der Bundestag mit Wirkung ab dem 16.03.2022 einen einrichtungsbezogenen Immunitätsnachweis beschlossen. Die Änderungen haben erhebliche Auswirkungen auf das Beschäftigungsverhältnis.

Mit Einführung des § 28 b IfSG dürfen Arbeitnehmer und Beschäftigte, Arbeitsstätten nur noch dann betreten, wenn sie geimpft, genesen oder getestet sind. Zudem muss ein Impfnachweis, einen Genesenennachweis oder einen offiziellen Testnachweis gemäß COVID-19-Schutzmaßnahmen-Ausnahmenverordnung (Testzentrum, Test unter Aufsicht des Arbeitgebers oder durch entsprechend geschultes Personal) mitgeführt werden.

Arbeitgeber sind gemäß § 28 b Abs. 3 IfSG nunmehr verpflichtet, die 3G-Bestimmungen durch Nachweiskontrollen täglich zu überwachen und regelmäßig zu dokumentieren; jeder Beschäftigte ist im Gegenzug verpflichtet, einen entsprechenden Nachweis auf Verlangen vorzulegen. Die Arbeitgeber dürfen im Rahmen ihrer Überwachungspflicht personenbezogene Daten einschließlich der Daten zum Impf-, Sero- und Teststatus verarbeiten.

Bei der Umsetzung der 3G-Prüfpflicht ist folgendes zu beachten:

- Verantwortliche haben Beschäftigten die Pflichtinformationen nach § 15 Abs. 1 und 2 KDG (Art. 13 Abs. 1 und 2 DS-GVO) zu erteilen. Diese Information über die Art und Weise der Datenverarbeitung sollte allen Beschäftigten zugänglich gemacht werden, in jedem

Fall zum Zeitpunkt der Kontrolle der entsprechenden Nachweise, wobei ein Informationsblatt oder ein Link zu einem digital bereit gehaltenen Dokument ausreichend sei.

- Das Verfahren der Verarbeitung des Impf-, Sero- und Teststatus soll in einem Verzeichnis von Verarbeitungstätigkeiten § 31 KDG (Art. 30 DS-GVO) dokumentiert werden.
- Die Vorgaben der Datensicherheit nach § 26 KDG (Art. 32 DS-GVO) sind einzuhalten. Nicht zulässig dürfte sein, Nachweise zu kopieren oder einzuscannen. Das Vermerken, dass Nachweise vorgelegen haben, genügt.
- Es muss verhindert werden, dass unbefugte Zugriff auf die Gesundheitsdaten der Beschäftigten erhalten. Befugt sind nur die mit der Verarbeitung betrauten Personen.
- Es gilt der Grundsatz der Zweckbindung. Eine Verarbeitung zu anderen Zwecken ist nicht zulässig. Nach Ablauf der Speicherdauer (spätestens 6 Monate) sind die Daten zu löschen.

Grundsätzlich sollte stets versucht werden, so datensparsam wie möglich vorzugehen. Kann auf Namenslisten verzichtet werden, sollte man dies auch tun. Kann darauf verzichtet werden, den Impf- und Genesenenstatus zu speichern, sollte auch hierauf verzichtet werden.

6.2 Namensschilder / Persönlichkeitsrechte von Mitarbeitenden werden konsequent ignoriert!

„Der Treue des Mitarbeiters muss von Seiten des Dienstgebers die Treue und Fürsorge gegenüber dem Mitarbeiter entsprechen“ (§ 1 Abs. 2 Kirchliche Dienstvertragsordnung).

Weil der Arbeitgeber es als besonderen Service zur Ansprechbarkeit betrachtet, werden Arbeitnehmer von Arbeitgebern immer wieder verpflichtet, ihren Vor- und Nachnamen im dienstlichen Kontext zu verwenden. Besonders häufig begegnet man solchen Forderungen in Kranken- und Pflegeeinrichtungen. Dort sind Arbeitnehmer verpflichtet, entsprechende Namensschilder zu tragen. Gerade aber im Bereich körpernaher Dienst-

leistungen besteht regelmäßig die Gefahr, dass Patienten in der Pflegeleistung mehr als eine Dienstverrichtung sehen.[61] Nach Dienstende oder außerhalb der Dienstzeit haben Arbeitnehmer ein schützenswertes Interesse nicht von Patienten kontaktiert zu werden. Der Arbeitgeber ist verpflichtet, alle Maßnahmen zu ergreifen, um die persönliche Integrität und das Sicherheitsinteresse von Mitarbeitenden zu schützen. Das Interesse des Arbeitgebers ist demgegenüber nur soweit schützenswert, wie das Persönlichkeitsrecht Betroffener nicht gefährdet wird.

Es ist deshalb erforderlich zwischen den betroffenen grundrechtlichen Positionen eine praktische Konkordanz herzustellen.

Durch die vollständige Nennung von Vor- und Nachnamen nebst Berufsbezeichnung ist es möglich per Onlinerecherche zahlreiche Informationen über Mitarbeitende zusammenzutragen oder Onlineprofile über sie zu erstellen.[62] Für die Zweckerreichung des Arbeitgebers ist die Verarbeitung personenbezogener Maßnahmen auf das notwendige Maß (§ 7 Abs. 1 lit. c) KDG) zu beschränken. Danach ist es ausreichend, wenn wahlweise der Vor- oder der Zuname auf dem Namensschild angebracht wird.

Diese Forderung ist keineswegs neu. Sie wurde mehrfach von unserer Dienststelle in unseren Tätigkeitsberichten publiziert.[63] Unsere Rechtsauffassung wird dabei von anderen Aufsichten im kirchlichen Bereich[64] ebenso geteilt, wie von Landesbeauftragten für Datenschutz.[65]

Auch in der außerkirchlichen Wirklichkeit ist diese Forderung längst angekommen.[66]

Dennoch gehen in der „Kirchlichen Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs“ (KDSA) Anfragen von Mitarbeitervertretungen oder Beschwerden von Arbeitnehmern ein. Arbeitgeber sind demnach offensichtlich nicht bereit, ihrer Fürsorgepflicht zum

61 TLfDI, 2. TB für den nichtöffentlichen Bereich 2014/2015 Punkt 5.13
62 Siehe dazu EuGH, Az.: C-362/14
63 KDSA Ost, TB 2019, Punkt 8.3.2, mit weiterem Hinweis auf TB 2017, Punkt 7.3.4
64 KDSA Nord, 7. TB 2020, S. 22
65 TLfDI, 1. TB zur DS-GVO 2018, Punkt. 7.14, mit weiterem Hinweis auf den TB für den nichtöffentlichen Bereich 2014/2015 Punkt 5.13
66 https://www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen-und-handlungshilfen/namensschilder-auf-der-arbeitskleidung-15400; https://www.datenschutz-notizen.de/namensschilder-in-gesundheitseinrichtungen-4615049/

Schutz der Persönlichkeitsrechte ihrer Mitarbeiter nachzukommen. Aufgrund der klaren und wiederholt dargestellten Rechtslage werden derartige Verstöße in Zukunft von der Kirchlichen Datenschutzaufsicht mit Sanktionen verfolgt!

7 Technischer Datenschutz

Die Datenschutzgesetze juristisch zu verstehen, ist nur die eine Seite eines erfolgreichen Datenschutzes im Unternehmen. Die technische Implementierung der gesetzlichen Vorgaben erfordert gute Kenntnisse im Bereich der IT-Sicherheit.

Je weiter die Digitalisierung und Zentralisierung unserer Daten voranschreitet, desto mehr verschmelzen zunehmend gesetzliche Vorgaben und technische Anforderungen. Wir bemerken das an den zunehmenden Datenschutzvorfällen und Cyber-Attacken, so dass die Sicherheit und damit auch der Schutz all unserer Daten und Informationen zunehmend wichtiger werden.

Im Zusammenhang mit dem technischen Datenschutz finden die Begriffe Datensicherheit, Informationssicherheit und IT-Sicherheit und Datenschutz Verwendung. Die Begriffe Datenschutz und Datensicherheit werden im Eifer des Gefechts oder aber aus Unwissenheit häufiger falsch verwendet.

Zunächst geht es um die Unterscheidung zwischen Datenschutz und Datensicherheit. Zunächst einmal ist zu betonen, dass eine klare Definition und exakte Abgrenzung der beiden Begrifflichkeiten nicht ohne weiteres möglich ist. Der folgende Versuch zur Abgrenzung soll als Orientierung dienen:

Datenschutz ist am einfachsten mit dieser kurzen Definition zu verstehen: Unter Datenschutz versteht man den Schutz von personenbezogenen Daten. Hierunter fallen alle Daten, die sich auf eine natürliche Person beziehen. Ziel des Datenschutzes ist der Schutz des allgemeinen Persönlichkeitsrechts der betroffenen natürlichen Personen. Normen hierzu finden sich in den jeweiligen Datenschutzgesetzen. Der Datenschutz dient somit dem Zweck natürliche Personen und ihre Grundrechte und Grundfreiheiten zu schützen.

Datensicherheit beschäftigt sich hingegen generell mit der Sicherheit von Daten. Ziel der Datensicherheit ist der Schutz von Daten allgemein, nicht nur von personenbezogenen Daten. Hierunter fallen damit auch reine Unternehmensdaten, also Daten von juristischen Personen. Das oberste Ziel der Datensicherheit besteht in der Gewährleistung

- der Vertraulichkeit
- der Integrität und
- der Verfügbarkeit von Daten

Vereinfacht könnte man sagen, dass es sich hier um die praktischen Sicherheitsmaßnahmen oder Ansätze zum Schutz von Daten handelt (z.B. Maßnahmen zur Datensicherung, technischer Schutz vor Datenverlust usw.).

Zu unterscheiden sind des Weiteren die Begriffe IT-Sicherheit und Informationssicherheit. Beide Begriffe hören sich ähnlich an, doch es gibt gravierende Unterschiede.

Zu Daten gehören auch Informationen, die nicht ausschließlich digital/elektronisch verarbeitet werden, z.B. Informationen durch „Wissen“ oder in Form einer Zeichensprache (Zinkerzeichen). In diesem Zusammenhang spricht man von **Informationssicherheit**. Diese hat den Schutz von Informationen zum Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Informationen stellen für jedes Unternehmen einen bedeutenden wirtschaftlichen Wert dar, und zwar nicht erst seit heute. Sie sind das Fundament ihrer Existenz und deshalb eine wesentliche Voraussetzung für erfolgreiches Wirtschaften.

Ein Beispiel für die Wichtigkeit der Informationssicherheit ist das so genannte Social Engineering. Dies dient seit Urzeiten als Grundlage für verschiedenste Betrugsmaschen. Im Zeitalter der digitalen Kommunikation stehen dem Kriminellen jedoch viele neue Möglichkeiten zur Verfügung, Millionen von Opfer zu erreichen. Ein Opfer wird z.B. dazu verleitet, vertrauliche Informationen preiszugeben, Überweisungen zu tätigen, Schadsoftware auf den privaten PC oder den Rechner im Firmennetzwerk herunterzuladen und Sicherheitsfunktionen außer Kraft zu setzen. Der Informationssicherheit ist daher immense Bedeutung beizumessen.

Als **IT-Sicherheit** (IT-Security) definiert man gemeinhin den Schutz von IT-Systemen vor Schäden und Bedrohungen. Das erstreckt sich von der einzelnen Datei über Computer, Netzwerke, Cloud-Dienste bis hin zu ganzen Rechenzentren. IT-Sicherheit umfasst alle technischen und organisatorischen Maßnahmen, um Systeme vor Cyber-Angriffen und anderen Bedrohungen zu schützen. Dazu zählen zum Beispiel Zugriffskontrollen, Kryptographie, Rechtemanagement, Firewalls, Proxies, Viren-scanner, Schwachstellenmanagement und vieles mehr. Der Begriff **Internet Security** bezieht sich konkret auf den Schutz vor Bedrohungen aus dem Internet. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.

Ein Beispiel, bei dem der Datenschutz und die IT-Sicherheit betroffen waren, gab es im aktuellen Berichtsjahr bei einem Hacker-Angriff auf den Landkreises Anhalt-Bitterfeld. Dabei wurden u.a. von den Cyber-Kriminellen Daten im sogenannten Darknet veröffentlicht.

Mit zunehmender Digitalisierung wird der technische Schutz von Daten eine immer wichtigere Rolle spielen. Allerdings sind „juristische" Vorgaben aus technischer Sicht nicht immer logisch und praktikabel umsetzbar. Mit juristischem Augenmaß und mit pragmatischen und sinnvollen technischen wie auch organisatorischen Maßnahmen sollten wir stehts versuchen, so viel Informationssicherheit wie möglich zu etablieren, regelmäßig auf den Prüfstand zu stellen und ggfs. nachzusteuern. Damit kommen wir nicht nur dem Schutz aller uns anvertrauten Daten und Informationen nach, sondern betrachten die Datenschutzgesetze nicht mehr als eine unbequeme gesetzliche Pflicht.

7.1 Windows datenschutzkonform – warum nicht

Seitdem das Betriebssystem Windows 10 mit seinen Versionen im Markt Einzug gehalten hatte, spielte der Datenschutz sowie eine Telemetriedaten-Übermittlung bei Computer-Betriebssystemen eine zunehmend sensiblere Rolle. Die Medien hatten dahingehend zur Genüge berichtet. Bereits bei der Installation von Microsoft Windows 10 zeigte sich, dass datensparsame Voreinstellungen nicht zum Standard gehören. Schnell erkannte man, dass es sich bei Windows 10 nicht mehr um ein einfaches Betriebssystem han-

delt, sondern vielmehr um eine Sammlung verschiedenster Funktionalitäten, die weit über ein „nur" Betriebssystem hinausgehen. Damit stieg u.a. die Skepsis, so ein System datenschutzfreundlich und/oder datensparsam zu betreiben, weshalb Administratoren, Betriebe und Behörden Windows 10 nicht unbedingt einsetzen wollten. Solche Bestrebungen waren allerdings nur von kurzer Dauer, denn die älteren Microsoft Betriebssysteme, wie Windows 7 oder Windows 8.1. waren Auslaufmodelle und zählten nicht mehr zum „Stand der Technik"[67].

Der Arbeitskreis Technik (AK Technik) der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands (DDSB) hatte sich im Berichtsjahr 2020 vor dem Hintergrund des EuGH-Urteils vom 16. Juli 2020 („Schrems II", C-311/18) u.a. mit dem Thema „Datenschutz unter Windows 10" (wie die Länder, Behörden, BSI) auseinandergesetzt und 2021 die Ergebnisse als „Technische Hinweise für Windows 10 im Rahmen der Verarbeitungstätigkeit"[68] im Internet veröffentlicht. Eine Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten war nicht Gegenstand der Überprüfung, vielmehr ging es darum, einen „datensparsamen Betrieb" mit Hilfe von Konfigurationsmöglichkeiten, die das Betriebssystem selbst bietet, weitestgehend zu ermöglichen. Dabei wurde nicht nur die große Windows 10 Enterpreis Version (EP) betrachtet, sondern auch die Windows 10 Professionell Version (Pro). Hintergrund war, dass die kirchlichen Einrichtungen, Betriebe oder Organisationen nicht immer die Möglichkeit haben, die speziellen Enterprise Versionen (Volumen Lizenz) einzusetzen.

Bei den getesteten Betriebssystemen konnte mit entsprechendem Aufwand ohne zusätzliche Tools ein datensparsamerer Betrieb konfiguriert werden. Das Problem, dass getroffene Einstelllungen nach einem Update zurückgesetzt werden, ist weiterhin geblieben. Zum Beispiel war nach einem Update die Taskleistenfunktion „Neuigkeiten und interessante Themen"67 als ein kleines Wettersymbol erkennbar, welches automatisch aktiviert war. Eine freiwillige Aktivierung war wieder einmal nicht dem Benutzer überlassen, eine Deaktivierung jedoch möglich. Die bereits getroffenen datensparsamen Einstellungen mussten erneut eingestellt werden.

67 https://www.teletrust.de/publikationen/broschueren/stand-der-technik
68 https://www.kdsa-ost.de/infothek/praxishilfen-arbeitshilfen.html#technischer-datenschutz

7.1.1 Nicht alles muss Online sein

Nicht nur für Microsoft Anwendungen, sondern auch für alle anderen Systeme und Anwendungen kommt es darauf an, wie und unter welchen Bedingungen diese betrieben werden. Die Mehrheit von Überprüfungen und Beurteilungen unterstellen bereits beim Ansatz eine ständige und teilweise unkontrollierte Internetanbindung. Warum ist das so? Hat sich die Online-Welt schon so eingebrannt, dass „nicht Onlinesysteme“ (nicht mit dem Internet verbunden) überhaupt nicht mehr im Fokus der Wahrnehmung stehen?

Organisatorisch könnten viele Systeme auch ohne Internetanbindung betrieben werden. Damit wäre z.B. die o.g. Windows 10 Problematik sofort gelöst. Beispielsweise könnte ein Office Arbeitsplatz wie folgt aussehen:

- Betriebssystem passend zur Betriebskultur
- Office Programme, z.B. MS Office 2019
- E-Mail-Programm
- Anwendungsprogramme, z.B. zur Abrechnung o.ä.

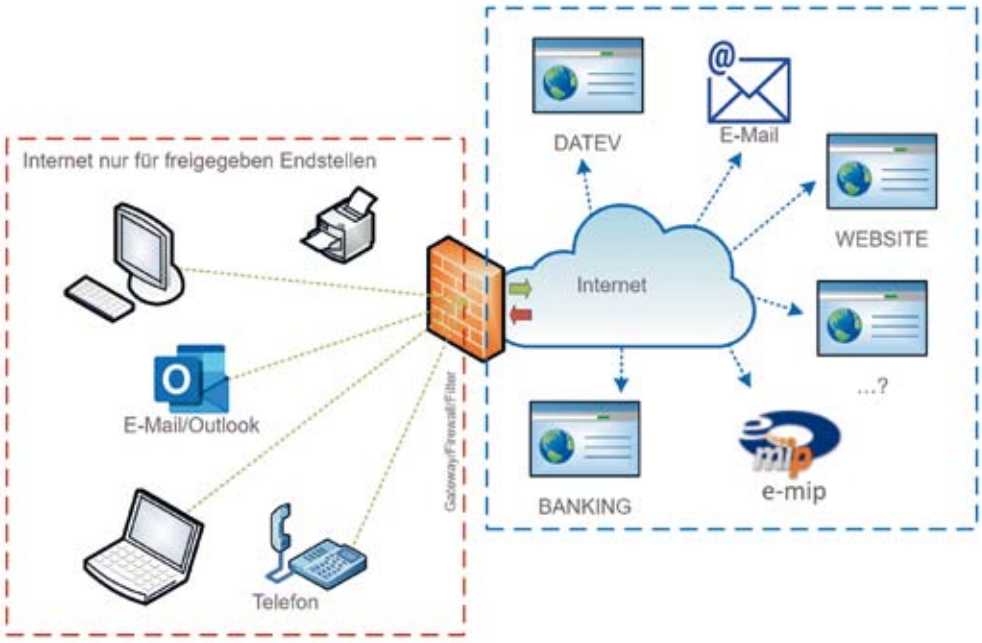
Ist das Betriebssystem einmal eingerichtet, erhält es ggfs. offline Aktualisierungen was u.a. mit einer Update-Datei oder einem eigenen Update-System erfolgen kann.

Die tägliche Arbeit kann mit den Office-Programmen erledigt werden. MS Office 2019 wurde beabsichtig erwähnt, da auch hier eine Offline-Installation möglich ist. Eine E-Mail-Kommunikation ist ebenfalls ohne permanenten Internetzugriff und ohne Einschränkungen realisierbar.

Bei den Anwendungen werden Offline- und Online-Anwendungen unterschieden (falls überhaupt erforderlich). Dafür ist aber auch kein permanenter freier Internetzugriff erforderlich. Möglich ist eine Verbindung zwischen fest definierten Endpunkten, z.B. DATEV, Banken oder e-mip.

Obwohl das Arbeitslatz-System keinen freien Internetzugriff erlaubt, müsste der Internetsurfer nicht unbedingt ausgeschlossen sein (falls IT-Richtlinien dies erlauben). Dafür gibt es genügend praxistaugliche Mög-

lichkeiten, die das vom Internet abgeschottete Arbeitsplatz-System nicht beeinflussen würden.



Fazit: Nicht Alles muss Online, nur „So viel wie nötig, so wenig wie möglich".

Es ist durchaus möglich, viele Systeme und Anwendungen sicherer und datenschutzgerecht zu betreiben. Mit überlegter Organisation und technischen Maßnahmen gelingt es das Risiko zu minimieren. Telemetriedaten, unbeabsichtigte Datenabflüsse oder automatisiert vorgeschlagenen Suchergebnisse können vernachlässigt werden und wären zumindest kontrollierbar. Das wäre u.a. ein Schritt zur Datenminimierung.

7.2 Länderübergreifende Prüfaktion

Die KDSA Ost beteiligte sich in ihrem Zuständigkeitsbereich an der bundesweit länderübergreifenden Kontrolle der Datenschutzaufsichtsbehörden der Länder zur Umsetzung der Schrems II Entscheidung des Europäischen Gerichtshofs. Für die Prüfaktion wurden Einrichtungen auf Basis folgender gemeinsamer Fragekataloge (angepasst auf das KDG) angeschrieben:

- Mailhoster (E-Mail-Dienstleister) und
- Tracking-Tools (Nutzertracking auf Websites).

Zur Vorauswahl von Einrichtungen und Organisationen für die Prüfaktion wurden in einem ersten Schritt ca. 100 Internet-Domains aus dem Zuständigkeitsbereich der KDSA Ost ermittelt und einer ersten technischen Überprüfung unterzogen. Als Selektions-Kriterium für den zu ermittelnden Serverstandort wurden die aus der Überprüfung resultierenden IP-Adressbereiche mit Hilfe des Whois-Dienstes abgefragt. Auch wenn dieses Kriterium nicht unbedingt eindeutig für eine Zuordnung zum tatsächlichen Serverstandort sein muss (z.B. Geolocation Services), war dieses Vorgehen für den Zweck ausreichend.

Im Ergebnis konnten wir feststellen, dass nur eine sehr geringe Anzahl an Einrichtungen/Organisationen Dienstleister im Ausland einsetzt. Bei der Mehrheit der überprüften Domains handelte es sich um Webhoster und E-Mail-Dienstleister mit Serverstandort innerhalb der EU. In den meisten Fällen war der Webhoster zugleich der E-Mail-Dienstleister – also alles beim selben Provider.

Das Ergebnis im **Fragebogen „Tracking-Tools“** zeigte dennoch einen Bedarf an Nachbesserungen:

- Bevor es zu einer Einwilligung durch einen sogenannten Cookie-Banner (Consent-Banner) kommt, werden oftmals Cookies mit einer längeren Lebensdauer von Dritt-Anbietern gesetzt.
- Websites enthielten eingebettete Code-Verlinkungen auf Websites „Dritter“. Damit erfolgt u.a. eine Datenübermittlung (zumindest der Web-Browser Metadaten) an den „Dritten“.
- Datenschutzinformationen waren nicht immer konform mit den Datenübermittlungen. Auffällig war u.a., dass verwendetet Vorlagen aus dem Internet nicht an die eigenen Bedürfnisse der Website angepasst waren (trotz der Hinweise in den Vorlagen).
- Die Voreinstellungen der Consent-Banner entsprach nicht dem Prinzip „Datenschutz by Default“.

Positiv festzustellen war, dass relativ wenig Website-Betreiber, die überprüft wurden, Tracking/Analyse-Tools mit Drittlandtransfer eingesetzt hatten. Zur Website-Analyse kam vorwiegend das Tool „Matomo“ zum Einsatz.

Der Tenor im **Fragebogen „Mailhoster“** lag auf dem Dienstleister, der für die Verarbeitung (speichern, versenden, archivieren, etc.) der betrieblichen E-Mails zuständig ist.

In dem o.g. ersten technischen Prüfungsschritt wurden Einrichtungen und Organisationen angeschrieben, die einen Microsoft 365 Service nutzen. Davon betroffen waren nur einige größere Einrichtungen.

Nach Auswertung der Antworten sind wir zu der Erkenntnis gekommen, dass den befragten Einrichtungen das Thema zur Schrems II Entscheidung und den damit verbundenen Auswirkungen bewusst ist. Zur Frage „An welchem Ort befinden sich die E-Mail-Server“ gaben die Einrichtungen an, dass ein Umzug auf Server in Deutschland bereits beim Dienstleister (Microsoft) beantragt wurde. Die Speicherorte für Kundeninhalte (ruhende Daten) lagen in der EU.

Im Ergebnis lief die Überprüfung kooperativ ab. Einer Bitte um Fristverlängerung zur Abgabe der Formulare wurde in allen Fällen entsprochen. Diese stichprobenartige, länderübergreifende Überprüfung diente lediglich einer Informationserhebung. Eine Sanktionierung durch die KDSA Ost war nicht beabsichtigt.

Im Rahmen dieser Aktion konnten wir eine Sensibilisierung dahingehend feststellen, dass einige Befragte die Fragebögen als Anlass nahmen, um ihre Website selbst noch einmal auf den Prüfstand zu stellen. Was in Anbetracht des Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG), welches seit dem 01.12.2021 in Kraft ist, auch für alle anderen Website-Betreiber sinnvoll wäre.

Der Datenschutz kann nicht dafür verantwortlich gemacht werden, dass Internetangebote teilweise mit vielen Bestätigungs-Bannern überfrachtet sind. Das Gegenteil ist der Fall, der Datenschutz öffnet den Benutzern die Augen, was alles beim Besuch einer Website oder bei Mobile-Apps über ihn gesammelt wird und später ausgewertet werden kann.

Unsere Prüfaktionen werden wir weiter ausbauen und sowohl anlassbezogen als auch anlasslos fortführen. Anlassbezogene Überprüfungen sind u.a. Beschwerden zum Inhalt oder zur Verarbeitung personenbezogener Daten (z.B. Formulardaten, Datenübermittlungen an Dritte) einer Website.

Allgemeine Abfragen im Rahmen eines Prüfformulars oder auf Grund einer besonderen Situation, wie einer bekanntgewordenen Schwachstelle (z.B. Exchange) oder einer Gesetzesänderung (z.B. TTDSG), sind Beispiele für anlasslose Überprüfungen.

7.3 Exchange Schwachstelle

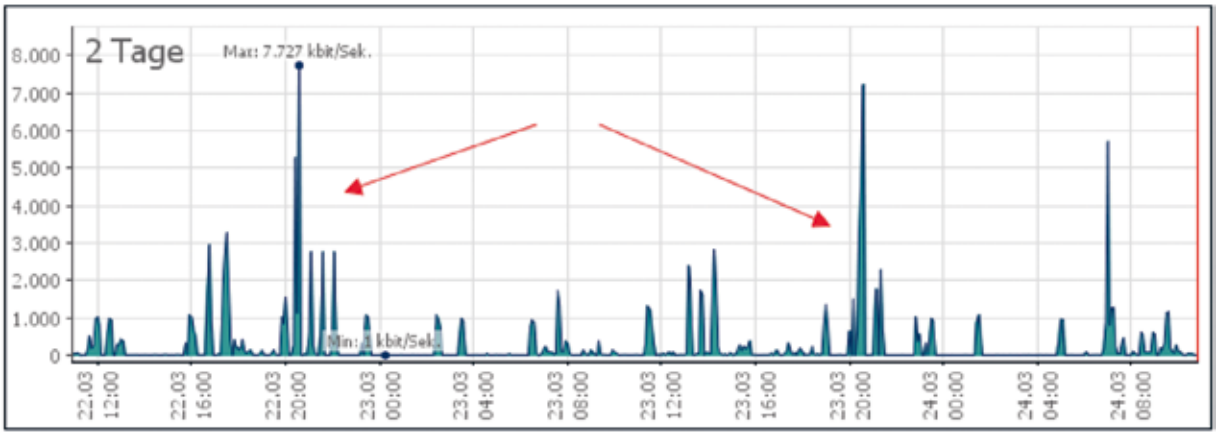
Im aktuellen Berichtsjahr wurden Schwachstellen im Microsoft Exchange[69] System festgestellt. Die Medien und das BSI[70] wie auch der Softwarehersteller sprachen eine Warnung zu einer kritischen Schwachstelle in Exchange-Servern aus. Anfällige Exchange-Systeme sollten aufgrund des sehr hohen Angriffsrisikos dringend auf entsprechende Auffälligkeiten geprüft werden. Es wurden entsprechende Informationen, Werkzeuge (Tools), etc. bis hin zur Eingrenzung und Behebung der bekannt gewordenen Schwachstellen veröffentlicht.

Diese Informationen zur Sicherheitsanfälligkeit betroffener Systeme, die über das Internet erreichbar sind, nahmen wir zum Anlass einer technischen Überprüfung. Ziel der Überprüfung über das Internet war die Ermittlung, inwieweit bei geprüften E-Mail-Domains ein Exchange Server eingesetzt wurde und soweit es möglich war, welche Software Version im

69 https://news.microsoft.com/de-de/hafnium-sicherheitsupdate-zum-schutz-vor-neuem-nationalstaatlichem-angreifer-verfuegbar
70 https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210305_Exchange-Schwachstelle.html;
https://twitter.com/BSI_Bund/status/1367854805654384641

Einsatz ist. Bei den überprüften E-Mail-Domains konnten wir feststellen, dass es in unserem Zuständigkeitsbereich nur einen geringen Anteil an Exchange Servern mit Außenanbindung gibt. Allerdings wurden die Systeme in einer älteren Version (CU Version) betrieben (soweit die verfügbaren Tools das ermitteln konnten). Verantwortliche Stellen wurden daraufhin aufgefordert, eine Überprüfung und Aktualisierung ihrer Systeme zeitnah vorzunehmen. Weitere Informationen und Empfehlungen zur Exchange Server Sicherheitsanfälligkeit konnten u.a. auf unserer Website abgerufen werden.

Im Rahmen einer stichprobenartigen Überprüfung im vierten Quartal 2021 (auf Grund der bekannt gewordenen Exchange Sicherheitslücke „Hafnium“) stellte sich heraus, dass noch immer viele ungepatchte produktive Exchange Server online sind. Es gibt u.a. Vermutungen, dass kompromittierte Systeme zum Teil nicht gänzlich bereinigt wurden. Eine gewisse Unsicherheit bringt die Tatsache mit sich, dass auch Dateien auf dem System abgelegt werden können, wie z.B. eine „Backdoor Anwendung“, die im Hintergrund ihre Dienste verrichtet. Ist diese erstmal gestartet, so kann ein Datenkanal vom Exchange Server über das Internet zu den Cyberkriminellen hergestellt werden. Dabei würde es sich um eine Standard Https-Verbindung von „Innen nach Außen“ handeln, die wahrscheinlich zeitnah keiner größeren Bedeutung zuzuordnen ist. Hilfreich sind zusätzliche Monitoring Mechanismen, die den Datenverkehr auf untypische Verbindungen z.B. auch auf untypischen Zeiten überwachen können.



Beispiel Monitoring: Datenverkehr ausgehend, untypische hohe Spitzen außerhalb der Geschäftszeiten

7.4 Telefax (nicht) datenschutzkonform

Auch im aktuellen Berichtsjahr war der Informationsversand per Telefax ein nicht unbedeutendes Thema. Behörden und Medien berichten unter dem Motto das „Telefax ist nicht Datenschutz konform!". Wie alles andere im Internet, macht auch schnell so eine pauschale Überschrift die Runde. Befasst man sich etwas genauer mit den entsprechenden Veröffentlichungen, so war festzustellen, dass enthaltene Aussagen teilweise unter verschiedenen Bewertungen bzw. Kriterien getroffen wurden. Beispielsweise wurde eine Datenübermittlung von einem Telefaxgerät zu einem Telefax-Service im Internet bewertet. Wie das Fax als Anlage weiter an die Empfänger gelangt, ist ungewiss und könnte zu einem Datenschutzproblem werden. In so einem Szenario wäre das aber keine direkte „Telefaxgerät-zu-Telefaxgerät" Verbindung[71] und demzufolge damit auch nicht gleichzustellen. Diesbezügliche pauschale Aussagen sollte man mit Vorsicht betrachten. Sie wären nicht unbedingt förderlich für das Verständnis, worum es beim Datenschutz (unsere Daten unter Schutz) geht. Es klingt dann wiedermal nach einem „pauschalen Verbot" für eine Technologie. Datenschutz und Informationssicherheit werden dann als unnötiger Ballast angesehen und nicht als ein Schutzschild vor einem Missbrauch unserer persönlichen Daten.

In unseren letzten Tätigkeitsberichten[72] gingen wir auf das Thema „Telefax vs. E-Mail" ein. Unbestritten ist, dass bei der Übermittlung personenbezogener Daten die Einrichtung entsprechende Sicherungsvorkehrungen treffen muss, damit sensible Informationen nicht an „Dritte" gelangen. Ein entsprechendes Schutzniveau richtet sich nach der Sensibilität der zu übermittelnden Informationen (persönliche oder sicherheitsrelevante), den potentiellen Gefahren bei der Datenübermittlung sowie dem Grad der Schutzbedürftigkeit des Betroffenen (Risiko, Datenkategorie, Datenschutzklasse). Das hat aber nicht nur etwas mit der Daten-

71 KDSA Ost, TB 2019, Abschnitt 7.4 Das Telefax im IP-Netz
72 KDSA Ost, TB 2020, Abschnitt 7.1 Das Telefax vs. Die E-Mail

übermittlung per Telefaxgerät zu tun, sondern auch mit einer Datenübertragung personenbezogener Daten und/oder sensibler Informationen im Allgemeinen.

Abgesehen vom Postweg zeigte sich, dass noch viele Einrichtungen, Betriebe, Behörden, Gerichte etc. keine andere praktikable Alternative zum Fax angeboten hatten. Damit sind die Fax-Nummern noch nicht ganz ausgestorben, was u.a. an den vielen öffentlichen Kontaktinformationen zu erkennen ist. Vielleicht liegt es an der Einfachheit der Bedienung und/oder der noch geltenden rechtskonformen Originalkopie. Aber auch, falls die gesamte IT auf Grund eines Cyber-Angriffs (Beispiel Ransomware) ausfällt und damit u.a. die gesamte E-Mail-Kommunikation brach liegen würde, könnte ein Telefaxgerät eine nicht von der Hand zuweisende rechtskonforme Kommunikations-Alternative darstellen.

7.4.1 Pauschale Aussagen nicht unbedingt förderlich für verständlichen Datenschutz

Eine Betrachtung der betriebenen IP-Netze aus einer gänzlich anderen Perspektive:

Dabei soll es nicht darum gehen, einen Kommunikationsdienst datenschutzrechtlich zu legitimieren oder zu verteidigen. Im Gegenteil, in sich stimmige Aussagen oder Beschlüsse sind eher kontraproduktiv für das Verständnis zum Datenschutz (meine Daten unter Schutz). Datenschutz darf nicht als Alibi-Funktion herhalten, um wirtschaftliche Interessen umzusetzen. Frei nach dem Motto: Muss wegen Datenschutz!

Folgende Aussagen machten im Berichtsjahr auf sich aufmerksam:

a) Das Telefax ist nicht datenschutzkonform.

b) Das IP-Netz ist standardmäßig unsicher, Faxe können ggfs. abgefangen werden und liegen dann im Klartext vor.

An dieser Stelle sei bemerkt:

1. Wird die Telefax-Strecken-Kommunikation richtig ein- und umgesetzt, dann ist ein Telefax datenschutzkonform anwendbar. Zudem sollte Beachtung finden, an welches Netz das Gerät angeschlossen ist.

So haben Gesundheitssysteme zum Teil eigens gesicherte IP-Netze (lt. KDG-DVO geschlossene oder gesicherte Netzwerke).

2. IP-Netzverbindungen (Netzstrecken) für Sprachverbindung (Telefonie) sind nicht grundsätzlich bei allen Netzbetreibern (Anbietern) mit den Kommunikationsstrecken nach Umstellung der alten Telefon-Technologie auf die aktuelle VoIP-Technologie über das öffentliche Internet gleichzusetzen. Es gibt z.B. geschützte (isolierte) Bereiche, über die eine Telefonie-Verbindung über den Träger „Internetleitung" geleitet wird. In unserem Tätigkeitsbericht 2020[73] hatten wir zur Veranschaulichung ein Rohrsysteme als Datenleitung skizziert. Wir stellen uns vor, dass in dem Rohr noch ein Rohr steckt (Telefonie-Verkehr), welches komplett vom äußeren Rohr (Internet-Verkehr) getrennt/isoliert verläuft.

3. Sicherheit und der Schutz der Datenübertragung spielen auch bei den Netzanbietern (z.B. Telekom) nach wie vor eine wichtige Rolle. Zudem sind sie u.a. durch geltende gesetzliche Vorgaben dazu verpflichtet, die Netze sicher zu betreiben und vor unbefugtem Zugriff zu sichern und zu schützen. So gibt es z.B. durch Verschlüsselung (z.B. SRTP) gesicherte Streckenverbindungen für die Echtzeitkommunikation, wo durch dann auch ein Abhören und/oder ein Abgreifen vom Kommunikationsdatenverkehr erschwert wird. Das ist aber eine „Verschlüsselung"!

4. Die Kontrolle der technischen Schutzmaßnahmen der Netzbetreiber obliegt u.a. der Bundesnetzagentur und dem BfDI (Bundesbeauftragte für den Datenschutz und Informationsfreiheit). Fraglich ist, ob Datenschutzbehörden im Rahmen der Datenschutzgesetze für die Sicherheit der Netze u.a. zuständig sind und ggfs. für das Betreiben dieser Netze Sicherheits-Anforderungen stellen können.

Fazit und offenen Fragen:

- Wer möchte das Telefax abschaffen und weshalb?
- Warum werden die Netzstrecken nicht so gesichert, dass die Frage nach einem verschlüsselten Datenverkehr in den Netzen, ähnlich wie bei TLS und E-Mail, sich erübrigt?

73 KDSA Ost, TB 2020, ab Abschnitt 7.2

- Vielleicht könnten zukünftige Geräte den Datenstrom verschlüsseln und entschlüsseln.
- Wer ist dafür verantwortlich, dass auch die Gegenstelle Sicherheitsmaßnahmen unterstützt, die der Absender in seinem Bereich mit Hilfe technischer Maßnahmen umgesetzt hat?

Werden die o.g. Aussagen so interpretiert, wie sie häufiger als Überschriften in Medien und Pressemitteilungen zu finden sind, dann ist es wohl nicht falsch zu unterstellen, dass das gesamte IP-Internet (paketvermitteltes IP-Netz) standardmäßig als unsicher anzusehen wäre. Allerdings ist dann nicht nur das Telefaxgerät ein Problemfall, sondern die gesamte Telefonie und weitere Datenübertragungen.

Wie würde man dann die Datenübermittlung per Mobilfunk einstufen, bei der es u.a. auch irgendwo einen Übergangsknoten zum IP-Internet-Netz gibt? Telefonate über persönliche Informationen müssten demnach auch Datenschutzverletzungen sein.

Müsste dann nicht das IP-Netzwerk mit seinen Backbone-Komponenten an sich auf den Prüfstand gestellt werden?

So eine Hypothese würde die Netzbetreiber wahrscheinlich nicht erfreuen. Denn es gibt für sie klare gesetzliche Vorgaben zum sicheren Betreiben von Telekommunikationsnetzen und Telekommunikationsdiensten, auf diese sich u.a. Endanwender, als Teilnehmen im IP-Netz, verlassen können sollten.

Nachfolgend einige Auszüge zu gesetzlichen Vorgaben für Telekommunikationsnetzte und -dienste (2021):

> **§ 165 TKG 2021**: *Technische und organisatorische Schutzmaßnahmen*
>
> *(1) Wer Telekommunikationsdienste erbringt oder daran mitwirkt, hat angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen*
>
> *1. zum Schutz des Fernmeldegeheimnisses und*
>
> *2. gegen die Verletzung des Schutzes personenbezogener Daten.*
>
> ...

Insbesondere sind Maßnahmen, einschließlich gegebenenfalls Maßnahmen in Form von Verschlüsselung, zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer, andere Telekommunikationsnetze und Dienste so gering wie möglich zu halten. Bei diesen Maßnahmen ist der Stand der Technik zu berücksichtigen.

BSI NET.4.2 (2021): *Verschlüsselung nur als „SOLL" – auch bei erhöhtem Schutzbedarf*

Der Baustein NET.4.2 VoIP ist auf alle Kommunikationsnetze anzuwenden, in denen VoIP eingesetzt wird. Unter 2.3 „Abhören von Telefongesprächen" wurde u.a. darauf hingewiesen, dass Sprachinformationen die beispielsweise mit dem Realtime Transport Protocol (RTP) übertragen werden, abgehört werden könnten.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Verschlüsselung der Signalisierung (H): Die Integrität und Vertraulichkeit der Signalisierungsinformationen SOLLTE durch geeignete kryptogarische Verfahren gewährleistet werden.

Sicherer Medientransport mit SRTP (H) - Mediendaten und Informationen zur Steuerung dieser Daten, die über das Real-Time Transport Protocol (RTP) übertragen werden, SOLLTEN in geeigneter Weise geschützt werden. Die Nutzdaten SOLLTEN durch den Einsatz von Secure Real-Time Transport Protocol (SRTP) beziehungsweise Secure Real-Time Control Protocol (SRTCP) geschützt werden.

ePrivacy-Richtlinie Art. 4: *Sicherheit der Verarbeitung*

Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten.

7.4.2 Telefaxübermittlung verschlüsselt

Viele VoIP Anbieter (Provider) unterstützen u.a. eine Transportverschlüsselung, die ggfs. standardmäßig an den Endgeräten nicht aktiviert ist. Ein erster Schritt wäre, beim Provider anzufragen, ob er eine Transportverschlüsselung für Telefonie (SDES-sRTP) unterstützt und ggfs. wie diese in der Telefonanlage (abhängig vom Anbieter) aktiviert werden könnte. Ggfs. ist sRTP auch schon in der Anlage/dem Endgerät aktiv.

Diese Einstellung gibt es u.a. auch bei der FritzBox ab einer entsprechenden Softwareversion. Dies kann über die Weboberfläche überprüft werden: „Rufnummer bearbeiten" auswählen und dann „Weitere Einstellungen" in den Optionen „Verschlüsselte Telefonie aktivieren" aktivieren.

Im 4. Tätigkeitsbericht[74] hatten wir für Fax das spezielle Protokoll T.38 erwähnt. Soll nun die Faxübertragung über das aktivierte sRTP Protokoll erfolgen, dann ist T.38 beim Faxanschluss und/oder dem Gerät zu deaktivieren. Das Telefaxgerät versendet danach die Faxdaten wieder als Audio-Media-Stream über sRTP, wie ein Telefonat.

So einen Hinweis hätte es u.a. in den vielen Pressemitteilungen zum „unverschlüsseltem Faxversand" geben können. Der Übermittlungs-Verschlüsselung wäre damit genüge getan.

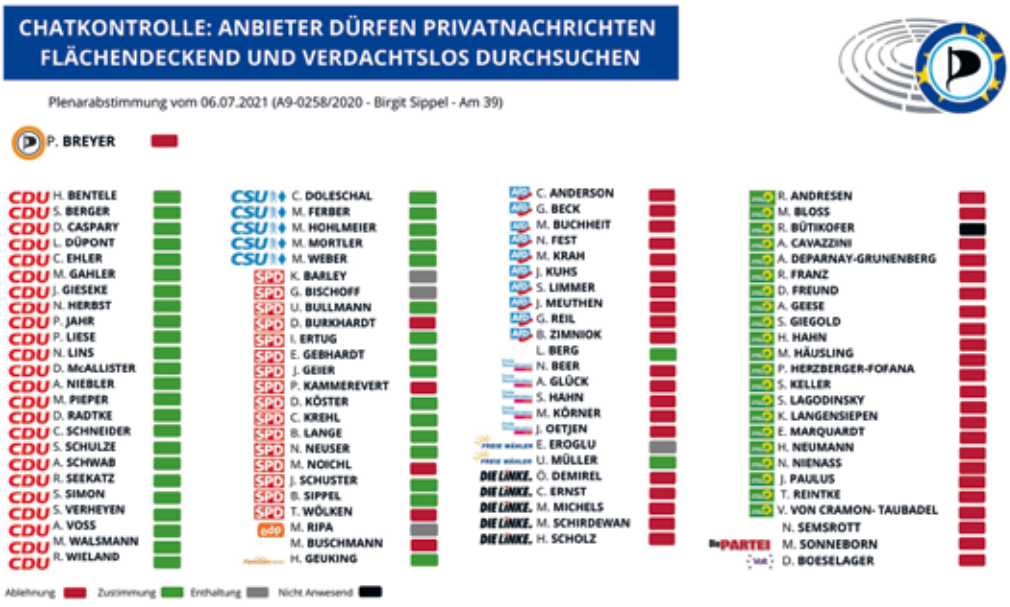
7.4.3 Verschlüsselte Kommunikation nur ein Schlagwort?

Was wäre, wenn alles Ende-zu-Ende verschlüsselt wäre, Daten verschlüsselt senden und ruhende Daten verschlüsselt speichern (außer die Kopfdaten wie IP-Adressen, damit die Datenpakete ihren Weg finden)? Nur derjenige kann sie verwerten, für den sie bestimmt sind oder deren Dateninhaber er ist. Eine Datenauskunft der Dienste-Anbieter wäre damit nicht möglich – weil eben verschlüsselt. Hier sollte nicht mit unterschiedlichen Maßstäben gemessen werden. Zugriffsschutz ist gegenüber allen Dritten, auch Sicherheitsbehörden, umzusetzen. Zur Erinnerung seien Schlagworte wie „Vorratsdatenspeicherung"[75] und das Gesetz zur Anpassung der Regelungen

74 KDSA Ost, TB 2019, Abschnitt 7.4.2
75 BT-Drs. 19/25891: Kleine Anfrage zur Praxis der Speicherung von Verkehrsdaten durch Telekommunikationsdiensteanbieter ; AK Vorrat an Koalition: Vorratsdatenspeicherung völlig ungeeignet zum Schutz von Kindern http://www.vorratsdatenspeicherung.de

über die Bestandsdatenauskunft[76] genannt. Und nicht unerwähnt bleiben sollten der Dienst „Telegram“ oder das „Scannen privater Kommunikation“ in der EU.[77]

Hinzuweisen ist auf eine Abstimmung im Bundestag zu der Frage, ob Anbieter auf Privatnachrichten und Chatverläufe anlasslos und flächendeckend zugreifen dürfen.



Einen weiteren interessanten Fall gab es beim E-Mail-Dienst Anbieter Tutanota [78] ein Dienst für Alle, denen Privatsphäre, der eigene Datenschutz und die Sicherheit bei den ruhenden Daten wichtig sind. Alles ist verschlüsselt, demzufolge hat der Anbieter alles richtig gemacht. Dennoch musste die Tutanota GmbH aufgrund eines Beschlusses des Ermittlungsrichters des BGH die Überwachung von zwei E-Mail-Adressen ermöglichen.

Es gibt noch viele weitere Beispiele, die offene Fragen aufkommen lassen:

Sind die vielen Gesetze, in denen es um den Datenschutz, die Sicherheit in der Kommunikation etc. geht, noch zueinander konform und verständlich? Ist „Verschlüsselung“ auch nur ein Schlagwort in den Gesetzestexten oder was ist damit wirklich gemeint, wenn Kommunikationsdaten und ruhende

76 Bundesgesetzblatt Jahrgang 2021 Teil 1 Nr. 13
77 https://twitter.com/echo_pbreyer/status/1412726238670696456 https://www.europarl.europa.eu/news/de/headlines/society/20210701STO07548/parlament-billigt-regelung-zur-bekampfung-von-kindesmissbrauch-im-internet
78 https://www.heise.de/news/Bundesgerichtshof-Sicherer-E-Mail-Dienst-Tutanota-muss-Ueberwachung-ermoeglichen-6051834.html; BGH, Beschluss vom 28.04.2021 -2 BJs 366/19-9 VS-NfD

Daten doch wieder für Dritte zugänglich gemacht werden müssten und das teilweise vor der Verschlüsselung? Unter diesen Gesichtspunkten ist die Aufregung zum Thema Telefax nicht nachvollziehbar.

7.5 E-Mail-Inhalt schützen nicht immer praxistauglich

Bei den Alternativen zum Fax wurde der Versand verschlüsselter E-Mails empfohlen. Es ergibt sich von selbst, dass in dem Fall Absender und Empfänger die Möglichkeiten haben müssen, verschlüsselte Inhalte per E-Mail zu senden und zu empfangen.

Es gibt unterschiedliche Möglichkeiten den Inhalt einer E-Mail-Nachricht vor einer unberechtigten Einsichtnahme zu schützen. Doch sind nicht alle Möglichkeiten für die Masse praxistauglich.

Um sensible Informationen schützen zu wollen, sind zwei Dinge zu unterscheiden:

1. Das ist zum einen der Transportweg, indem Daten von einer Endstelle zur anderen Endstelle transportiert (übertragen) werden.

2. Und zum anderen der Inhalt der Nachrichten selbst, die irgendwo abgelegt sind. Man spricht in dem Fall auch von den „ruhenden Daten“.

Für das Erstere kommt die uns bekannte Transportverschlüsselung (TLS) zum Einsatz und das Zweite ist eine Inhaltsverschlüsselung der gesamten Nachricht (u.a. auch Ende-zu-Ende Verschlüsselung genannt). Auf Einzelheiten soll hier nicht weiter eingegangen werden. Weitreichende Informationen haben wir u.a. in unserem Tätigkeitsbericht 2020[79] aufgeführt. Hinzuweisen ist, dass TLS ein geeignetes Verschlüsselungsverfahren zur Datenübermittlung und eine zusätzliche Inhaltsverschlüsselung nicht zwingend bei jeder Datenkategorie erforderlich ist.

Unter dem Punkt zum Thema Telefax wurde bereits erwähnt, welche Meinung einige Behörden vertreten. Zugleich wird der Hinweis zur sicheren E-Mail-Kommunikation durch eine Inhaltsverschlüsselung per S/MIME (Se-

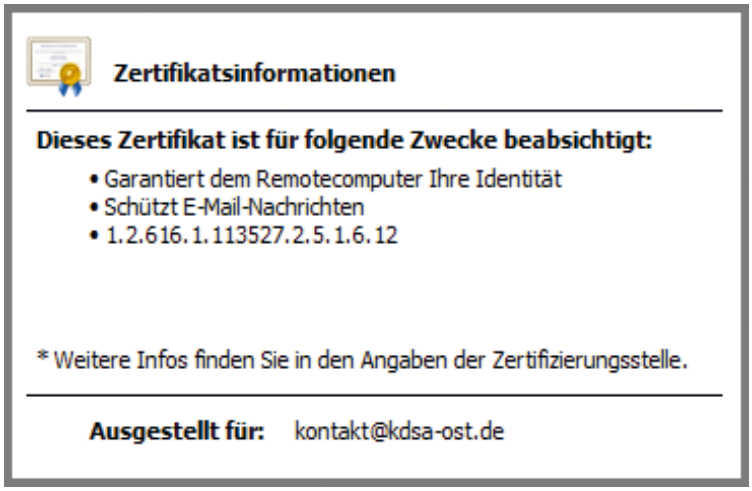
79 KDSA Ost, TB 2020, Punkt 7.2

cure / Multipurpose Internet Mail Extensions) oder per PGP (Pretty Good Privacy) Verfahren genannt. Beide Verfahren sind unstrittig und gehen über die reine Transportverschlüsselung hinaus. Das würde im Umkehrschluss bedeuten, dass bei sachgerechter Inhaltsverschlüsselung keine Transportverschlüsselung erforderlich wäre.

Die Beauftragung und die Integration von S/MIME oder PGP ist für die breite Masse mit den unterschiedlichsten E-Mail-Programmen kaum praktikabel. Glaubwürdige S/MIME Zertifikate haben beispielsweise nur eine begrenzte Laufzeit und sind kostenpflichtig. Ein weiteres Problem stellt sich beim Wechsel der E-Mail-Adresse oder bei der Archivierung von verschlüsselten Nachrichten, wenn das Zertifikat bereits abgelaufen und nicht mehr verfügbar ist. Verschlüsselte Nachrichten können immer nur mit dem entsprechenden und installierten Zertifikat geöffnet werden. Ist das Zertifikat einmal verloren, dann kann auch die E-Mail-Nachricht nicht mehr geöffnet werden. Viele Organisationen und Behörden die S/MIME oder PGP empfehlen, müssen sich oftmals nicht selbst um das Sicherheits-Schlüssel-Management kümmern. Die Ver- bzw. Entschlüsselung übernehmen zentrale Sicherheits-Gateway für sie.

Verwechselungsgefahr nicht unbedingt ausgeschlossen.

In einer Welt, in der alle E-Mail-Sender und Empfänger ein S/MIME Zertifikat hätten, könnte es auch zu Fehlzustellungen kommen, indem ausversehen ein scheinbar ähnliche E-Mail-Adressat ausgewählt wird. Der einzige Unterschied bleibt bei den „ruhenden Daten", die dann verschlüsselt vorliegen.

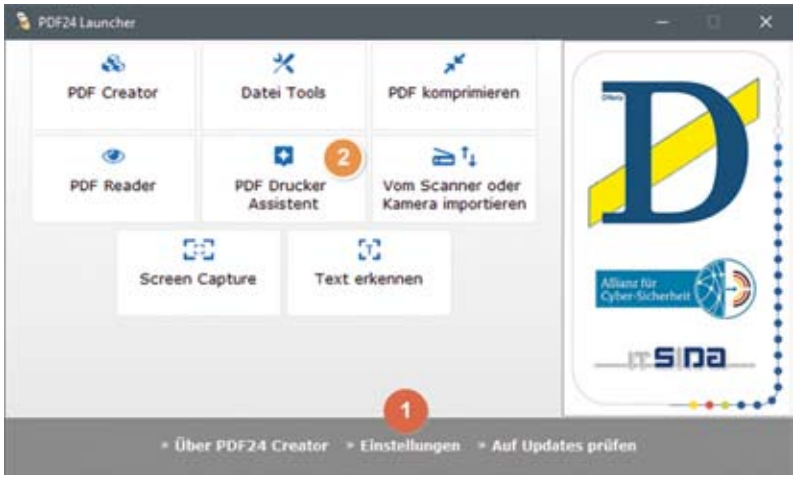


7.5.1 Inhaltsverschlüsselung durch verschlüsseltes PDF

Es gibt viele Möglichkeiten Dokumente oder Dateien vor unberechtigtem Zugriff zu schützen. Eine einfache und vielfach genannte Variante zur Inhaltsverschlüsselung ist, sensible Informationen als E-Mail-Anlage in Form eines verschlüsselten PDF's zu versenden. Sie ist praktisch ohne viel Aufwand realisierbar und mit dem passenden Kennwort u.a. auch gut zur Archivierung geeignet. Bei einer Kommunikation mit wiederkehrenden Empfängern oder im Rahmen einer Gruppenkommunikation könnten sich die Beteiligten zuvor auf ein Kennwort einigen, welches nur einmal mitgeteilt werden muss. Zudem bietet diese Art des Dokumentenschutzes einen Zugriffsschutz bei internen oder externen Dokumentenablagen (z.B. im Dateisystem oder der Cloud) und würde als Faxersatz geeignet sein.

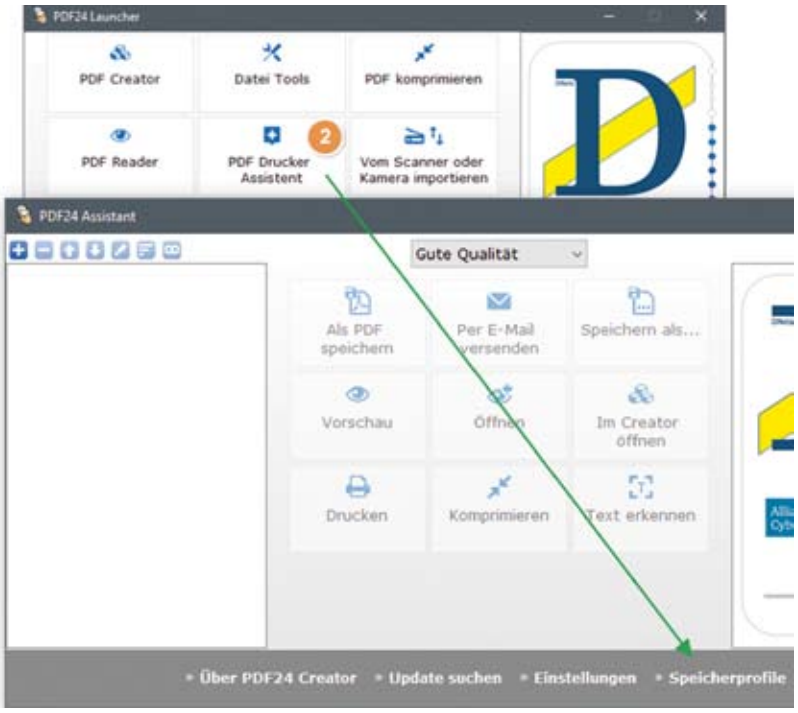
Programme, die ein PDF erstellen und verschlüsseln können, gibt es viele. Je nach Einsatzzweck (privat, betrieblich/gewerblich) sind die Nutzungs- und Lizenzbestimmungen der Softwarehersteller zu beachten. Am Beispiel der Software „PDF24 Creator" (PDF24) soll gezeigt werden, wie mit Hilfe eines dafür vorbereiteten Profils eine verschlüsselte PDF-Anlage auf einfache Weise erstellt werden kann.

Es wird angenommen, dass die Software „PDF24 Creator" (pdf24.org) bereits installiert wurde. Für die Verteilung im Netzwerk bietet sich dafür das MSI Paket an. Installiert werden sollten nur Optionen/Funktionen, die auch tatsächlich benötigt werden.



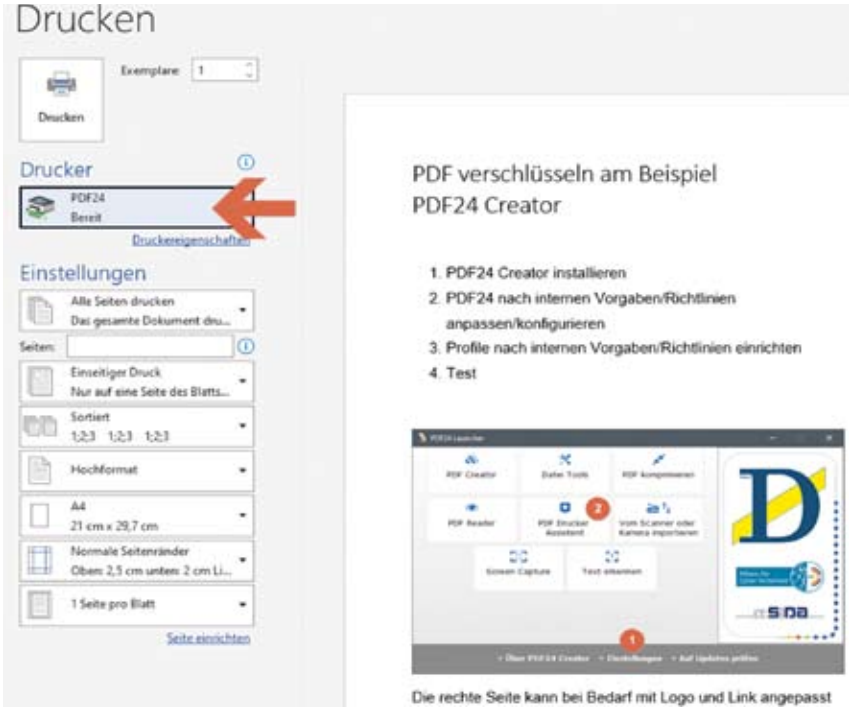
Schritt 1): Das Programm PDF24 starten und nach internen Vorgaben/Richtlinien grundlegende Einstellungen vornehmen (in der Abbildung unter 1). Benutzerspezifische Profile können im Bereich „PDF Drucker Assistent" (in der Abbildung unter 2) eingerichtet werden.

Schritt 2): Ein neues Profil einrichten. Dazu Im Bereich „PDF Drucker Assistent“ unter „Speicherprofile“ ein spezielles Profil zur PDF-Verschlüsselung einrichten. Dieses steht später zur Auswahl zur Verfügung.



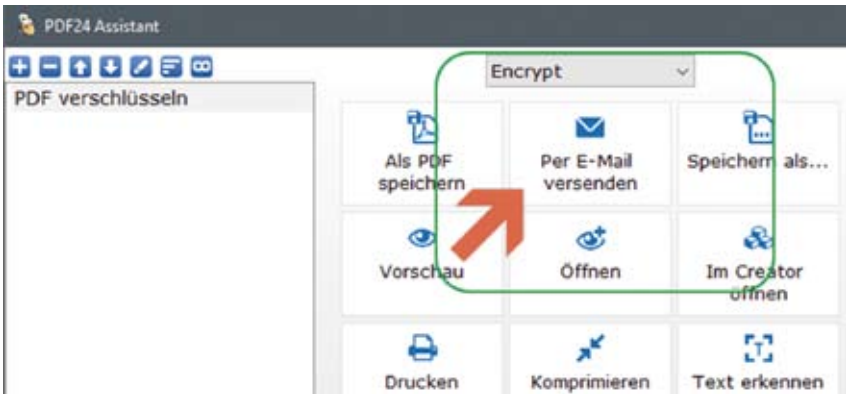
Dem neuen Profil einen Namen geben, z.B. „Encrypt“, und nach den Bedürfnissen einrichten. In diesem Beispiel ist das Profil so eingerichtet, dass vor PDF-Erstellung bei Auswahl des Profils eine Kennwort-Eingabe erscheint. Nur mit diesem Kennwort kann das PDF-Dokument anschließend geöffnet werden.

Weiter unten in diesem Bereich gibt es weitere Einstellmöglichkeiten u.a. kann noch eine zusätzliche Datei am Anfang oder am Ende des Dokuments hinzugefügt werden oder ein Wasserzeichen wie z.B. „Vertraulich“ integriert werden.

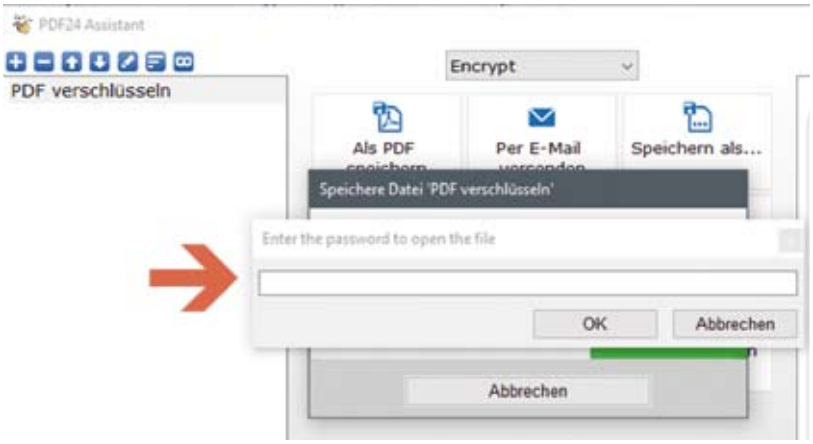


Schritt 3): Der Test, dafür beispielsweise ein Testdokument mit Word erstellen und über den PDF24 Druckerdialog ausdrucken.

Nachdem der PDF24 Druckerdialog erscheint, wird das neu angelegte Profil „Encrypt“ ausgewählt.

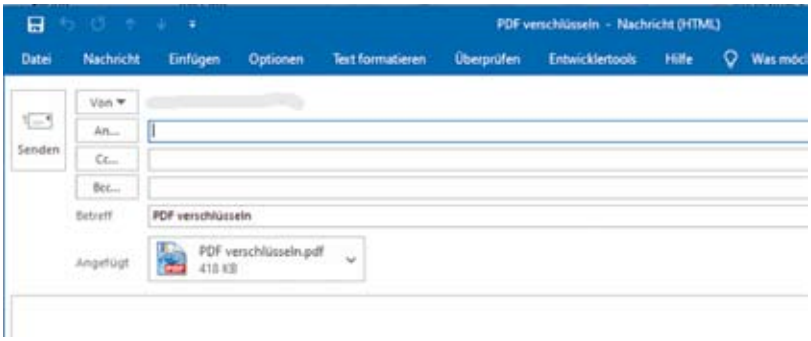


Hier kann noch entschieden werden, ob das Dokument als PDF gespeichert werden soll oder direkt als Anlage in einer neuen E-Mail geöffnet wird.

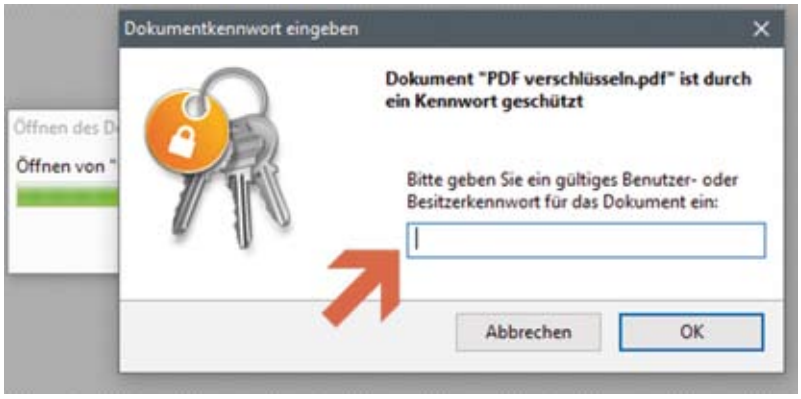


Im weiteren Dialog erfolgt die Kennworteingabe. Achtung: Nur mit diesem Kennwort kann das Dokument später wieder geöffnet werden, also Kennwort gut merken.

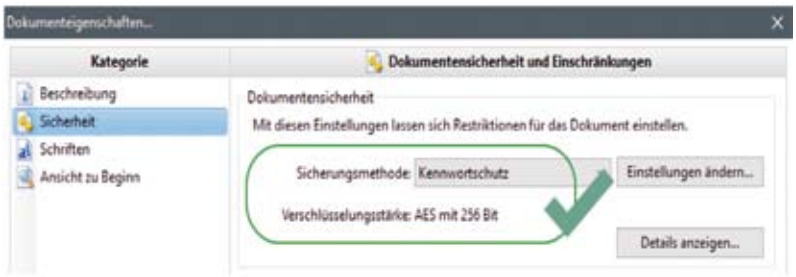
Bei korrekter Einrichtung öffnet eine neue E-Mail-Nachricht mit der eben erstellten PDF-Anlage.



Zum Testen, ob auch alles so funktioniert hat, sollte die Anlage nur noch mit dem dazu passenden Kennwort geöffnet werden können. Das lässt sich prüfen, indem versucht wird, die Anlage zu öffnen. Jetzt sollte die Aufforderung zur Eingabe des Dokumenten-Kennworts erscheinen.



In den Dokumenteneigenschaften kann die Sicherheit zusätzlich überprüft werden.Falls alles funktioniert hat, ist das Dokument somit vor einer unberechtigten Kenntnisnahme geschützt. Die E-Mail ist in diesem Fall nur noch das Transportmittel des geschützten Dokuments.



7.6 Sensible Daten sammeln, so einfach war es noch nie

Die Corona-Pandemie und Smartphones machen es möglich, wovor immer wieder gewarnt wurde. An Eingängen von Einrichtungen, in Garderoben, bei Veranstaltungen, in Bädern, in Hotels etc. wird in Form von Hinweisschildern darauf hingewiesen, dass für die Sicherheit seiner Wertsachen keine Gewähr übernommen werden könne.

Polizei, Banken und Behörden hatten regelmäßig dahingehend sensibilisiert, dass Wertsachen sicher aufbewahrt werden sollten und nicht überall mitzutragen sind. Es wurde auf unseriöse Telefanrufe, die Enkeltrickmasche, unseriöse Haustürbesucher, u.a. hingewiesen, zum Teil zusätzlich in Rundfunk und Fernsehen.

Was früher nur einem eingeschränkten Kreis möglich war (Behörden, Polizei), so wurden auf einmal Dienstleister, Gastronomen und Veranstalter verpflichtet, Impf-/Test-Nachweise in Kombination mit einem gültigen Ausweisdokument zu kontrollieren. "Normale Personen" wurden auf einmal zu einer Kontrollinstanz und betroffene Besucher mussten zusätzlich Identitätsnachweise mit sich führen.

Die Kontrolle/ der Abgleich eines Impfausweises oder eines digitales Impfzertifikates mit einem amtlichen Ausweisdokument[80] kann etwas Zeit in Anspruch nehmen. Das reine Hinhalten der Dokumente reicht dabei oftmals nicht aus, denn die Überprüfung sollte ja korrekt sein – ansonsten droht ein Bußgeld.

Vor Corona gab es auf Festveranstaltungen (Stadtfest, Straßenfest, etc.) die unendlich vielen Preisausschreiben, an denen man sich mit seinen Daten z.B. auf einer Postkarte in der Hoffnung auf einen Gewinn beteiligen konnte. Datensammler kamen so beispielsweise an Adressdaten. Es kam zwar nicht immer zu einem Gewinn, aber irgendwann, als die freiwillige Teilnahme am Preisausschreiben in Vergessenheit geraten war, kam es zu unliebsamen Werbesendungen.

Mit Corona hat sich dahingehend einiges geändert und es für Adresssammler und kriminelle Machenschaften vereinfacht. Der Gesetzgeber hat

80 Bildquelle Bundesministerium des Innern und für Heimat

allen vorhergehenden Sensibilisierungen mit seinen Daten achtsam umzugehen getrotzt und das Sammeln sensibler Daten legitimiert, vermutlich in der Hoffnung, dass sicher und sorgsam damit umgegangen wird. Hinzu kam, dass dann auch noch die Daten wie Vorname, Name und Geburtsdatum mit einem amtlichen Dokument verifiziert werden sollten – ansonsten drohte ein Bußgeld. In Rundfunk und Fernsehen wurde zusätzlich explizit darauf hingewiesen, die Impfnachweise und den Personalausweis zu Identifikationsprüfung mitzuführen.

Jede gewiefte Person, die an Personendaten ein Interesse haben könnte, bräuchte sich nur vor einen Eingang einer größeren Einrichtung stellen und die Nachweise kontrollieren. Mit einer App wäre das schnell getan, dann noch schnell ein Bild vom Personalausweis fertigen. Für Cyber-Kriminelle wären das bereits keine normalen Adressdaten mehr, vielmehr wären es bereits qualifizierte und geprüfte Daten - quasi Echtdaten. Vor einer Preisgabe der **Kombination: Vornamen, Name, mit Geburtsdatum** hatten Behörden und Sicherheitsexperten schon immer gewarnt.

Wir können nur hoffen, dass diese Daten u.a. auch die Daten der geführten Listen nicht an Kriminelle gelangen und/oder im Internet angeboten werden. Dem Missbrauch solch qualifizierter Daten und Informationen, gerade im Bereich des Social-Engineering oder Phishing, steht fast nichts mehr im Weg. Trickbetrüger können damit noch besser Vertrauen aufbauen oder Vertrauen gewinnen.

7.7 Doxing – Was wollen Die mit meinen Daten, ich habe doch nichts zu verbergen!

Diese und ähnliche Kommentare gibt es fast immer bei Veranstaltungen oder Diskussionen, sobald es um das Thema Datenschutz geht. Ist allerdings jemand Opfer durch einen Missbrauch seiner persönlichen Daten geworden, tritt gelegentlich ein Bewusstseinswandel auf. Erst als Betroffene von Cyberkriminalität oder Cyber-Mobbing merken viele, was sie in der Vergangenheit besser hätten verbergen sollen. Geschäftsmodelle der Cyberkriminalität könnten ohne die Verwendung personenbezogener Daten nicht so erfolgreich sein wie sie sind! Darunter zählen u.a. die altbekannten Enkeltricks, Telefonanrufe von angeblichen Bankmitarbeitern und/oder Behörden oder auch Anrufe von angeblichen Microsoft Support-Mitarbeitern.

Doxing und Datenschutz[81]

Die Wortmischung stammt u.a. aus der Informationssicherheit und setzt sich aus einer Mischung aus Dokument und Tracing (Doc+Tracing) zusammen. Dabei handelt es sich um eine Art Informationssammlung persönlicher Daten von Zielpersonen, den späteren Opfern. Das erfolgt zum Teil legal aus öffentlichen Quellen, aber auch illegal, um vorhandene Daten mit weitreichenden Informationen anzureichern. Je größer der Umfang der Datensammlung ist, desto erfolgversprechender ist die persönliche Ansprache des Opfers. Das Doxing Opfer merkt nicht sofort, dass seine persönlichen Daten für kriminelle Vorhaben präpariert wurden. Der Umfang der Daten, die das Internet zur Verfügung stellt, weil viele Menschen so freizügig mit ihren personenbezogenen Daten oder oftmals auch mit den personenbezogenen Daten Anderer (z.B. Daten in Adressbüchern, Bilder, Messanger, etc.) umgehen, macht es den Cyber-Kriminellen einfach, an Informationen zu gelangen. Und bis dahin noch, ohne Daten zu stehlen.

Reichen dennoch die verfügbaren Daten für einen geplanten oder einen in Auftrag gegebenen Cyber-Angriff nicht aus, so wird mit Hilfe anderer Tricks (Techniken) versucht, an die benötigten Informationen zu gelangen. Hierbei helfen den Cyber-Kriminellen die zuvor gesammelten Informationen, um noch gezielter z.B. per Phishing und Social Engineering den Datenbestand mit weiteren wichtigen Informationen (z.B. Beschäftigungsverhältnis, Vorlieben, Hobbys usw.) anzureichern. Sind für einen Cyber-Angriff auf eine Person, einen Betrieb oder eine Organisation genügend qualifizierte Daten vorhanden, können sich die Betroffenen dem nicht mehr entziehen. **Die „Maschinerie“ ist angelaufen und kaum noch zu stoppen.**

Für das Geschäftsmodell der Cyber-Kriminellen sind persönliche Daten von großem Vorteil. Diese Informationen haben die Opfer häufig selbst veröffentlicht oder sie wurden von Dritten bekannt gemacht. Dazu gehören u.a. auch Bilder, Chatinhalte oder Kontakte auf dem Smartphone. Es gilt deshalb das, was schon das Bundesverfassungsgericht festgestellt hat:

Es gibt keine unwichtigen Daten!

81 KDSA-Ost, TB 2019, Punkt 7.9; Doxing im Business von Kaspersky in Englisch „Doxing in the corporate sector (engl)“ https://securelist.com/corporate-doxing/101513/

7.7.1 Die Masche mit der SMS zur falschen Tracking App

Auch im Berichtsjahr gingen sehr viele Menschen auf Online-Shopping-tour. In der Zeit der vielen Paketzustellungen machte vor allem die SMS-Tracking-Masche[82] auf sich aufmerksam. Hier wurden gefälschte Pakte-Benachrichtigungen per SMS an Mobilrufnummern versendet. Empfänger waren teilweise verwundert, woher die realistische Anrede mit eindeutigem Namen stammt und sahen die SMS als vertrauenswürdig an.

Es fing mit dem Empfang einer SMS zur angeblichen Paketverfolgung an: Die SMS-Nachrichten schienen durch die Anrede mit „Hallo …" aus einer **scheinbar vertrauten Quelle** zu sein.

Falls jetzt jemand meint: Das kann mir nicht passieren! Dann wäre allerdings die Verbreitung an die mobilen Empfänger-Rufnummern (SMS) nicht so erfolgreich.

82 https://www.n-tv.de/ratgeber/Warnung-vor-gefaelschten-Paket-SMS-article22478017.html
https://www.heise.de/news/Ihr-Paket-kommt-an-Links-in-falschen-Tracking-SMS-fuehren-zu-Banking-Trojaner-5995597.html

Ein Klick auf den Link führt zu einer Website, die optisch so aufbereitet erschien, dass sie einer von DHL ähnelte. Hier kann der Benutzer die „angebliche“ App zur Paketverfolgung heruntergeladen [1].

Nach dem Herunterladen und dem Ausführen der App war es auch schon passiert. Das Gerät wurde mit einem Trojaner/Virus (Schadprogramm) quasi „verseucht“ und damit kompromittiert.

Alles Weitere spielt sich ab diesem Zeitpunkt im Hintergrund des Smartphones ab, bei in einem ersten Schritt alle Kontaktdaten des Gerätes auf Systeme der Kriminellen übertragen wurden. Mit diesen Kontaktdaten können wiederum SMS-Nachrichten an weitere Personen verteilt werden. **Daher stammen u.a. die vertrauten Anreden in den SMS-Nachrichten.**

Unter „Analyse der Berechtigungen“ der Mobile-App kann man erahnen, was so alles im Hintergrund geschehen könnte:

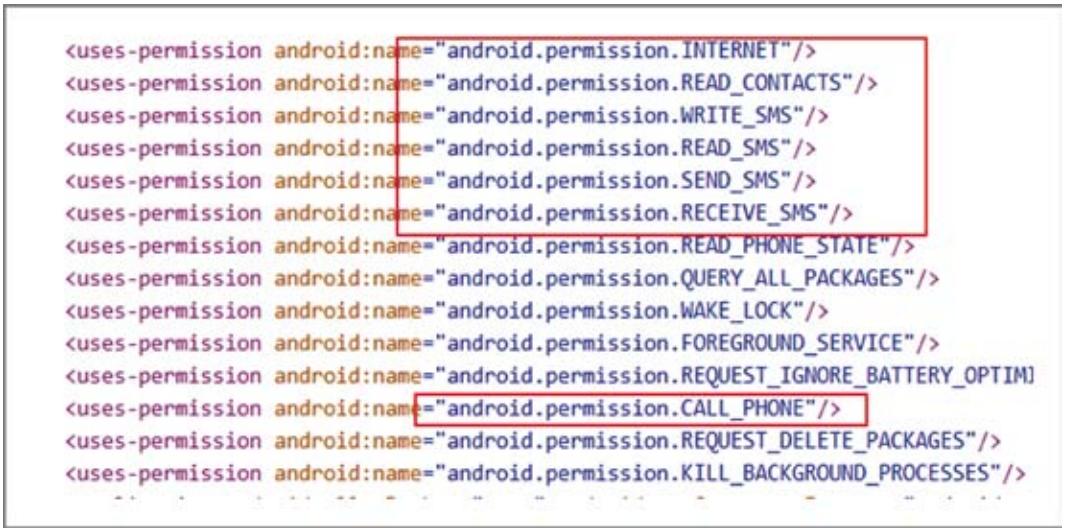
- System Broadcast-Nachrichten auswerten (das sind u.a. Nachrichten, die auf dem Gerät aufpoppen, wie z. B. beim Eingang einer neuen Chat-Nachricht, einem Telefonanruf oder einer SMS, Systemnachrichten, etc.).
- das Telefon verwenden um Anrufe zu tätigen, z.B. kostenpflichtige Rufnummern

- SMS-Nachrichten verarbeiten – abhören, senden, empfangen, erstellen etc. Z.B. SMS an kostenpflichtige Rufnummern senden oder Bank-Transaktionsnummern abfangen, diese verändern und die geänderte Nummer anzeigen
- u.v.m.

Für Techniker - hinter die Kulissen geschaut

Nachdem auf der angezeigten Website auf den Link geklickt wird (im Bild unter [1]), erfolgte eine Weiterleitung zu einer anderen Webadresse, von der die eigentliche App heruntergeladen wurde [2]. Wie oben im Bild dargestellt, kann sich die Webadresse in der SMS-Nachricht ändern. Hierbei könnte es sich auch um kompromittierte Websites handeln, die speziell für solche Zwecke den Kriminellen zur Verfügung stehen.

Analyse der Berechtigungen der App:



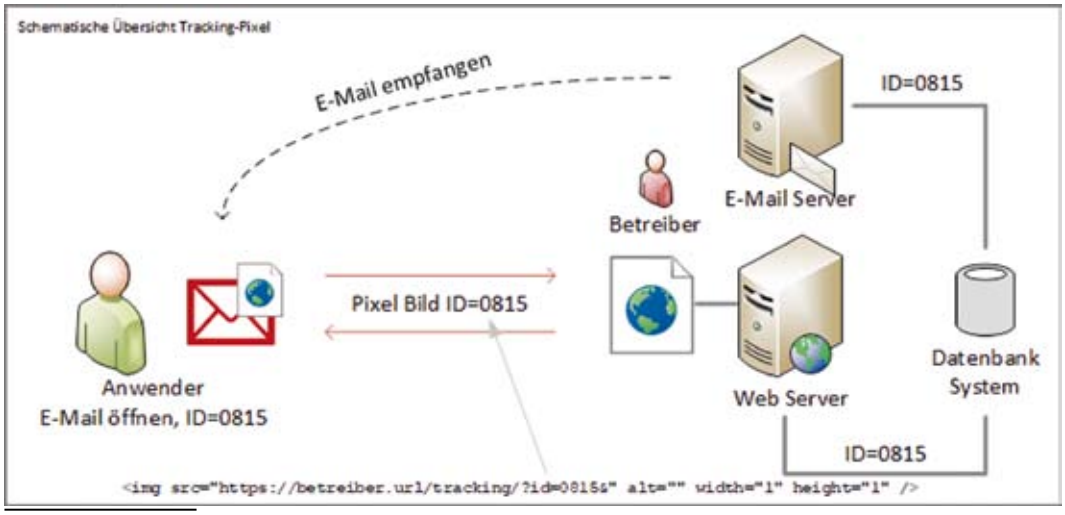
```
<activity android:launchMode="singleTop" android:name="com.iqiyi.i18n.Co
    <intent-filter>
        <action android:name="android.intent.action.SEND"/>
        <action android:name="android.intent.action.SENDTO"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <category android:name="android.intent.category.BROWSABLE"/>
        <data android:scheme="sms"/>
        <data android:scheme="smsto"/>
        <data android:scheme="mms"/>
        <data android:scheme="mmsto"/>
    </intent-filter>
```

7.8 E-Mail-Tracking im Hintergrund

In unserem letzten 5. Tätigkeitsbericht[83] wurde zum Thema „Cookies und Tracking“ u.a. auch das E-Mail-Tracking erwähnt.

In Zeiten in denen es sich überwiegend um Website-Cookies und Consent-Banner dreht, ist die Sensibilisierung auf diese Art des Tracking mit Hilfe eines Tracking-Pixels in den Hintergrund geraten. Wobei es sich um eine gängige Praxis zur Nachverfolgung von E-Mail-Nachrichten handelt.

Die Art und Weise des E-Mail-Trackings, also versendete Nachrichten nachverfolgbar zu gestalten, ist keine neue Erfindung, sondern eine recht alte und auch einfach umzusetzende Technologie. Einzige Voraussetzung ist,



83 KDSA Ost, TB 2020, Punkt 7.4

dass so eine E-Mail-Nachricht im HTML Format erzeugt wird und geöffnet werden darf.

Auslöser des Nachrichten-Trackings ist ein eingebettetes kleines Bild, welches auf dem Display nicht ersichtlich ist - das sogenannte 1x1 Pixel Bild (Tracking-Pixel). Sobald eine E-Mail-Nachricht im HTML Format angezeigt wird (mit allen Bildern) und sich darin ein Tracking-Pixel befindet, wird eine Verbindung zu dem Server, der das Bild verwaltet (Betreiber), hergestellt. An dem Verbindungslink des Tracking-Pixels (IMG-URL) hängt zusätzlich ein für diese Nachricht generiertes Identifikationskennzeichen (ID). Damit kann der Betreiber die Nachricht anhand der ID direkt zuordnen.

Da sich alles im Hintergrund abspielt, während die Nachricht geöffnet wird und Bilder, die sich in der Nachricht befinden, nachgeladen werden, bemerkt der Anwender davon nichts.

Anders verhält es sich auf der Seite des Betreibers. Er erhält dadurch eine Menge an Informationen, wie z.B.:

- dass die E-Mail-Adresse existiert
- dass es sich um eine „Aktive E-Mail-Adresse“ handelt, also eine E-Mail-Adresse, die u.a. auch verwendet wird
- dass der Endbenutzer HTML formatierte Nachrichten empfängt und komplett herunterlädt (Daten nachladen darf)

Zusätzlich werden, wie beim Surfen mit einem Webbrowser, Metadaten an den Betreiber übermittelt.

Wer Tracken will - egal welche Daten - wird immer nach Möglichkeiten suchen und diese auch einsetzen. Denn es handelt sich dabei um ein attraktives Geschäftsmodell, welches u.a. auch bei vielen „scheinbar kostenfreien“ Mobile-Apps Anwendung findet. Endanwender denken oftmals nicht darüber nach, dass eine Entwicklung und das Betreiben z.B. von Mobile-Apps irgendwie finanziert werden muss. Bezahlt wird meisten dann nicht mehr in Euro, sondern mit den eigenen persönlichen Daten, die u.a. als Ware verkauft werden könnte (siehe auch den Beitrag unter 1.2.3 in diesem Bericht).

Anhang

Vorlagen

Checkliste zur Selbstkontrolle

Organisationskontrolle	Ja	Nein
Ist ein Datenschutzbeauftragter (§ 36 KDG) vorhanden?		
Sind Mitarbeiter zum Datengeheimnis nach § 5 KDG verpflichtet?		
Ist eine Mitarbeiterschulung zum Datenschutz erfolgt?		
Gibt es Unterlagen zum Datenschutz wie Datenschutzkonzept, Handbuch, Verzeichnis von Verarbeitungstätigkeiten (§ 31 KDG)?		
Zutrittskontrolle (physischer Zutritt)	**Ja**	**Nein**
Gibt es eine Zutrittsbeschränkung zum Gebäude?		
Sind Räume mit Server oder TK nur für befugtes Personal zugänglich?		
Sind die Server sicher aufgestellt?		
Gibt es eine Zutrittsbeschränkung für Räume, in denen personenbezogene Daten abgelegt werden (Akten, Datenträger)?		
Zugangskontrolle	**Ja**	**Nein**
Sind Bildschirmsperren eingerichtet?		
Gibt es eine installierte Firewall, die aktiviert ist und aktualisiert wird?		
Gibt es ein installiertes Anti-Virenprogramm, das aktiviert ist und aktualisiert wird?		
Müssen sich Benutzer identifizieren bzw. authentifizieren?		
Werden sichere Passwörter verwendet?		
Zugriffskontrolle	**Ja**	**Nein**
Gibt es ein Rollen- und Rechtekonzept?		
Werden DS-Verletzungen protokolliert?		
Gibt es ein Löschkonzept für die unterschiedlichen Daten?		
Weitergabekontrolle	**Ja**	**Nein**
Gibt es Verschlüsselungsmöglichkeiten beim Datentransport?		
Werden Datenverarbeitungssysteme regelmäßig gewartet und geprüft?		
Werden veraltete Geräte und Zubehör sicher entsorgt?		
Ist die Nutzung privater Geräte beschränkt?		

Eingabekontrolle	Ja	Nein
Gibt es für das Erheben, Ändern und Löschen von personenbezogenen Daten Protokolle?		
Wird der Umgang mit Verwaltungsakten dokumentiert?		
Auftragskontrolle	**Ja**	**Nein**
Werden mit Auftragnehmer die notwendigen Vereinbarungen gemäß § 29 KDG getroffen?		
Werden Auftragnehmer auch auf das Datengeheimnis nach § 5 KDG verpflichtet?		
Verfügbarkeitskontrolle	**Ja**	**Nein**
Sind die Daten gegen unbeabsichtigtes Löschen oder Vernichten gesichert?		
Werden Datensicherungen, Archive oder Backups sicher aufbewahrt?		
Trennungskontrolle	**Ja**	**Nein**
Werden Daten, die für unterschiedliche Zwecke erhoben wurden, auch voneinander getrennt voneinander verarbeitet?		

Muster - Informationspflicht für Fotos gemäß §§ 14, 15 KDG

A. Datenverarbeiter

1. Verantwortlicher:

Einrichtung / Firma: <Name der Einrichtung>

Name: <Name der verantwortlichen Person>

(in der Regel die Einrichtungsleitung oder der Träger)

Anschrift: <...>

Telefon: <...>

E-Mail: <...>

Ggf. Vertreter: <Name>

(Die Angaben zum Verantwortlichen haben eine ladungsfähige Anschrift zu enthalten. Bei juristischen Personen ist zudem die Firma anzugeben.)

2. Betrieblicher Datenschutzbeauftragter

Name: <…>

Anschrift: <…>

Telefon: <…>

E-Mail: <…>

B. Verarbeitungsrahmen

1. Zweck der Datenerhebung:

Die Anfertigung und Nutzung von Fotos erfolgen zur:Dokumentation / Information / Einblicke in die pädagogische Arbeit

- Führen eines Portfolios oder einer Entwicklungsdokumentation
- Veröffentlichung oder Information zu Aktivitäten (z.B. Ausflüge, Projekte, Veranstaltungen)
- Festhalten von Erinnerungen (z.B. Kassenfotos, Jahrgangsfotos) etc.

(Hinweis: Eine Verarbeitung für einen der hier genannten Zwecke findet nur statt, wenn dieser auf der Einwilligungserklärung für Fotoaufnahmen durch den Erziehungsberechtigten angekreuzt / ausgewählt worden ist.)

2. Rechtsgrundlage:<…>

Die Veröffentlichung sowie auch die Weitergabe von Fotos erfolgt nur, wenn Sie Ihre Einwilligung dazu gegeben haben.

(Das Führen einer Entwicklungsdokumentation als gesetzliche Verpflichtung darf hier nur aufgeführt werden, wenn diese eine Dokumentation in Form von Fotos vorschreibt. Eine Kann-Bestimmung ist nicht ausreichend.)

3. Berechtigte Interessen der Datenerhebung:<…>

(Berechtigte Interessen gemäß § 6 Abs. 1 lit. g) sind zu begründen.)

4. Dauer der Speicherung personenbezogener Daten:

Dokumentation der pädagogischen Arbeit	SD-Karte der Digitalkamera	2 Wochen
	Festplatte Laptop	bis zur Entwicklung über Fotodienstleister, maximal 2 Monate
	Webseite Kita	Solange bis der Zweck erfüllt ist
Jahrgangsfoto	SD-Karte Digitalkamera	maximal 2 Wochen
	Festplatte Laptop	bis zum Druck des Jahrgangsbuch, maximal 1 Schuljahr ab Erstellung
	Jahrgangsbuch / Schulchronik	dauerhaft
Fotos für die Entwicklungsdokumentation / Portfolio	SD-Karte Digitalkamera	maximal 2 Wochen
	Festplatte Laptop	bis zur Entwicklung über Fotodienstleister, maximal 2 Monate
	Entwicklungsdokumentation / Portfolio	bis zum Ende der Betreuungszeit

5. Erforderlichkeit bzw. gesetzliche Verpflichtung zur Bereitstellung der personenbezogenen Daten

> *Es gibt keine gesetzliche oder vertragliche Grundlage für das Erstellen und Verarbeiten von Fotos. Fotos in der Entwicklungsdokumentation können hilfreich beim Dokumentieren sein. Aus einer Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile.*

6. Profiling: Ein Profiling findet nicht statt.

C. Weitergabe an Dritte und Auslandsbezug

1. Empfänger oder Kategorien von Empfängern der Fotos:

- Besucher der Webseite

- Fotodienstleister
- Presse

(sofern die ausgewählten Zwecke dies zulassen)

2. Absicht, die personenbezogenen Daten an oder in ein Drittland oder an eine internationale Organisation zu übermitteln: <...>

3. Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses: <...>

D. Rechte der Betroffenen

1. Auskunftsrecht: <...>

2. Recht auf Berichtigung: <...>

3. Recht auf Löschung: <...>

4. Recht auf Einschränkung der Verarbeitung <...>

5. Recht auf Datenübertragbarkeit: <...>

6. Widerspruchsrecht: <...>

7. Widerrufsrecht der Einwilligungserklärung:
   (Diese Angabe ist erforderlich, da die Erhebung der personenbezogenen Daten auf eine Einwilligung nach § 6 Abs. 1 lit. b) KDG KDG beruht.)

8. Recht auf Beschwerde bei der Datenschutzaufsicht: <...>

9. Recht auf gerichtlichen Rechtsbehelf: <...>

Stand: TT.MM.JJJJ

Microsoft Windows 10 Versionsinformationen

Windows 10 - Lebenszyklus und Supportende (Stand der Technik)

Version	Latest Revision Date	End of serviing: Home, Pro, Pro Education and Pro for Workstations	End of servicing: Enterprise, Education and IoT Enterprise
21H2	**2022-02-15**	**2023-06-13**	**2024-06-11**
21H1	2022-02-15	2022-12-13	2022-12-13
20H2	2022-02-15	2022-05-10	2023-05-09
1909	2022-02-08	End of servicing	2022-05-10

Quelle: https://docs.microsoft.com/en-us/windows/release-health/release-information

Windows 11 - Allgemeine Verfügbarkeit ab Oktober 2021

Microsoft Exchange Server (Stand 2021)

Exchange Server 2019 CU11	9. November 2021	15.02.0986.014
Exchange Server 2016 CU22	9. November 2021	15.01.2375.017
Exchange Server 2013 CU23	9. November 2021	15.00.1497.026
Updaterollup 32 für Exchange Server 2010 SP3	2. März 2021	14.03.0513.000

Quelle: https://docs.microsoft.com/de-de/exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019

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.

Organigramm

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.

Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
ArbG	Arbeitsgericht
ArbSchG	Arbeitsschutzgesetz
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BSI	Bundesamt für Sicherheit und Information
BT-Drs.	Bundestag-Drucksache
BVerfG	Bundesverfassungsgericht
BZRG	Bundeszentralregistergesetz
BZSt	Bundeszentralamt für Steuern
DiGA	Digitale Gesundheitsanwendungen
DSB	Datenschutzbehörde
DSK	Datenschutzkonferenz
DS-GVO	Datenschutz-Grundverordnung
DVPMG	Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz
DVG	Digitale-Versorgung-Gesetz
ePA	elektronische Patientenakte
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GG	Grundgesetz

HTML	Hypertext Markup Language (Auszeichnungssprache für Webseiten)
http	Hypertext Transfer Protokoll (unverschlüsselt)
https	Hypertext Transfer Protokoll Secure (verschlüsselt)
IDSG	Interdiözesane Datenschutzgericht
LABG	Lehrerausbildungsgesetz
LAG	Landesarbeitsgericht
LehVDVO	Lehrervorbereitungsdienstverordnung
LG	Landgericht
KDG	Kirchliches Datenschutzgesetz
KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz
KIS	Krankenhausinformationssystem
MAV	Mitarbeitervertretung
MAVO	Mitarbeitervertretungsordnung
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PDSG	Patientendaten-Schutz-Gesetz
PVS	Verband der Privatärztlichen Verrechnungsstelle e.V.
RegMoG	Registermodernisierungsgesetz
RiLi	Richtlinie
SDES-sRTP	VoIP-Telefonie mit Sprachverschlüsselung
SGB	Sozialgesetzbuch
SMTP	E-Mail-Übertragungsprotokoll
SSL	Secure Socket Layer (TLS)

StGB	Strafgesetzbuch
SVB	Schulverwaltungsblatt
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TLS	Transport Layer Security
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
VDD	Verbandes der Diözesen Deutschlands
VG	Verwaltungsgericht
VwVfG	Verwaltungsverfahrensgesetz
ZMV	Zeitschrift für Mitarbeitervertretung

Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und des Katholischen Militärbischofs
Badepark 4 • 39218 Schönebeck
Telefon: 03928 7179018
www.kdsa-ost.de • kontakt@kdsa-ost.de